INFORME DE AUDITORÍA TI-22-11

31 de mayo de 2022

Departamento de Salud

Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública

(Unidad 5290 - Auditoría 14434)

Período auditado: 5 de mayo de 2014 al 30 de noviembre de 2020

CONTENIDO

Página

OBJETIVOS DE AUDITORÍA **2**

CONTENIDO DEL INFORME **3**

ALCANCE Y METODOLOGÍA **3**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **4**

COMUNICACIÓN CON LA GERENCIA **6**

CONTROL INTERNO **7**

OPINIÓN Y HALLAZGO **8**

Falta de cláusulas en los contratos para proveer servicios de procesamiento, y de respaldos de las transacciones procesadas 8

RECOMENDACIONES **13**

APROBACIÓN **14**

ANEJO 1 - INFORMES PUBLICADOS **15**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **16**

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

31 de mayo de 2022

Al Gobernador, y a los presidentes del Senado de
Puerto Rico y de la Cámara de Representantes

Incluimos los resultados de la auditoría de tecnología de información que realizamos de la Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública del Departamento de Salud (Secretaría Auxiliar para Salud Ambiental). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones de los sistemas de información computadorizados del Departamento se efectuaron de acuerdo con la ley y la reglamentación aplicables.

Objetivo específico

Determinar si el Departamento estableció las cláusulas en los contratos de servicios, para el procesamiento de solicitudes y renovaciones de licencias y permisos, y solicitudes de certificaciones y endosos, las cláusulas para garantizar la continuidad del servicio en caso de la terminación del contrato, y asegurar la información de las transacciones y de los ciudadanos. Esto, de acuerdo con las políticas incluidas en la *Carta Circular 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la entonces directora de la Oficina

de Gerencia y Presupuesto (OGP)[1]; y en la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el entonces director de la OGP.

CONTENIDO DEL INFORME

Este es el tercer y último informe, y contiene 1 hallazgo del resultado del examen que realizamos de los objetivos indicados. En el **ANEJO 1**, se incluye información de los 2 informes publicados anteriormente. Los 3 informes están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 5 de mayo de 2014 al 30 de noviembre de 2020. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards* emitido por la Oficina de rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como entrevistas a funcionarios, empleados y contratistas, inspecciones físicas; exámenes y análisis de informes y de documentos generados por la entidad auditada y por fuentes externas; y de otros procesos.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgo.

[1] La *Carta Circular 77-05* fue derogada por la *Carta Circular 140-16.* Esta última contiene disposiciones similares a las de la *Carta Circular 77-05*.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento de Salud se creó en virtud de la *Ley Núm. 81 del 14 de marzo de 1912*, según enmendada, y fue elevado a rango constitucional por disposición del Articulo IV, Sección 6 de la Constitución. Es el organismo de carácter normativo en la prestación de servicios de salud en Puerto Rico. Su misión es propiciar y conservar la salud para que cada ser humano disfrute del bienestar físico, emocional y social que le permita contribuir al esfuerzo productivo y creador de la sociedad.

El Departamento es dirigido por un secretario nombrado por el gobernador con el consejo y el consentimiento del Senado de Puerto Rico. Mediante la *Orden Administrativa 240* aprobada el 4 de septiembre de 2008 por la entonces secretaria de Salud, se reorganizó la estructura organizacional conforme a la política pública del Estado Libre Asociado de Puerto Rico, y a la misión y visión del Departamento.

El Departamento cuenta con las oficinas del Secretariado y del Subsecretario de Asuntos Fiscales, de Sustancias Controladas y Cannabis Medicinal, de Comunicaciones y Asuntos Públicos, de Informática y Avances Tecnológicos, de Recursos Externos, y de Asesores Legales; y con el Consejo General de Salud. Además, cuenta con las siguientes secretarías auxiliares: de Planificación y Desarrollo; de Recursos Humanos y Relaciones Laborales, de Administración, de Promoción de la Salud, de Servicios de Médicos y Enfermería; para Salud Ambiental y Laboratorio de Salud Pública; de Reglamentación y Acreditación de Facilidades de Salud; y de Salud Familiar y Servicios Integrados.

La Secretaría Auxiliar para Salud Ambiental[2] es el componente del sistema de salud de Puerto Rico que tiene la encomienda de planificar, dirigir, coordinar y evaluar los servicios de salud ambiental que operan en los niveles central, regional y local del Departamento. Dicha responsabilidad

[2] Las actividades de la Secretaría Auxiliar para Salud Ambiental se desarrollan en tres niveles. El nivel central ejerce las funciones normativas de asesoramiento técnico, evaluación y adiestramiento. El nivel regional ejerce la función administrativa de dar dirección al sistema de acuerdo con las normas y los procedimientos establecidos por el nivel central. El nivel local realiza operaciones de campo, tales como inspecciones; reinspecciones; toma de muestras para análisis químico, bacteriológico y físico; decomisos; embargos; y clausuras.

está dirigida a la prevención y el control de problemas del ambiente que afectan la salud pública. Con este propósito, y conforme a lo establecido en el *Reglamento 7655*, *Reglamento General de Salud Ambiental* aprobado el 29 de diciembre de 2008 por el entonces secretario de Estado, la Secretaría Auxiliar para Salud Ambiental otorgaba licencias sanitarias, emitía permisos de exhumación de cadáveres y endosos para permisos y planos de construcción, realizaba inspecciones, emitía certificaciones, y realizaba y analizaba muestras de agua, entre otros.

Mediante la *Ley 161-2009, Ley para la Reforma del Proceso de Permisos de Puerto Rico*, se incorporaron las licencias sanitarias como parte del *Permiso Único*[3]. Esta certificación debe ser expedida como parte del proceso para la evaluación en el otorgamiento de un permiso de uso, por la Unidad de Salud y Seguridad de la Oficina de Gerencias y Permisos (OGPe) o un inspector autorizado, al dueño, operador o administrador de un establecimiento público y, desde octubre de 2019, se tramita como parte del *Permiso Único* mediante el Single Business Portal (SBP) de la OGPe. En el Capítulo 4.3, "Licencia Sanitaria" del Tomo IV del *Reglamento 9233*, *Reglamento Conjunto para la Evaluación y Expedición de Permisos Relacionados al Desarrollo, Uso de Terrenos y Operación de Negocios* (*Reglamento Conjunto*)[4], aprobado el 2 de diciembre de 2020 por el entonces secretario de Estado y vigente desde el 2 de enero de 2021, se establece que obtener la *Licencia Sanitaria* o *Permiso Único* no exime de cumplir con los requerimientos del *Reglamento General de Salud Ambiental* y cualquier otro reglamento, ley o normativa vigente o aplicable.

---

[3] Permiso para el inicio o la continuación de la operación de un negocio, construcción o actividad incidental, en el que se consolidan permisos, licencias, autorizaciones o certificaciones, el cual será expedido por la Oficina de Gerencia de Permisos, o los municipios autónomos con jerarquía de la I a la III, conforme a la *Ley 161-2009*.

[4] Conforme a las declaraciones del secretario de Desarrollo Económico y Comercio del 3 de febrero de 2022, recientemente el Tribunal Supremo de Puerto Rico dio por terminada la controversia sobre dos casos relacionados con la validez del *Reglamento Conjunto*, versión del 2020, llevados ante su consideración por la Junta de Planificación. No obstante, el Tribunal Supremo todavía tiene ante su consideración una controversia jurisdiccional presentada por la OGPe. La adjudicación final de esta controversia sería la decisión final del caso y, por ende, la que sostendría la nulidad del *Reglamento Conjunto* o dejaría sin efecto las declaraciones del Tribunal de Apelaciones. Por tanto, se continúa la utilización del *Reglamento Conjunto*, hasta tanto el Tribunal Supremo adjudique el asunto jurisdiccional pendiente.

Los recursos para financiar las actividades administrativas, operacionales y funcionales del Departamento provienen de resoluciones conjuntas del Fondo General, asignaciones especiales de la Asamblea Legislativa, fondos especiales estatales, fondos federales e ingresos propios. El presupuesto consolidado estimado del Departamento, para los años fiscales 2018-19 al 2020-21, fue de $899,858,000, $1,010,889,000, y $1,115,384,000, respectivamente. En los años fiscales del 2018-19 al 2020-21, el presupuesto de la Secretaría Auxiliar para Salud Ambiental fue de $19,286,000, $17,257,000 y $31,988,000, respectivamente.

El **ANEJO 2** contiene la relación de los funcionarios principales del Departamento que actuaron durante el período auditado.

El Departamento cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.salud.gov.pr. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Mediante correos electrónicos del 17 de marzo de 2022, remitimos el borrador de este *Informe* para comentarios del Hon. Carlos Mellado López, secretario de Salud; y el borrador del **Hallazgo** de este *Informe* para comentarios de los doctores Lorenzo González Feliciano, Rafael Rodríguez Mercado y Ana C. Ríus Armendáriz, exsecretarios de Salud.

El secretario contestó el 11 de abril de 2022, en el **Hallazgo** se incluyeron algunos de sus comentarios.

Mediante correo electrónico del 18 de marzo de 2022, el doctor Rodríguez Mercado nos indicó lo siguiente:

> […] el contrato ya estaba en el departamento de salud ejecutandose desde el 2014. No estaba de secretario de salud al renovarse y al hacer la enmienda mencionada realizada mayo 2020. Fui secretario de salud del 2 de enero 2017 al 13 de marzo del 2020. [*sic*]

La doctora Ríus Armendáriz contestó mediante correo electrónico del 23 de marzo de 2022 y nos indicó lo siguiente:

> En torno al hallazgo correspondiente al periodo del 2014 al 2016 no tengo información para reaccionar, ya que al 31 de diciembre de 2016 cese en mis funciones como secretaria de Salud. De igual manera me acojo a las medidas correspondientes sometidas por el departamento de salud. [*sic*]

El doctor González Feliciano no contestó.

CONTROL INTERNO

La gerencia del Departamento es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de lo siguiente:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de este *Informe*. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno del Departamento.

En el **Hallazgo** se comentan las deficiencias de controles internos significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGO

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones del Departamento, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicable; y que dichos controles eran efectivos. Esto, excepto por el **Hallazgo**, que se comenta a continuación.

Falta de cláusulas en los contratos para proveer servicios de procesamiento, y de respaldos de las transacciones procesadas

a. Las agencias deben establecer medidas para lograr la recuperación de desastres y garantizar la continuidad de sus servicios de tecnología en la nube. Para esto, las agencias y los proveedores deben tener un entendimiento de sus roles y responsabilidades relacionadas con la implementación, la operación y el apoyo de esta solución tecnológica y establecer acuerdos de nivel de servicio en donde se establezcan los niveles de respuesta de los proveedores en caso de incidentes. Además, deben contar con un plan de migración en caso de que se determine cambiar de proveedor o instalar la solución en la infraestructura tecnológica dentro de la agencia, y asegurarse de que el contrato contenga cláusulas que establezcan de forma explícita que los datos son propiedad exclusiva del Estado Libre Asociado de Puerto Rico. Todos los servicios requeridos y contratados deben estar descritos detalladamente en el texto del contrato.

   La Oficina de Asesores Legales del Departamento es responsable, entre otras cosas, de redactar y formalizar los contratos, y asegurarse de que estos incluyan la información y las cláusulas requeridas por la reglamentación aplicable y necesaria para proteger los mejores intereses del Departamento.

Entre el 5 de mayo de 2014 y el 21 de mayo de 2020, el Departamento otorgó 2 contratos, 1 enmienda y 1 orden de servicio[5] a una compañía. Esto, para proveerle a la ciudadanía acceso a una plataforma digital[6] que, a la fecha de nuestra auditoría, era utilizada para procesar en línea[7] las solicitudes de inspección, las renovaciones de licencias y los permisos, las verificaciones y los endosos que otorgaba la Secretaría Auxiliar para Salud Ambiental. Además, mediante esta plataforma se emitían las facturas, se procesaban los pagos por concepto de los servicios solicitados y el cargo de procesamiento[8]; y se enviaban los correos electrónicos relacionados con estas transacciones. También, era utilizada para asignar inspectores, mantener la documentación digital de las inspecciones y procesar la autorización final; y para obtener informes de los servicios procesados, entre otros. Estos servicios debían estar disponibles 24 horas al día y 7 días a la semana.

El examen realizado el 17 de noviembre de 2020 de los dos contratos y la enmienda reveló que estos carecían de las cláusulas necesarias para garantizar, durante una emergencia, la continuidad de los servicios

[5] El primer contrato se otorgó el 5 de mayo de 2014 por $1.00 y con vigencia hasta el 30 de abril de 2019. El 30 de abril de 2019 se emitió una orden de servicio para extender la vigencia del 1 de mayo al 30 de septiembre de 2019 o hasta que se emitiera un nuevo contrato. El 21 de mayo de 2020 se otorgó el segundo contrato por $1.00, el cual fue enmendado el 29 de mayo de 2020 para extender su vigencia hasta el 30 de junio de 2021. El 30 de junio de 2021 se formalizó una segunda enmienda al contrato para extender los servicios del 1 de julio de 2021 al 30 junio de 2022.

[6] Esta plataforma digital también es utilizada para procesar servicios provistos por la Oficina de Sustancias Controladas, el Registro General Demográfico de Puerto Rico, y la Secretaría de Reglamentación y Acreditación de Facilidades de Salud del Departamento.

[7] Esta plataforma proveía servicios bajo una infraestructura de nube y aplicaciones que emplean lenguajes de programación apoyados por el proveedor.

[8] La compañía tenía derecho a cobrar una cantidad por cada transacción procesada mediante la plataforma. El cargo por servicio para todos los servicios de la Secretaría Auxiliar para Salud Ambiental, que fueran menor de $100, sería de $15. El cargo para los servicios que fueran mayor de $150 sería el 12% del valor de los servicios.

ofrecidos mediante la plataforma digital y proteger los intereses del Departamento. Entre las cláusulas que debieron incluir, están las siguientes:

- Las medidas para garantizar la continuidad de los servicios y la recuperación, en caso de desastres que afecten el funcionamiento de la plataforma digital y las instalaciones donde se procesan los datos.

- Los procedimientos para informar a la compañía los incidentes que afectan el servicio y obtener respuesta de esta.

- El requisito al proveedor de presentar los informes de las evaluaciones de seguridad, realizadas por una entidad competente, que evidencien la utilización de sistemas que protegen los datos, y una certificación de que cumple con los estándares actualizados de seguridad.

- El derecho de que los datos y su uso son propiedad exclusiva del Estado Libre Asociado de Puerto Rico.

b. Los datos e información que las agencias mantienen en los sistemas de información son vitales para la toma de decisiones y el desarrollo de estrategias que benefician los servicios ofrecidos por el gobierno. Los datos producidos y mantenidos en estos sistemas deben ser respaldados y mantenidos con una frecuencia que esté de acuerdo con la sensibilidad de los datos y el volumen de trabajo diario.

En la tercera cláusula, "Mantenimiento", del primer contrato mencionado en el **apartado a.**, se establece que la compañía se comprometía a brindarle al Departamento respaldos semanales de la base de datos del sistema e informes semanales o mensuales. Estas bases de datos eran solo para tenerlas como respaldo, y el Departamento no podía utilizarlas en algún programa que se asemejara o fuera igual al sistema creado por la compañía. En el segundo contrato dicha cláusula establecía que la compañía realizaría los respaldos

semanales de la base de datos del sistema, y proveería los informes semanales o mensuales, según le fueran solicitados por el Departamento.

Al 16 de julio de 2020, el ayudante especial de la Secretaría Auxiliar para Salud Ambiental nos informó que el Departamento no contaba con algún respaldo de la información procesada mediante la plataforma digital.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la sección Guías de la *Política TIG-017, Tecnologías en la Nube*, de la *Carta Circular 77-05* y la *Política ATI-012, Tecnologías en la Nube*, de la *Carta Circular 140-16*.

Lo comentado en el **apartado b.** es contrario a lo establecido en la tercera cláusula de los contratos; en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 77-05*; y en la *Política ATI-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 140-16*.

Efectos

Lo comentado en el **apartado a.** provocó que, ante la carencia de cláusulas de transición en la terminación del contrato que garantizaran la continuidad de los servicios, el Departamento quedara desprovisto de acceso a sus datos. El Departamento enfrentó una situación como esta durante la pandemia del COVID-19 cuando el contrato estaba vencido y la compañía desconectó de la plataforma los servicios relacionados con la Secretaría Auxiliar para Salud Ambiental. Además, el no contar con respaldos puede ocasionar que, en caso de emergencias, el Departamento no tenga disponible los respaldos de información necesarios para la continuidad de sus operaciones. **[Apartado b.]**

Causas

La situación comentada en el **apartado a.** se atribuye a que el personal de la Secretaría Auxiliar para Salud Ambiental no participó directamente en el proceso de la contratación, por lo que no pudieron incluir los aspectos

relacionados con la continuidad. Además, los abogados de la Oficina de Asesores Legales del Departamento no se aseguraron de que en los contratos evaluados se incluyeran las cláusulas relacionadas con la continuidad, conforme a lo establecido en las cartas circulares *77-05* y *140-16*.

La situación comentada en el **apartado b.** se atribuye a que, según informó el presidente de la compañía, el personal de la Secretaría Auxiliar para Salud Ambiental contaba con los privilegios de acceso para preparar los respaldos, y este no entregó los respaldos diarios y semanales que preparaba, debido a que el Departamento no se los solicitó. Obedece, además, a que el personal de la Secretaría Auxiliar para Salud Ambiental no procuró que se cumpliera con lo establecido en la tercera cláusula sobre la entrega de los respaldos semanales. También a que el personal no tenía conocimiento de cómo se realizaban los respaldos. Esto, según nos informó el ayudante especial de Salud Ambiental.

Comentarios de la Gerencia

El secretario informó que como parte de las medidas correctivas que implementarán durante el próximo año fiscal, enmendarán el contrato para que incluya cláusulas adicionales que requieran al contratista certificar que cuenta con un plan de contingencia, garantizar la confidencialidad de los datos, y proveer los respaldos de estos en una frecuencia y formato establecido. Además, incluirán una cláusula para establecer que los datos e información recopilada mediante la plataforma son propiedad del Departamento, y nos proveyó copia del *Independent Service Auditor's SOC 3 Report* del 2021, entre otros.

También informó que el 5 de abril de 2022, la secretaria auxiliar de Salud Ambiental, Laboratorios de Salud Pública y Bioseguridad solicitó al contratista que provea al personal un taller sobre el proceso para obtener los informes y respaldos del sistema.

Véanse las recomendaciones 1 y 2.

RECOMENDACIONES **Al secretario de Salud**

1. Asegurarse de que el gerente[9] de asesores legales, en coordinación con la secretaria auxiliar de la Secretaría Auxiliar para Salud Ambiental, cumpla con lo siguiente:

    a. Evalúe las cláusulas del contrato y vea que en la próxima enmienda se incluyan las cláusulas comentadas en el **apartado a.** Además, incluyan una cláusula que establezca que, en caso de cancelación del contrato, el contratista proveerá copia del respaldo completo más reciente de los datos procesados, sin contraseñas o cifrados que impidan el libre acceso al mismo, para garantizar la continuidad de los servicios.

    b. Se asegure de que en otros contratos que otorgue el Departamento para obtener servicios similares se incorporen estas cláusulas para garantizar la continuidad de los servicios y proteger los mejores intereses de este, conforme a lo establecido en las políticas *Carta Circular140-16*. **[Apartado a.]**

2. Asegurarse de que la secretaria auxiliar de la Secretaría Auxiliar para Salud Ambiental le requiera al contratista lo siguiente: **[Apartado b.]**

    a. Provea, en el término establecido, los respaldos de los datos procesados mediante la plataforma.

    b. Adiestre al personal designado sobre los procesos para acceder y grabar estos respaldos. Una vez adiestrados, se asegure de que los respaldos se graben periódicamente y se mantengan en un lugar seguro.

[9] En la contestación del secretario del 11 de abril de 2022, entre otras cosas, indica que hay nombrada una gerente de asesores legales, desde el 4 de octubre del 2021 hasta el presente.

APROBACIÓN

A los funcionarios y a los empleados del Departamento, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

ANEJO 1

DEPARTAMENTO DE SALUD
SECRETARÍA AUXILIAR PARA SALUD AMBIENTAL
Y LABORATORIO DE SALUD PÚBLICA

INFORMES PUBLICADOS

INFORME	FECHA	CONTENIDO DEL INFORME
TI-20-07	12 may. 20	Resultado del examen de los cambios a los sueldos de empleados regulares, y si estaban documentados, justificados y autorizados
TI-21-16	21 jun. 21	Resultado del examen de las políticas de cuentas de acceso y seguridad, en el dominio principal y los subdominios de la red del Departamento, las políticas de seguridad locales en los servidores principales donde están configurados estos dominios; y si se inactivan las cuentas de los exempleados

ANEJO 2

DEPARTAMENTO DE SALUD
SECRETARÍA AUXILIAR PARA SALUD AMBIENTAL
Y LABORATORIO DE SALUD PÚBLICA

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Lorenzo González Feliciano	Secretario	27 mar. 20	30 nov. 20
Dr. Rafael Rodríguez Mercado	"	1 ene. 17	26 mar. 20
Dra. Ana C. Ríus Armendáriz	Secretaria	5 may. 14	31 dic. 16
Dra. Iris Cardona Gerena	Subsecretaria	8 jun. 20	30 nov. 20
Dra. Concepción Quiñones de Longo	"	1 ene. 17	13 mar. 20[10]
Dr. Greduvel Durán Guzmán	Subsecretario	5 may. 14	31 dic. 16
Lcdo. Miguel Verdiales Morales	Asesor Legal	1 abr. 20	30 nov. 20
Lcdo. Raúl Bandas del Pilar	"	1 jul. 19	31 mar. 20
Lcdo. Michael Rey Delgado	"	1 ene. 17	30 jun. 19
Lcda. Mayra Maldonado Colón	Gerente de Asesores Legales	5 may. 14	31 dic. 16
Sra. Mayra Toro Tirado	Secretaria Auxiliar de Salud Ambiental, Laboratorios de Salud Pública y Bioseguridad[11]	1 ene. 17	30 nov. 20
Dr. Carlos M. Carazo Gilot	Secretario Auxiliar de Salud Ambiental, Laboratorios de Salud Pública y Bioseguridad	5 may. 14	31 dic. 16
Sra. Sonia N. Carrasquillo Cotto	Directora de Contratos	5 may. 14	30 nov. 20

[10] El puesto estuvo vacante del 14 de marzo al 7 de junio de 2020.

[11] La señora Toro Tirado ocupó el puesto de secretaria auxiliar de Salud Ambiental, Laboratorios de Salud Pública y Bioseguridad interina del 2 de septiembre al 30 de noviembre de 2020.

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-18-19* del 27 de abril de 2018, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensiones 2801 o 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos y el tipo de opinión del informe.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el administrador de documentos al (787) 754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: **TI-22-11** Número de unidad: **5290** Nombre de la entidad auditada: **DEPARTAMENTO DE SALUD-Secretaría Auxiliar para la Salud Ambiental y Laboratorio de Salud Pública**

Fecha del informe de auditoría o especial: **31 de mayo de 2022** Período auditado: **5 de mayo de 2014 al 30 de noviembre de 2020**

Indique el informe que remite: ☐ PAC ☐ ICP - _____ Indique si incluye anejo/s: ☒ Sí ☐ No

Funcionario de enlace: **Sra. Mayra Toro Tirado** Puesto: Secretaria Auxiliar Teléfono: (787) 765-2929 ext. 3211

Funcionario principal o su representante autorizado: **Dr. Carlos R. Mellado López** Puesto: Secretario de Salud Teléfono: (787) 765-2929 .

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 28 de septembre de 2022
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Incluir cláusula en el contrato especificando que los datos y su uso con propiedad exclusiva del ELA	Se incluyó en el contrato para el año fiscal 2022-2023 clausulas y/o acápites estableciendo que los datos y su uso son propiedad exclusiva del Departamento de Salud y que el contratista mantendrá confidencialidad de la información a la que por razón del servicio tendrá acceso.	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado
Incluir cláusula en el contrato estableciendo las medidas para garantizar la continuidad de los servicios en caso de desastre.	La cláusula de mantenimiento dispone que se realizarán respaldos ("back-ups") semanales sobre los datos e información obtenida de los usuarios, habida en la base de datos del sistema y a proveer la misma, en o antes del día viernes de cada semana, al Departamento de Salud. El formato para proveer la información se determinará por el DS. Las referidas bases de datos únicamente tendrán una función de apoyo y se utilizarán como respaldo ("back-up") de la totalidad de las transacciones realizadas en el Sitio Web. El contratista certifica que posee un plan de contingencia para asegurar la continuidad de los servicios en caso de emergencia o eventos de fuerza mayor. Copia del plan de hace formar parte del contrato.	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado
Incluir cláusula en el contrato con el procedimiento para informar a la compañía incidentes que afecten el servicio.	La cláusula de mantenimiento dispone sobre el procedimiento ante cualquier situación que impida el buen funcionamiento y acceso al Sitio Web- Se incluyó cláusula de notificación con los datos correspondientes para comunicación vía email o telefónica.	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: **TI-22-11** Número de unidad: **5290** Nombre de la entidad auditada: **DEPARTAMENTO DE SALUD-Secretaría Auxiliar para la Salud Ambiental y Laboratorio de Salud Pública**

Fecha del informe de auditoría o especial: **31 de mayo de 2022** Período auditado: **5 de mayo de 2014 al 30 de noviembre de 2020**

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Incluir cláusula en el contrato requiriendo al contratista certificar que cumple con los estándares actualizados de seguridad.	Se incluyeron en el contrato para el año fiscal 2022-2023 clausulas y/o acápites estableciendo requisitos sobre acceso, disponibilidad y entrega de informes, monitoreo en vivo de transacciones, todo compatible con el sistema de contabilidad del Departamento de Salud. La cláusula de mantenimiento dispone que la contratista es responsable del mantenimiento del Sitio Web y se obliga a mantenerlo disponible 24 horas al día, 7 días a la semana.	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado, Anejo 1
Incluir cláusula en el contrato requiriendo al contratista certificar que cumple con los estándares actualizados de seguridad.	Se incluyó en la cláusula de mantenimiento obligación del contratista a prestar los más altos estándares de seguridad en el Sito Web incluyendo contraseñas cifradas Todos los datos a utilizarse en el Sitio Web se almacenarán y transferirán en formado cifrado, haciendo uso del Protocolo de Capa de conexión segura ("Secure Sockets Layer", SSL), lo que a su vez proporcionará conexión segura al internet. El acceso al Sitio Web será a través de correo electrónico validado y contraseña	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado, Anejo 1
Incluir cláusula en el contrato atendiendo la copia final de respaldo en caso de terminación del contrato.	Se incluyeron en el contrato para el año fiscal 2022-2023 clausulas y/o acápites estableciendo la obligación del contratista para la eliminación de datos e información a tenor con las instrucciones a ser provistas por la Oficina de Informática del Departamento de Salud, en caso de terminación de contrato.	Oficina de Asesores Legales	Al otorgamiento del contrato	Completado, Anejo 1
Asegurarse que en otros contratos que otorgue el Departamento para obtener servicios similares se incorporen las cláusulas para garantizar la continuidad de los servicios	Se proveyeron instrucciones y recomendaciones a los asesores legales sobre disposiciones relacionadas a contratos de tecnología.	Oficina de Asesores Legales	Recurrente	Completado Anejo 2

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: **TI-22-11** Número de unidad: **5290** Nombre de la entidad auditada: **DEPARTAMENTO DE SALUD-Secretaría Auxiliar para la Salud Ambiental y Laboratorio de Salud Pública**

Fecha del informe de auditoría o especial: **31 de mayo de 2022** Período auditado: **5 de mayo de 2014 al 30 de noviembre de 2020**

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Asegurarse que la Secretaría Auxiliar de Salud Ambiental le requiera al contratista que provea en el término establecido los respaldos de los datos procesados mediante la plataforma	Se colocará un resguardo FULL a través de un SFTP en un servidor del Departamento de Salud.	Oficina de Informática del Departamento de Salud	Se incluye plan de trabajo	En proceso, Anejo 3
" "	Establecer requerimientos de solución (View/Read Only) para acceder a los datos de resguardo.	Oficina de Informática del Departamento de Salud	Se incluye plan de trabajo	En proceso, anejo 3
Adiestrar al personal designado sobre los procesos para acceder y realizar respaldos de información	Coordinar Taller de capacitación con proveedor y usuarios del Departamento de Salud	Secretaria Auxiliar de Salud Ambiental y Laboratorio de Salud Pública	Coordinado para 21 de septiembre de 2022	Pendiente de reprogramar por emergencia Huracán Fiona, Anejo 4

(Véanse instrucciones al final).

INSTRUCCIONES PARA COMPLETAR Y REMITIR EL PLAN DE ACCIÓN CORRECTIVA

Instrucciones:

1. Este documento debe estar completado en todas sus partes.

   a. La primera página debe contener, entre otra información: el número y la fecha del informe de auditoría o especial relacionado; indicación sobre el documento que se remite (*PAC* o *ICP*); el nombre del funcionario de enlace y del funcionario principal; y la firma del funcionario principal o su representante autorizado.

   b. En las columnas se requiere la siguiente información:

      1) **Recomendación**: En esta columna se detallan las recomendaciones. Las recomendaciones se presentan en el mismo orden y con el número de identificación que aparece en el informe de auditoría o especial.

      2) **Acción Correctiva**: En esta columna se indican las medidas adoptadas o las que adoptarán para corregir las situaciones señaladas y eliminar las causas de estas. Las acciones correctivas deben ser alcanzables y diseñadas para prevenir que las situaciones se repitan.

      3) **Persona o área responsable**: En esta columna se identifica/n el/los funcionario/s o el/las área/s responsable/s de implantar las acciones correctivas.

      4) **Fecha de implantación**: En esta columna se indica la fecha probable para cumplir con las acciones correctivas.

      5) **Estatus de la recomendación**: En esta columna se indica el nivel de cumplimiento de la recomendación. Esto es:

         - **Cumplimentada**: Recomendaciones para las cuales se tomaron acciones correctivas y se obtuvieron los resultados deseados.
         - **Parcialmente cumplimentada**: Recomendaciones para las cuales se han establecido medidas correctivas, pero quedan algunos asuntos pendientes.
         - **No cumplimentada**: Recomendaciones para las cuales no se han establecido acciones correctivas.

      En cada una de los columnas descritas en el apartado del **b.2) al 5)** de esta instrucción se deben ofrecer datos que permitan una evaluación adecuada. Si se objeta alguna recomendación, se deben incluir las razones y una descripción específica de la/s acción/nes correctiva/s alterna/s.

2. Cuando el funcionario principal delegue la función de certificar este documento, antes de remitir el mismo, debe notificar por escrito a la dirección de correo electrónico AdminPAC@ocpr.gov.pr el nombre y el puesto del funcionario en quien delegó la misma.

3. El documento digitalizado debe remitirse a la Oficina mediante la aplicación *Sistema Plan de Acción Correctiva* que esta creó para estos propósitos[1]. Esto, dentro del término de 90 días consecutivos, contados a partir del primer día del mes siguiente a la fecha de publicación del informe de auditoría o el especial. Cuando queden recomendaciones pendientes de cumplimentar, a la fecha del primer informe, se prepararán informes complementarios *(ICP)* cada 90 días, contados a partir del primer día del mes siguiente a la fecha de la notificación del resultado de la evaluación. El envío debe ser en la forma indicada anteriormente.

4. Los documentos que se utilicen para justificar las acciones correctivas informadas deben estar disponibles para examen por esta Oficina.

---

[1] La aplicación *Sistema Plan de Acción Correctiva* v1.0 está localizada en nuestra página en Internet: www.ocpr.gov.pr bajo la sección Contraloría Digital. Si no tiene una cuenta registrada en dicha aplicación envíe un correo electrónico a AdminPAC@ocpr.gov.pr para solicitar información de cómo registrar una cuenta en la misma.

2023-DS0212

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DE SALUD
SAN JUAN, PUERTO RICO

CONTRATO DE SERVICIOS PROFESIONALES

C O M P A R E C E N

DE LA PRIMERA PARTE: EL DEPARTAMENTO DE SALUD, representado por su Secretario de Salud, **CARLOS MELLADO LÓPEZ, MD,** mayor de edad, casado, médico de profesión y vecino de San Juan, Puerto Rico, o por el Subsecretario de Salud, **FÉLIX RODRÍGUEZ SCHMIDT, MD,** mayor de edad, casado, médico de profesión y vecino de Caguas, Puerto Rico, o por el Principal Oficial Administrativo del Departamento, **ESDRAS VÉLEZ RODRÍGUEZ,** mayor de edad, casado, abogado de profesión y vecino de Guaynabo, Puerto Rico, quienes comparecen en representación del Secretario de Salud y están autorizados a firmar este Contrato en virtud de la delegación hecha por el Secretario en comunicación con fecha de 16 de marzo de 2021, de conformidad con la Ley Núm. 81 de 14 de marzo de 1912, según enmendada, en adelante denominada la **PRIMERA PARTE**

DE LA SEGUNDA PARTE: **TECSECURE, INC.** una corporación creada al amparo de las Leyes del Estado de Libre Asociado de Puerto Rico, representada por **MANUEL GUERRA-MONDRAGÓN** en calidad de presidente mayor de edad, casado y vecino de San Juan, Puerto Rico, en adelante denominada la **SEGUNDA PARTE.**

EXPONEN

POR CUANTO: La **PRIMERA PARTE** brinda servicios directos a la ciudadanía e interesa utilizar la plataforma privada y propiedad de la **SEGUNDA PARTE** bajo los conceptos Platform as a Service (PaaS) a través de su sitio web renovacionesonline.com (en adelante Sitio Web) para el procesamiento de solicitudes y/o renovación de permisos, certificaciones, licencias y/o servicios que la **PRIMERA PARTE** está facultada a expedir bajo las leyes y reglamentos que administra.

POR CUANTO: A tenor con la Ley Núm.81 de 14 de marzo de 1912, según enmendada, el Memorando Circular Número 07-93, emitido el 8 de marzo de 1993 y el Boletín Administrativo Núm. OE-1991-24, emitido el 18 de junio de 1991, según enmendado por el Boletín Administrativo Núm. OE-1992-52 de 28 de agosto de 1992, **AMBAS PARTES** convienen en efectuar este contrato, con arreglo a las siguientes:

CLÁUSULAS Y CONDICIONES

PRIMERA: **SERVICIOS:** La **SEGUNDA PARTE,** a través del personal que para ello contrate, prestará los Servicios Profesionales que se enumeran y describen a continuación:

1. Concederá, a la **PRIMERA PARTE**, una licencia de uso limitada, no exclusiva, revocable y no transferible sobre el software utilizado en el Sitio Web para que la **PRIMERA PARTE** pueda expedir y renovar permisos, certificaciones y licencias

2. Proveer acceso online veinticuatro (24) horas al día, siete (7) días a ala semana, mediante el Sitio Web para el procesamiento de solicitudes y/o renovación de permisos, certificaciones, licencias y/o servicios a las siguientes unidades operacionales de la **PRIMERA PARTE**:

    a. Secretarías de Salud Ambiental (SASA);

    b. Registro Demográfico;

    c. Secretaría Auxiliar de Reglamentación y Acreditación de Facilidades de Salud (SARAF), incluyendo:
        i. División de Medicamentos y Farmacia
        ii. División de Certificados de Necesidad y Conveniencia
        iii. División de Instituciones de Salud
        iv. División de Laboratorios

Anejo 1

v. División de Certificados de Salud y Artistas Dermatógrafos.
vi. División de Investigaciones.

3. Brindar a la **PRIMERA PARTE** acceso a solicitudes y renovaciones de permisos, certificaciones y licencias, a través del Sitio Web.

4. Brindar a la **PRIMERA PARTE** acceso del recaudo y de la contabilización y datos financieros de todos los ingresos que pertenecen a la **PRIMERA PARTE** generados mediante el Sitio Web, incluyendo los recaudos por la presentación de solicitudes, por el otorgamiento de permisos, certificaciones y licencias, multas y por cualquier otra venta efectuada mediante el Sitio Web.

5. La **SEGUNDA PARTE** proveerá a la **PRIMERA PARTE** reportes a través del Sitio Web incluyendo la cantidad de solicitudes presentadas, ventas realizadas y permisos, certificaciones y licencias emitidas. Los datos mencionados que permita generar reportes confiables que cuantifiquen cantidades relacionadas a las transacciones efectuadas en el Sitio Web para determinados periodos de tiempo.

6. La **SEGUNDA PARTE** proveerá el equipo electrónico necesario: tabletas, scanner, computadoras, impresoras, etc., para facilitar el acceso del personal de la **PRIMERA PARTE**, así como la conexión a internet necesaria para que los empleados puedan acceder al Sitio Web.

SEGUNDA: SERVICIOS INTERAGENCIALES: Ambas partes contratantes reconocen y acceden a que lo servicios contratados podrán ser brindados a cualquier entidad de la Rama Ejecutiva con la cual la entidad contratante realice un acuerdo interagencial o por disposición directa de la Secretaría de la Gobernación. Estos servicios se realizan bajo los mismos términos y condiciones en cuanto a horas de trabajo y compensación consignados en este contrato. Para efectos de esta cláusula, el término "entidad de la Rama Ejecutiva" incluye a todas las agencias del Gobierno de Puerto Rico, así como a las instrumentalidades y corporaciones públicas y a la Oficina el Gobernador.

TERCERA: CARGO POR SERVICIO: La **SEGUNDA PARTE** tendrá derecho a cobrar una cantidad "processing fee" por cada transacción que se realice a través del Sitio Web. Dicha cantidad será fija para todos los servicios, de la siguiente forma:

Secretaría u Oficina	Monto de la Transacción	Cargo de Procesamiento	Monto de la Transacción	Cargo de Procesamiento
Registro Demográfico	$0.01- $41.67	$5.00	$41.68 >	$12% p/t
Salud Ambiental	$0.01-$125.00	$15.00	$125.00>	$12% p/t
SARAF	$0.01-$84.00	$8.00	$84.00 >	9.5% p/t
SARAF-Certificados de Salud	---	$3.00	---	---
SARAF-Sustancias Controladas	$0.01- $84.00	$12.00	$84.00>	9.5% p/t

El costo del servicio, determinado por la **PRIMERA PARTE**, será depositada en una cuenta bancaria que llevará el nombre de la **PRIMERA PARTE**, cada Secretaría tiene su cuenta con la correspondiente descripción. Será responsabilidad de la **PRIMERA PARTE** crear dicha cuenta bancaria y su reconciliación contable. Una segunda transacción, identificada como pago por transacción será depositada en una cuenta bancaria a nombre la de la **SEGUNDA PARTE** y será responsabilidad de esta parte su reconciliación.

La **SEGUNDA PARTE** se compromete a que la **PRIMERA PARTE**, recibirá de forma íntegra, el valor de los servicios descritos en el presente contrato, y según establecidos por ésta en sus reglamentos vigentes a la fecha de la firma de este acuerdo, y serán depositados en la cuenta bancaria que se determine a estos efectos. La **SEGUNDA PARTE** asume los gastos operacionales de las transacciones y/o cualquier otro cargo bancario producto de los pagos realizados por tarjetas de crédito. Todo cargo que se haga a la cuenta del Secretario de Hacienda debe ser reembolsado por la **SEGUNDA PARTE.**

La **SEGUNDA PARTE** se compromete a dar acceso a la **PRIMERA PARTE** para que pueda ver sus transacciones a través de su propio sistema de pago y una entidad cuyo propósito es procesar los

pagos ("Sistema de pago electrónico"). La **PRIMERA PARTE** acepta que la **SEGUNDA PARTE** será la única con facultad para escoger la entidad que fungirá como el sistema de pago electrónico.

La **PRIMERA PARTE** evaluará el funcionamiento del sistema y los servicios provistos por la **SEGUNDA PARTE**. La **SEGUNDA PARTE** proveerá los reportes directamente del sitio web y de no estar disponible se crearán dichos reportes para una evaluación completa y oportuna del funcionamiento de los servicios. La **PRIMERA PARTE** tendrá acceso a través del Sitio Web a toda la información relacionada a la contabilidad de las transacciones de los pagos realizados y a toda la información relacionada a la contabilidad de las transacciones depositadas a favor de la **PRIMERA PARTE**. Mediante el sistema de pago del Sitio Web se podrán monitoreara en vivo todas las transacciones, además d, el sistema de pago tendrá la capacidad de crear múltiples reportes y archivos para que sean compatibles al sistema de contabilidad de la **PRIMERA PARTE**.

CUARTA: COMPENSACIÓN. La **PRIMERA PARTE** se obliga a pagar a la **SEGUNDA PARTE**, a cambio de las licencias de uso y servicios prestados, bajo los términos y condiciones del presente contrato, la cantidad de un dólar ($1.00) al año.

Este contrato será administrado por **SECRETARIO DE SALUD o su REPRESENTANTE AUTORIZADO** y será evaluado para medir resultados obtenidos conforme a la necesidad del servicio.

QUINTA: RECURSOS PARA PAGAR LOS SERVICIOS: Los servicios prestados bajo este contrato se pagarán de la cifra de cuenta **234-0710000-081-2021 (PRIFAS); E1290-234-0710170-006-2021 (8.4)** y/o cualquier otra cifra de cuenta disponible, hasta un máximo de **UN DÓLAR ($1.00)** durante la vigencia del contrato.

SEXTA: PROPIEDAD INTELECTUAL: Queda expresamente convenido que los datos e información recopilada por la **SEGUNDA PARTE** con relación a los usuarios, sus peticiones o solicitudes, incluyendo la información provista por el usuario para el trámite será propiedad única y exclusivamente de la **PRIMERA PARTE**. Queda, además, expresamente convenido que la **PRIMERA PARTE** tiene pleno derecho para dar a dicha información el uso oficial que estime conveniente. La **SEGUNDA PARTE** deberá guardar y proteger la información que obtenga como parte de los servicios objeto del presente contrato y producir los mismos o dar acceso a la **PRIMERA PARTE** a petición de ésta durante el mismo período de vigencia de este acuerdo.

Una vez terminado el acuerdo entre las partes, la **SEGUNDA PARTE** procederá a eliminar los datos e información recopilada de la **PRIMERA PARTE y sus usuarios** utilizando el método e instrucciones a ser provistas por la Oficina de Informática y Avances Tecnológicos de la **PRIMERA PARTE**.

El software está protegido por la Ley de Derechos de Autor de los Estados Unidos. Las partes acuerdan que, la **SEGUNDA PARTE** ya tiene creado el sistema desde mucho antes de la otorgación de dicho contrato y posee todos los derechos aplicables sobre el software, incluyendo, pero no limitado a: derechos de autor y cualquier otro derecho de propiedad intelectual aplicable; derechos de comercialización, alquiler o venta del software o cualquier parte de este; derechos de hacer obras derivadas del software; y todos los derechos para distribuir el software y copias de este. Este acuerdo no otorga a la **PRIMERA PARTE** ningún derecho de propiedad sobre el software ni sobre base de datos ya existente y de ninguna marca de bienes o servicios perteneciente a la **SEGUNDA PARTE**. Mediante la ejecución de este contrato y el pago de la cantidad indicada en la cláusula Quinta, la **PRIMERA PARTE** obtiene un permiso limitado para utilizar el software tal como se expone en la Cláusula Tercera del presente contrato. Cualquier otro uso del software por cualquier persona, negocio, empresa, gobierno, organización o cualquier otra entidad está estrictamente prohibido y es una violación de este contrato. De ocurrir tal violación la **SEGUNDA PARTE** automáticamente apagará la plataforma y notificará a la **PRIMERA PARTE** la incidencia detectada. La **SEGUNDA PARTE** estará actualizando su sistema de seguridad para poder identificar terceros que su intención de navegación a través de este sea sospechosa.

SÉPTIMA: MANTENIMIENTO: AMBAS PARTES acuerdan que la **SEGUNDA PARTE** será la única encargada y responsable del mantenimiento y administración del Sitio Web. La **SEGUNDA PARTE** se obliga a que el Sitio Web se encuentre disponible y funcione adecuadamente las veinticuatro horas (24) del día, los siete (7) días de la semana.

Cualquier situación o evento que ocasione o impida el buen funcionamiento y acceso ordinario al Sitio Web, la **SEGUNDA PARTE** deberá notificar inmediatamente por escrito mediante entrega personal o correo electrónico de acuerdo con la cláusula de notificación, a todas las divisiones correspondientes de la **PRIMERA PARTE**, el estatus del Sitio Web, las limitaciones a los servicios existentes, gestiones realizadas para reestablecer los servicios completos y un estimado del tiempo requerido para resolver la situación.

La **SEGUNDA PARTE** se obliga, además, a brindar los más altos estándares de seguridad en el Sitio Web, incluyendo contraseñas cifradas.

EVR

La **SEGUNDA PARTE** se compromete además a lo siguiente:

1. Todos los datos a utilizarse en el Sitio Web se almacenarán y transferirán en formado cifrado, haciendo uso del Protocolo de Capa de conexión segura ("Secure Sockets Layer", SSL), lo que a su vez proporcionará conexión segura al internet.

2. El acceso al Sitio Web será a través de correo electrónico validado y contraseña.

3. A realizar respaldos ("*back-ups*") semanales sobre los datos e información obtenida de los usuarios, habida en la base de datos del sistema y a proveer la misma, en o antes del día viernes de cada semana, a la **PRIMERA PARTE**. El formato para proveer la información se determinará. Las referidas bases de datos únicamente tendrán una función de apoyo y se utilizarán como respaldo ("*back-up*") de la totalidad de las transacciones realizadas en el Sitio Web.

4. d. La **SEGUNDA PARTE** certifica que posee un plan de contingencia para asegurar la continuidad de los servicios en casos de emergencias o eventos de fuerza mayor Copia del mismo formará parte del presente contrato, como **ANEJO I.**

La **SEGUNDA PARTE** proveerá acceso inmediato e ininterrumpido a toda la información de reportes relacionados a todas las solicitudes de la ciudadanía o empresas a la **PRIMERA PARTE**.

La **SEGUNDA PARTE** será la única responsable del mantenimiento y reemplazo del equipo utilizado para la conexión al Sitio Web y del equipo que en este momento tiene la **PRIMERA PARTE**.

La **SEGUNDA PARTE** tiene el conocimiento y ha puesto a la disposición de la **PRIMERA PARTE** la infraestructura necesaria para que las oficinas locales obtengan el equipo necesario para que ésta pueda prestar el servicio. La **SEGUNDA PARTE** proveerá equipo adicional, según la necesidad de la **PRIMERA PARTE** o el reemplazo del equipo que se encuentre dañado o en mal funcionamiento.

Será responsabilidad de la **PRIMERA PARTE** responder a la **SEGUNDA PARTE,** en el término de cinco (5) días calendario, cualquier requerimiento de información o cambio, relacionado a los términos objeto del presente contrato. Cualquier solicitud de cambio, que suponga una enmienda a los servicios aquí descritos, deberá realizarse mediante la enmienda correspondiente.

La **SEGUNDA PARTE** presentará copia de los siguientes documentos que formarán parte del expediente del contrato:

1. Informe SOC ("Service Organization Control") nivel 2
2. Certificación ISO 27001

OCTAVA: **USOS PROHIBIDOS DEL SOFTWARE:** La **PRIMERA PARTE** se compromete a:

1. No usar el software de manera tal que violente los términos y condiciones de este contrato.
2. No copiar el software.
3. No permitir que un tercero, ajeno a los propósitos de este contrato, pueda tener acceso al sistema.
4. No adaptar ni modificar el software, ni mezclarlo con otro programa de computadoras.
5. No llevar a cabo ingeniería inversa del software, ni tampoco desmontar, descompilar o realizar cualquier intento para descubrir el código fuente del software.
6. No borrar marcas, símbolos de derechos de autor o cualquier otro símbolo que indique el interés propietario de la **SEGUNDA PARTE** sobre el software.
7. No colocar el software en algún servidor que lo convierta en software público.
8. No sub-licenciar, rentar, prestar o transferir el software.
9. No dar acceso a terceros no autorizados por la **SEGUNDA PARTE** a utilizar el software.
10. No crear una obra derivada del software.
11. No podrá permitir acceso a ningún tercero, que no sea funcionario o empleado de ésta al sistema o software.
12. No remover el software de una computadora sin la autorización de la **SEGUNDA PARTE.**

NOVENA: **CONTRATISTA INDEPENDIENTE. AMBAS PARTES** libre y voluntariamente acuerdan que bajo los términos de este contrato no se están estableciendo relaciones de patrono y empleado entre éstas y que la **SEGUNDA PARTE** actuará y prestará servicios en todo momento como contratista independiente y convienen que ninguno de los miembros de ésta, así como los que trabajen para ésta, reclamará a la **PRIMERA PARTE** por concepto de vacaciones, licencia por enfermedad, retiro, bono de navidad, póliza de responsabilidad profesional, ni Seguro Social Federal.

A la **SEGUNDA PARTE** no se le efectuarán retenciones ni descuentos de sus honorarios para el pago del Seguro Social Federal. La **PRIMERA PARTE** podrá retener del pago debido a la **SEGUNDA PARTE** por servicios prestados hasta el 10% que dispone la Ley Núm. 257 del año 2018 para enmendar la Sección 1062.3 del Código de Rentas Internas (2011), según enmendada, de conformidad con los reglamentos aprobados por el Secretario de Hacienda. En el caso de los relevos parciales que dispone el apartado (g) de la Sección 1062.03 del Código, las enmiendas introducidas por la Ley 257-2018 establecen que la retención aplicable será de 6% por ciento.

La **SEGUNDA PARTE** se obliga, como condición necesaria a este contrato, a presentar las certificaciones, relevos y documentos que acrediten su situación contributiva, que sean requeridos por la **PRIMERA PARTE** o su representante autorizado.

La **SEGUNDA PARTE** es responsable de rendir sus planillas y pagar las aportaciones correspondientes, al Seguro Social Federal y al Negociado de Contribución Sobre Ingresos del Departamento de Hacienda, por cualquier cantidad tributable como resultado de los ingresos devengados bajo este contrato. La **PRIMERA PARTE** notificará al Negociado de Contribución Sobre Ingresos los pagos y reembolsos que sean efectuados a la **SEGUNDA PARTE.**

La **SEGUNDA PARTE** será responsable de asegurar con el Fondo del Seguro del Estado a sus empleados y a todo el personal que preste servicios bajo este contrato.

DÉCIMA: **INFORMES:** La **SEGUNDA PARTE** vendrá obligada a rendir cuantos informes.le solicite la **PRIMERA PARTE** o su representante autorizado, sobre el servicio que se compromete a prestar y los deberes que se compromete a cumplir, en virtud de este contrato.

DÉCIMA PRIMERA: **NEGLIGENCIA O ABANDONO:** El desempeño negligente de sus funciones o el abandono de éstas por la **SEGUNDA PARTE** se considerará una violación a este contrato y será causa suficiente para que la **PRIMERA PARTE** lo declare terminado inmediatamente, sin sujeción a la Cláusula de Resolución y quede relevada de toda obligación y responsabilidad bajo el mismo. Queda expresamente convenido que la **SEGUNDA PARTE** completará cualquier trabajo que quede pendiente al momento de la resolución, sin que por ello la **PRIMERA PARTE** venga obligada a pagar a la **SEGUNDA PARTE** retribución o compensación adicional sobre el mismo.

DÉCIMA SEGUNDA: **DISCRIMEN EN LA PRESTACION DE LOS SERVICIOS.** La **SEGUNDA PARTE** se compromete a no discriminar en la prestación de estos servicios por razones de índole política, religiosa, de raza, condición social, sexo, edad, nacionalidad, condición o impedimento físico o mental o por orientación sexual o identidad de género.

DÉCIMA TERCERA: **VIGENCIA Y DURACION.** Este contrato entrará en vigor a partir de la firma de la **PRIMERA PARTE,** no obstante, la **SEGUNDA PARTE** comenzará a prestar servicios a partir de la orden de comienzo, que nunca será antes de la firma de la **PRIMERA PARTE** y estará vigente hasta el **30 DE JUNIO DE 2023** y podrá ser renovado durante períodos adicionales, previa enmienda escrita a esos efectos, firmada por **AMBAS PARTES**.

DÉCIMA CUARTA: **RESOLUCIÓN.** Este contrato podrá ser resuelto antes de su vencimiento, por cualquiera de **AMBAS PARTES**, mediante notificación escrita a la **OTRA PARTE**, con treinta (30) días de antelación a la fecha de resolución deseada, sin que por ello incurran las **PARTES** entre sí en obligación alguna.

La insuficiencia de fondos será causa suficiente para la terminación inmediata o modificación en la cláusula de Compensación de este contrato.

Serán causas suficientes para que la **PRIMERA PARTE** declare el contrato terminado inmediatamente, por la infracción o incumplimiento por la **SEGUNDA PARTE** a las siguientes condiciones y la **PRIMERA PARTE** queda relevada de toda obligación y responsabilidad bajo el mismo:

1. La infracción o infracciones por la **SEGUNDA PARTE** a la Ley Núm. 1 de 3 de enero de 2012, según enmendada, conocida como Ley de Ética Gubernamental de Puerto Rico.

2. El desempeño negligente por la **SEGUNDA PARTE** de sus funciones o por el abandono de éstas.

3. El incumplimiento por la **SEGUNDA PARTE** de los Reglamentos y Procedimientos establecidos por la **PRIMERA PARTE.**

4. La convicción o determinación de causa probable para arresto contra la **SEGUNDA PARTE** por la comisión de algún delito contra el erario, la fe o la función pública; contra el ejercicio gubernamental; o que involucre fondos o propiedad pública, en el ámbito federal o estatal.

5. De la **SEGUNDA PARTE** incurrir en actos que van en contravención con legislación de Política Pública, tales como, Hostigamiento Sexual, Hostigamiento Laboral) Ley Núm.90-2020), Discrimen y Uso y Abuso de Sustancias Controladas.

6. En caso de que la **SEGUNDA PARTE** haya sido acusada, administrativa o criminalmente, o convicta de haber obtenido fraudulentamente cualquier credencial.

7. Si la **SEGUNDA PARTE** queda desprovista de su licencia profesional durante la vigencia del contrato o de no mantener su licencia profesional vigente.

8. Quedar desprovisto de la Licencia Estatal y Federal para la prescripción de Drogas y Narcóticos durante la vigencia de este contrato.

9. La cancelación o modificación de cualquiera de las pólizas requeridas a la **SEGUNDA PART** bajo este contrato.

10. La **PRIMERA PARTE** podrá terminar inmediatamente este contrato si en su total y única discreción determina que la **SEGUNDA PARTE** ha incurrido en una violación de los acuerdos de privacidad, confidencialidad y seguridad en cuanto al uso y divulgación de la información de salud protegida de los pacientes de la **PRIMERA PARTE.** Será causa de terminación contractual la falta de notificación a la **PRIMERA PARTE** de cualquier violación al manejo de la Información de Salud Protegida (Protected Health Information PHI por sus siglas en inglés) por parte de la **SEGUNDA PARTE**, sus asociados y/o sub-contratistas. La **PRIMERA PARTE** se reserva el derecho de referir al Departamento de

Salud y Servicios Humanos Federal sobre violaciones no subsanadas de la **SEGUNDA PARTE.**

11. El incumplimiento con las credenciales profesionales necesarias para ejercer las funciones para las que se le contrata, expedidas por la Junta Acreditadora correspondiente.

12. El incumplimiento con cualquier cláusula del contrato será causa suficiente para la terminación inmediata del mismo.

EVR

13. La secretaria de la Gobernación tendrá la facultad para dar por terminado el presente contrato en cualquier momento.

14. El incumplimiento con las políticas establecidas por la Junta de Supervisión y Administración Financiera respecto a la contratación con el Gobierno de Puerto Rico y sus instrumentalidades, aplicables a la **SEGUNDA PARTE.** (POLÍTICA DE LA JSAF: REVISIÓN DE CONTRATOS de 6 de noviembre de 2017, modificada el 30 de abril de 2021).

15. El incumplimiento con las disposiciones de la Orden Ejecutiva OE2021-029 de 27 de abril de 2021 o cualquier enmienda subsiguiente a la misma cuando sea de aplicabilidad.

Queda expresamente convenido que la **SEGUNDA PARTE** completará cualquier trabajo que quede pendiente al momento de la resolución, sin que por ello la **PRIMERA PARTE** venga obligada a pagar a la **SEGUNDA PARTE** retribución o compensación adicional sobre el mismo. Al momento de la resolución la **SEGUNDA PARTE** preparará y entregará a la **PRIMERA PARTE** un respaldo ("back up") que incluya toda la información pendiente al momento de la terminación, incluyendo las todas transacciones solicitadas y no completadas a esa fecha. Una vez entregado el respaldo la **SEGUNDA PARTE** procederá con la eliminación de los datos conforme dispuesto en la cláusula titulada **MANTENIMIENTO.**

DECIMA QUINTA: <u>INTERES PECUNIARIO</u>:

_____La **SEGUNDA PARTE** hace constar que a su mejor conocimiento **ningún** funcionario o empleado de la **PRIMERA PARTE** o algún miembro de su unidad familiar tienen directa o indirectamente interés pecuniario en este contrato.

_____La **SEGUNDA PARTE** hace constar que a su mejor conocimiento **ningún** funcionario o empleado de la **PRIMERA PARTE** ha tenido durante los últimos dos (2) años antes de ocupar su cargo, directa o indirectamente interés pecuniario en este contrato.

_____La **SEGUNDA PARTE** certifica que a su mejor conocimiento ninguno de sus socios, oficiales, directores o empleados **NO** tiene relación de parentesco, con **ningún** funcionario o empleado que tenga facultad de decidir o influenciar y participar en las decisiones institucionales de la **PRIMERA PARTE.**

NA____La **SEGUNDA PARTE** certifica que alguno de sus oficiales, directores o empleados **tiene** relación de parentesco con un funcionario o empleado de la **PRIMERA PARTE** y que se le otorgó Dispensa de la Oficina de Ética Gubernamental. La **SEGUNDA PARTE** se obliga, a indicar la relación de parentesco, nombre y lugar de trabajo, del funcionario o empleado, según queda expresamente establecido en la certificación. Copia de la certificación y de la dispensa se hacen formar parte del expediente del contrato.

La **PRIMERA PARTE** certifica que, a su mejor entender, ningún empleado o funcionario de esta agencia o algún miembro de su unidad familiar tiene, directa o indirectamente, interés pecuniario en este contrato y que ningún funcionario o empleado de la Rama Ejecutiva tiene interés en las ganancias o beneficios producto de este contrato.

DECIMA SEXTA: INTERPRETACIÓN: Este contrato estará sujeto en todo momento a las Leyes y Reglamentos del Estado Libre Asociado de Puerto Rico y será interpretado de acuerdo a los mismos. Si cualquiera de las cláusulas, párrafos, oraciones, palabras o partes de este contrato es declarado nulo o inconstitucional por un Tribunal de Justicia, el resto de las cláusulas, párrafos, oraciones, palabras o partes de este contrato continuarán en efecto para asegurar la intención de las partes contratantes, pudiendo ser interpretados de acuerdo a las provisiones aplicables del Código Civil de Puerto Rico y las leyes que gobiernan la contratación del Gobierno de Puerto Rico.

DECIMA SÉPTIMA: INTRANSFERIBILIDAD: Los servicios que prestará la SEGUNDA **PARTE** no pueden ser transferidos, sin previa notificación y acuerdo con la **PRIMERA PARTE.** La delegación de éstos, sin previa notificación y acuerdo con la **PRIMERA PARTE** será causa suficiente para dar por terminado inmediatamente este contrato. El incumplimiento de esta cláusula hará responsable a la **SEGUNDA PARTE** por cualesquiera daños y perjuicios que fueran causados a la **PRIMERA PARTE**, ya sean éstos en forma directa o indirecta.

EVR

DECIMA OCTAVA: RESPONSABILIDAD POR DAÑOS Y PERJUICIOS: La **SEGUNDA PARTE** será responsable por cualesquiera daños y perjuicios causados por el desempeño negligente o el abandono de las obligaciones asumidas bajo este contrato y releva así de cualquier obligación y responsabilidad a la **PRIMERA PARTE.**

DECIMA NOVENA: POLITICA ADMINISTRATIVA: Convienen las **PARTES** que la **SEGUNDA PARTE** no podrá alterar los procedimientos establecidos o tomar decisiones que afecten sustancialmente la Política Administrativa establecida por la **PRIMERA PARTE,** sin el previo consentimiento por escrito de ésta.

VIGÉSIMA: EX-SERVIDORES PUBLICOS:

_____ La **SEGUNDA PARTE** certifica que, a su mejor conocimiento, ninguno de sus socios, oficiales o directores ha sido servidor público.

NA La **SEGUNDA PARTE** certifica que han transcurrido más de dos (2) años desde el cese de las funciones como servidor público de alguno de sus socios, oficiales o directores, y que no ha ofrecido información, intervenido, cooperado, asesorado en forma alguna o representado directa o indirectamente a persona privada, negocio o entidad pública, ante la agencia para la que laboró, ésta de conformidad con la sección 4.6 de la Ley de Ética Gubernamental, Ley Número 1 de 3 de enero de 2012.

NA La **SEGUNDA PARTE** certifica que no han transcurrido más de dos (2) años desde el cese de las funciones como servidor público de alguno de sus socios, oficiales o directores, y/o uno o más de sus socios, oficiales o directores y continúa en funciones como servidor público. No obstante presta servicios de salud de conformidad con el Código Político de 1902, según enmendado, Artículo 177 (3 L.P.R.A. §551) el cual exime a los médicos, dentistas, farmacéuticos, asistentes dentales, enfermeras, practicantes, técnicos de rayos-x y personal de laboratorio de la prohibición de doble compensación para aquellos que hayan sido servidores públicos con cualquiera de las instrumentalidades del Estado Libre Asociado de Puerto Rico o municipio.

NA La **SEGUNDA PARTE** certifica que no han transcurrido más de dos (2) años desde el cese de las funciones de alguno de sus socios, oficiales o directores como servidores públicos, no obstante presta servicios *ad honorem* de conformidad con la sección 4.6 de la Ley de Ética Gubernamental, Ley Núm. 1 del 3 de enero de 2012.

NA La **SEGUNDA PARTE** certifica que alguno de sus socios, oficiales o directores, ha sido servidor público con la **PRIMERA PARTE** y no han transcurrido más de dos (2) años desde el cese de sus funciones.

Cuando medien circunstancias excepcionales y a discreción de la Oficina de Ética Gubernamental podrá expedir dispensa, siempre que resulte en beneficio del servicio público la contratación dentro de los dos (2) años del ex-servidor público.

VIGÉSIMA PRIMERA: AUDITORIAS: La **SEGUNDA PARTE** se compromete a viabilizar las auditorías que la **PRIMERA PARTE** o la Oficina del Contralor de Puerto Rico consideren necesarios, por lo cual deberán:

1. Mantener disponible para examen o inspección, en cualquier momento por la **PRIMERA PARTE** o la Oficina del Contralor de Puerto Rico, todos los expedientes, documentos, libros y datos relacionados con los asuntos objeto de este contrato.

2. Retener todos los expedientes o cualquier documento pertinente a este contrato, por un período de seis (6) años luego de terminado el mismo. De haberse iniciado una auditoría cuyos resultados no se hubieran solucionados al finalizar los seis (6) años, los expedientes deberán ser retenidos hasta que se emitan los resultados de la auditoría.

VIGESIMA SEGUNDA: DELITOS CONTRA EL ERARIO PÚBLICO: La SEGUNDA PARTE certifica que ni ella, ni ninguno de sus accionistas, socios, oficiales, principales, empleados, subsidiarias o compañías matrices ha sido convicto, ni se ha encontrado causa probable para su arresto, por ningún delito contra el erario, la fe o la función pública; contra el ejercicio gubernamental; o que involucre fondos o propiedad pública, en el ámbito federal o estatal.

La SEGUNDA PARTE reconoce su deber continuo de informar, durante la vigencia del contrato, cualquier hecho que se relacione con la conducción de cualquier investigación por la comisión de un delito contra el erario, la fe o con la función pública; contra el ejercicio gubernamental; que involucre fondos o propiedad pública, en el ámbito federal o estatal.

La **SEGUNDA PARTE** reconoce su deber continuo de informar si ella, y/o alguno de sus accionistas, socios, oficiales, principales, empleados, subsidiarias o compañías matrices ha sido convicto, o encontrada causa probable para su arresto, por delitos contra el erario, la fe o la función pública; contra el ejercicio gubernamental; o que involucre fondos o propiedad pública, en el ámbito federal o estatal.

VIGESIMA TERCERA: CERTIFICACIÓN CONTRIBUTIVA:

_____ La **SEGUNDA PARTE** certifica y garantiza que al momento de suscribir este contrato ha rendido su planilla contributiva durante los cinco (5) años previos a este contrato y no adeuda contribuciones al Gobierno de Puerto Rico. También certifica que no tiene deuda contributiva alguna, entendiéndose por deuda contributiva, cualquier deuda por concepto de contribución sobre ingresos, arbitrios, contribución sobre la propiedad mueble e inmueble, incluyendo cualquier imposición de carácter especial, derechos de licencias, contribuciones retenidas en el origen en el pago de salarios a empleados, en el pago de intereses, dividendos, rentas, salarios y otros emolumentos a individuos o por cualquier otro concepto.

O

__NA__ La **SEGUNDA PARTE** certifica y garantiza que al momento de suscribir este contrato ha rendido planilla contributiva durante los cinco (5) años previos a este contrato y que se encuentra acogida a un plan de pago, con cuyos términos y condiciones está cumpliendo.

O

__NA__ La **SEGUNDA PARTE** certifica que al momento de suscribir este contrato **NO** ha rendido su planilla contributiva durante alguno de los periodos contributivos dentro de los cinco (5) años previos a este contrato y que no adeuda contribuciones al Gobierno de Puerto Rico. También certifica que no tiene deuda contributiva alguna, entendiéndose por deuda contributiva, cualquier deuda por concepto de contribución sobre ingresos, arbitrios, contribución sobre la propiedad mueble e inmueble, incluyendo cualquier imposición de carácter especial, derechos de licencias,

contribuciones retenidas en el origen en el pago de salarios a empleados, en el pago de intereses, dividendos, rentas, salarios y otros emolumentos a individuos o por cualquier otro concepto.

Y

La SEGUNDA PARTE se compromete, además, a someter con su última factura el Modelo SC-6096, Certificación de Deuda expedido por el Departamento de Hacienda. La SEGUNDA PARTE acepta y reconoce que el último pago a efectuarse bajo el contrato, sólo se tramitará si la Certificación de Deuda indica que la SEGUNDA PARTE no tiene deuda con el Departamento de Hacienda. De tener deuda, la SEGUNDA PARTE se compromete a cancelar la misma mediante retención en los pagos a que tiene derecho a recibir por los servicios objeto de esta contratación.

Expresamente se reconoce que éstas son condiciones esenciales del presente contrato, y de no ser correcta en todo o en parte la anterior certificación, esto será causa suficiente para que la **PRIMERA PARTE** pueda dejar sin efecto el mismo y la **SEGUNDA PARTE** tenga que reintegrar a la **PRIMERA PARTE** toda suma de dinero recibida bajo este contrato.

VIGESIMA CUARTA: <u>CERTIFICACIÓN DE IMPUESTO SOBRE VENTAS Y USO-IVU</u>:

NA La **SEGUNDA PARTE** certifica y garantiza que al momento de suscribir este contrato ha rendido su planilla **mensual o anual** contributiva por concepto de impuesto sobre ventas y uso-IVU durante los cinco (5) años previos a este contrato y no adeuda contribuciones al Gobierno de Puerto Rico.

O

NA La **SEGUNDA PARTE** certifica y garantiza que al momento de suscribir este contrato ha rendido su planilla **mensual o anual** contributiva por concepto de impuesto sobre ventas y uso-IVU durante los cinco (5) años previos a este contrato y que se encuentra acogida a un plan de pago, con cuyos términos y condiciones está cumpliendo.

O

NA La **SEGUNDA PARTE** certifica que al momento de suscribir este contrato **NO** ha rendido su planilla **mensual o anual** contributiva por concepto de impuesto sobre ventas y uso-IVU durante alguno de los periodos contributivos dentro de los cinco (5) años previos a este contrato y que no adeuda contribuciones al Gobierno de Puerto Rico.

O

La **SEGUNDA PARTE** certifica que no tiene obligación de radicar la planilla **mensual o anual** de impuesto sobre ventas y uso IVU y/o la planilla **mensual o anual** de impuesto sobre importaciones por ser considerado agente no retenedor al momento de suscribir este contrato.

Y

La SEGUNDA PARTE se compromete además, a someter con su última factura el Modelo SC-6096, Certificación de Deuda expedido por el Departamento de Hacienda. La SEGUNDA PARTE acepta y reconoce que el último pago a efectuarse bajo el contrato, sólo se tramitará si la Certificación de Deuda indica que la SEGUNDA PARTE no tiene deuda con el Departamento de Hacienda. De tener deuda, la SEGUNDA PARTE se compromete a cancelar la misma mediante retención en los pagos a que tiene derecho a recibir por los servicios objetos de esta contratación.

Expresamente se reconoce que éstas son condiciones esenciales del presente contrato, y de no ser correcta en todo o en parte la anterior certificación, esto será causa suficiente para que la **PRIMERA PARTE** pueda dejar sin efecto el mismo y la **SEGUNDA PARTE** tenga que reintegrar a la **PRIMERA PARTE** toda suma de dinero recibida bajo este contrato.

VIGESIMA QUINTA: **CERTIFICACION A FAVOR DEL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS.** La **SEGUNDA PARTE** certifica y garantiza que al momento de suscribir este contrato ha pagado las contribuciones de:

N/A Seguro por Desempleo
N/A Incapacidad Temporal
N/A Seguro Social para Choferes

N/A La **SEGUNDA PARTE** se encuentra acogida a un Plan de Pago, con cuyos términos y condiciones está cumpliendo.

Expresamente se reconoce que ésta es una condición esencial del presente contrato, y de no ser correcta en todo o en parte la anterior certificación, esto será causa suficiente para que la parte contratante pueda dejar sin efecto el mismo y la **SEGUNDA PARTE** tenga que reintegrar a la **PRIMERA PARTE** toda suma de dinero recibida bajo este contrato.

VIGESIMA SEXTA: **CONFLICTOS DE INTERESES:** La **SEGUNDA PARTE** reconoce que en el descargo de su función profesional tiene un deber de lealtad completa hacia la agencia, lo que incluye el no tener intereses adversos a dicho organismo gubernamental. Estos intereses adversos incluyen la representación de clientes que tengan o pudieran tener intereses encontrados con la **PRIMERA PARTE**. Este deber, además, incluye la obligación continua de divulgar a la agencia todas las circunstancias de sus relaciones con clientes y terceras personas y cualquier interés que pudiera influir en la agencia al momento de otorgar el contrato o durante su vigencia.

La **SEGUNDA PARTE** certifica que no está representando ni representará durante la vigencia de este contrato, intereses particulares en casos o asuntos que involucren conflictos de intereses o de política pública contra la **PRIMERA PARTE**.

La **SEGUNDA PARTE** representa intereses encontrados cuando, en beneficio de un cliente es su deber promover aquello a que debe oponerse en cumplimiento de sus obligaciones para con otro cliente anterior, actual o potencial. Representa intereses en conflicto, además, cuando su conducta es descrita como tal en las normas éticas reconocidas a su profesión, o en las leyes y reglamentos del Estado Libre Asociado de Puerto Rico.

En contratos con sociedades o firmas constituirá una violación de esta prohibición el que alguno de sus directores, asociados o empleados incurra en la conducta aquí descrita. La **SEGUNDA PARTE** evitará aún la apariencia de la existencia de intereses encontrados.

La **SEGUNDA PARTE** reconoce el poder de fiscalización del jefe de la agencia con relación al cumplimiento de las prohibiciones aquí contenidas. De entender el jefe de la agencia que existen o han surgido intereses adversos para con la **SEGUNDA PARTE**, le notificará por escrito sus hallazgos y su intención de resolver el contrato en el término de treinta (30) días. Dentro de dicho término la **SEGUNDA PARTE** podrá solicitar una reunión a dicho jefe de agencia para exponer sus argumentos a dicha determinación de conflicto, la cual será concedida en todo caso. De no solicitarse dicha reunión en el término mencionado o de no solucionarse satisfactoriamente la controversia durante la reunión concedida, este contrato quedará resuelto.

VIGESIMA SEPTIMA: **PÓLIZAS:** La **SEGUNDA PARTE** mantendr[a en vigor, durante la vigencia de este contrato:

1. Póliza de Responsabilidad Pública bajo la forma "Commercial General Liability" con límites combinados no menores de ($1,000,000.00). La misma debe incluir en sus límites combinados: "personal & advertising injury", "products and complete operations". Dicha póliza deberá contener los siguientes endosos:
   a. Nombrando al Departamento de Salud como asegurado adicional
   b. Hold Harmless Agreement a favor del Departamento de Salud

2. Póliza de seguro "Cyber Liability" con limite no menor de ($2,000,000.00). Esta póliza debe tener cubierta de "network security liability", "network privacy liability", "electronic media liability", con endoso a favor del Departamento de Salud.

3. Póliza de "errors and omissions professional liability" con límite no menor de ($500,000.00.)

Todas las pólizas contendrán una disposición a los efectos de que las mismas no podrán ser canceladas ni modificadas, a menos que medie una notificación por escrito con treinta (30) días de anticipación a la **PRIMERA PARTE,** Oficina de Riesgos y Seguros, Apartado 70184, San Juan, Puerto Rico 00936-8184.

Copia de las pólizas pasarán a formar parte de este contrato y el incumplimiento de cualquiera de las disposiciones de esta cláusula, será causa suficiente para la terminación inmediata del mismo, sin sujeción a la cláusula de Resolución.

La **PRIMERA PARTE** no pagará los servicios prestados durante cualquier período de tiempo en que la póliza no esté vigente.

VIGESIMA OCTAVA: **CREDENCIALES Y SEGUROS DE IMPERICIA:** La **SEGUNDA PARTE** certifica que todo personal asignado a ofrecer servicios conforme a lo establecido en este contrato, tiene vigente las licencias y credenciales profesionales correspondientes a la profesión que practique, a saber: Licencia Profesional, Certificado de Especialidad, Registro de Profesionales y Educación Continuada, Colegiación, y otros documentos pertinentes como el Certificado de "Good Standing", de así requerirlo la profesión. Igualmente, la **SEGUNDA PARTE** certifica que todo personal asignado a ofrecer servicios conforme a lo establecido en este contrato, cuenta con los seguros de impericia profesional según le sea requerido por su profesión o por la **PRIMERA PARTE.** La **SEGUNDA PARTE** releva de responsabilidad a la **PRIMERA PARTE** por cualquier daño derivado del incumplimiento de su personal con los requisitos de licenciamiento, certificación o seguros relacionados a la profesión que practican.

LA **PRIMERA PARTE** podrá requerir a la **SEGUNDA PARTE** evidencia de las licencias, credenciales, seguros y otros documentos que evidencien la preparación y aptitud del personal asignado por la **SEGUNDA PARTE** a prestar servicios bajo el presente contrato.

La **SEGUNDA PARTE** certifica que posee todos los permisos, seguros y licencias asociadas a su negocio o práctica y hará disponibles las mismas cuando la **PRIMERA PARTE** así lo requiera.

En caso de que la **SEGUNDA PARTE** haya sido acusada, administrativa o criminalmente, o convicta de haber obtenido fraudulentamente cualquier credencial, esto será motivo suficiente para que la **PRIMERA PARTE** pueda dar por terminado este contrato inmediatamente.

Queda claramente establecido que, si la **SEGUNDA PARTE** queda desprovista las licencias, credenciales o seguros necesarios para su negocio o práctica profesional, o el personal asignado por la **SEGUNDA PARTE** a brindar servicios no cuenta con las licencias o credenciales requeridos, esto será motivo suficiente para dar por terminado este contrato inmediatamente

VIGESIMA NOVENA: **CODIGO ANTICORRUPCIÓN PARA EL NUEVO PUERTO RICO:** La **SEGUNDA PARTE** certifica conocer y cumplir con las disposiciones éticas establecidas en la Ley Núm. 2-2018 conocida como el "Código Anticorrupción para el Nuevo Puerto Rico".

TRIGÉSIMA: **CUMPLIMIENTO CON POLÍTICA PÚBLICA:** De los profesionales que ofrecen servicios bajo las disposiciones de este contrato incurrir en actos que van en contravención con legislación de Política Pública, tales como, Hostigamiento Sexual, Hostigamiento Laboral, (Ley Núm. 90-2020), Discrimen y Uso y Abuso de Sustancias Controladas, el contrato será terminado de inmediato sin sujeción a la Cláusula de Resolución.

TRIGÉSIMA PRIMERA: **CUMPLIMIENTO CON LEY NÚMERO 127 DE 31 DE MAYO DE 2004: AMBAS PARTES** reconocen y aceptan que ninguna prestación o contraprestación objeto de este contrato podrá exigirse hasta tanto el mismo se haya presentado para registro en la Oficina del Contralor, a tenor con lo dispuesto en la Ley Núm. 18 de 30 de octubre de 1975, según enmendada por la Ley Núm. 127 de 31 de mayo de 2004.

TRIGÉSIMA SEGUNDA: **LITIGIOS:** La **SEGUNDA PARTE** certifica que al momento de suscribir este contrato no tiene litigios en proceso contra ninguna agencia o instrumentalidad gubernamental, incluyendo al Departamento de Salud.

TRIGÉSIMA TERCERA: CERTIFICACIÓN DE LA ADMINISTRACIÓN PARA EL SUSTENTO DE MENORES: La **SEGUNDA PARTE** mantendrá informada a la **PRIMERA PARTE** de cualquier cambio sobre su estado de cumplimiento con la Administración para el Sustento de Menores (**ASUME**), durante la vigencia de este contrato. De haber algún cambio, la **SEGUNDA PARTE** deberá solicitar una nueva Certificación de Cumplimiento a ASUME y someterla a la **PRIMERA PARTE**.

TRIGÉSIMA CUARTA: CUMPLIMIENTO CON LA LEY NÚM. 168 DE 12 DE AGOSTO DE 2000: Cuando sea aplicable, durante la vigencia de este contrato, la **SEGUNDA PARTE** mantendrá informada a la **PRIMERA PARTE** de cualquier cambio en su estatus en el cumplimiento con las disposiciones de la Ley Núm. 168 del 12 de agosto de 2000, según enmendada, conocida como la "Ley de Mejoras al Sustento de Personas de Edad Avanzada de Puerto Rico" mediante la cual se establece el Programa para el Sustento de Personas de Edad Avanzada adscrito a la Administración para el Sustento de Menores **(ASUME)**. el incumplimiento de esta cláusula conllevará la terminación inmediata del presente contrato.

EVR

Expresamente se reconoce que ésta es una condición esencial del presente contrato, y de no cumplir cabalmente con este deber de informar, esto será causa suficiente para que la **PRIMERA PARTE** pueda dejar sin efecto el mismo y la **SEGUNDA PARTE** tendrá que reintegrar a la **PRIMERA PARTE** toda suma de dinero recibida bajo este contrato.

TRIGÉSIMA QUINTA: CONFIDENCIALIDAD: La **SEGUNDA PARTE** reconoce y acepta que, como producto de los servicios requeridos, pudiese adquirir información de carácter sensitivo, protegida, o propiedad de la **PRIMERA PARTE y/o sus usuarios,** que no es conocida ni accesible a terceros. Se considera confidencial; (1) cualquier información de cualquier tipo y naturaleza que la **PRIMERA PARTE** desee mantener confidencial, (2) información de salud protegida, (3) comunicaciones escritas, auditivas o electrónicas, (4) aquella información contenida en cualquier documento o formato preparada, creada o revelada por la **PRIMERA PARTE**, (5) toda información que se obtenga o sea creada por la **PRIMERA PARTE**, (6) toda información declarada confidencial por alguna ley estatal o federal.

Salvo que la divulgación sea requerida legalmente, la **SEGUNDA PARTE** acuerda mantener absoluta confidencialidad de toda que adquiera durante la vigencia de este contrato y mientras dicha información permanezca confidencial.

La **SEGUNDA PARTE** acuerda que, respecto a la información obtenida, no la copiará, utilizará, hará público, divulgará o de ninguna otra manera comunicará de forma directa o indirecta, a cualquier otra persona, fuera del curso de las funciones que le fueran asignadas, o ya sea durante el curso de la prestación de servicios o cualquier tiempo en lo sucesivo, a menos que algún representante autorizado de la **PRIMERA PARTE** lo establezca mediante permiso escrito. En caso de que aplique, la **SEGUNDA PARTE** reconoce y acepta que dicho deber de confidencialidad y secreto quedará extendido a sus empleados, representantes, contratistas, asesores, así como a cualquier persona que, por estrictas razones, deba tener acceso a dicha información.

La **SEGUNDA PARTE** conviene expresamente que la información confidencial no podrá ser utilizada por la **SEGUNDA PARTE** para propósitos ajenos a la **PRIMERA PARTE**, ni para propósitos distintos a los servicios que la **SEGUNDA PARTE** proveerá a la **PRIMERA PARTE**, ni para obtener directa o indirectamente ventaja o beneficio económico para sí, algún miembro de su unidad familiar ni para cualquier otra persona, negocio o entidad.

La **SEGUNDA PARTE** adoptará, respecto a dicha información confidencial, las mismas medidas de seguridad que adoptaría normalmente respecto a su información confidencial, evitando en la medida de lo posible su pérdida, robo, sustracción, divulgación y/o uso. Al momento de concluir el presente Contrato, la **SEGUNDA PARTE** acuerda que devolverá a la **PRIMERA PARTE** toda la información confidencial que hubiese obtenido como parte de la ejecución de este.

La **SEGUNDA PARTE** será responsable en caso de que revele, divulgue, distribuya, reproduzca o utilice la información o documentación confidencial, protegida y/o propietaria de la **PRIMERA PARTE**, en violación a esta Cláusula, ya sea de forma dolosa o por mera negligencia, la **SEGUNDA PARTE** habrá de responder por los daños ocasionados. La **SEGUNDA PARTE**, entiende, que la violación a su deber de confidencialidad podrá acarrear, entre otros mecanismos legales, la terminación de este Contrato.

TRIGÉSIMA SEXTA: **SUB-CONTRATACIÓN:** La **SEGUNDA PARTE** no podrá subcontratar con entidad privada alguna para delegar los servicios esenciales objeto de esta contratación. La **SEGUNDA PARTE** sólo podrá subcontratar servicios personales y servicios profesionales y consultivos con el fin de dar cumplimiento a los servicios objeto de esta contratación. De ninguna manera y bajo ninguna circunstancia debe interpretarse que el consentimiento de la **PRIMERA PARTE** para autorizar dichas subcontrataciones implica que la **PRIMERA PARTE** incurre en obligaciones adicionales al monto total en dólares convenido en este contrato, o que la **SEGUNDA PARTE** queda relevada de responsabilidad por cualesquiera daños y perjuicios que pueda ocasionar la parte que se subcontrate.

Cualquier subcontratación que la **SEGUNDA PARTE** estime necesaria realizar y que no esté contemplada entre las subcontrataciones permisibles, requerirá la autorización escrita de la **PRIMERA PARTE.** Todo subcontrato estará sujeto a las condiciones especiales estipuladas en este contrato y a cualquier otra condición que la **PRIMERA PARTE** estime necesaria para su aprobación, y a todas las leyes y reglamentos estatales y federales aplicables al contrato originado entre la **PRIMERA PARTE** y la **SEGUNDA PARTE.**

TRIGÉSIMA SÉPTIMA: **ESCENARIO DE TRABAJO LIBRE DE HUMO:** La **SEGUNDA PARTE** se compromete con las disposiciones de la Ley Núm. 40 de 3 de agosto de 1993, según enmendada, conocida como "Ley para Reglamento la Práctica de Fumar en Determinados Lugares Públicos y Privados"; y con el Reglamento del Secretario de Salud y la Policía de Puerto Rico Núm.7304, según enmendado, las cuales prohíben la práctica de fumar en sus instalaciones, incluyendo áreas internas y externas tanto abiertas como cerradas, entre otros.

TRIGÉSIMA OCTAVA: OTRAS DISPOSICIONES:

La **SEGUNDA PARTE** hace constar que trabaja bajo contrato para la o las siguientes entidades gubernamentales NSTP, DACO y que los servicios que presta bajo el o los mismos no confligen de forma alguna con los que prestará bajo las disposiciones de este contrato. La **SEGUNDA PARTE** certifica que la o las antes mencionadas, son todas las entidades del Gobierno de Puerto Rico con las que tiene alguna relación contractual. La **SEGUNDA PARTE** reconoce y acepta que el omitir mencionar alguna entidad gubernamental, con la cual tenga una relación contractual vigente puede resultar en la rescisión de la presente contratación de así requerirlo la **PRIMERA PARTE**.

TRIGÉSIMA NOVENA: **VESTIMENTA:** La **SEGUNDA PARTE** prestará sus servicios en las facilidades de la **PRIMERA PARTE**, por lo que deberá observar una vestimenta apropiada y profesional. La **PRIMERA PARTE** cuenta con un Código de Vestimenta, aprobado el 19 de enero de 2021, el que podrá ser utilizado como guía para cumplir con este requisito.

CUADRAGÉSIMA: **CERTIFICACIÓN DE CUMPLIMIENTO CON LA LEY NÚM. 73-2019: REGISTO ÚNICO DE PROVEEDORES DE SERVICIOS PROFESIONALES (RUP).** La **SEGUNDA PARTE** someterá a la **PRIMERA PARTE** la certificación de cumplimiento (Certificado de Elegibilidad) emitido por la Administración de Servicios Generales (ASG) del Registro Único de Proveedores de Servicios Profesionales bajo la categoría correspondiente a los servicios a ser provistos en este contrato.

La **SEGUNDA PARTE** reconoce y acepta que ninguna prestación o contraprestación objeto de este contrato podrá exigirse hasta tanto y en cuanto esté registrado en el RUP y someta a la **PRIMERA PARTE** el Certificado de Elegibilidad.

CUADRAGÉSIMA PRIMERA: **CERTIFICACIÓN DE CUMPLIMIENTO CON LAS POLÍTICAS ESTABLECIDAS POR LA JUNTA DE SUPERVISIÓN Y ADMINISTRACIÓN FINANCIERA (JUNTA).** La **SEGUNDA PARTE** certifica que conoce la política establecida por la **JUNTA** (POLÍTICA DE LA JSAF: REVISIÓN DE CONTRATOS de 6 de noviembre de 2017, modificada el 30 de abril de 2021, disponible en www.juntasupervision.pr.gov/contract-review/), referente a los contratos (o series de contratos relacionados, incluyendo las enmiendas, modificaciones o extensiones, con un valor agregado de **$10,000,000.00** o más, los cuales deben presentarse a la **JUNTA** para su revisión y aprobación previo a su otorgamiento, cumpliendo con el siguiente requisito:

- La información incluída en el Anejo C de la **JUNTA** (Requisito de Certificación del Contratista) es completa, precisa y correcta. La información provista debe incluir según sea aplicable, el nombre de todo principal (personas y/o entidades que tienen plena autoridad para actuar en nombre de la **SEGUNDA PARTE**) y parte interesada principal (personas o entidades con un interés de propiedad o membresía, igual o superior al diez porciento (10%), incluyendo subcontratistas de la **SEGUNDA PARTE**.

La **SEGUNDA PARTE** reconoce además que la **JUNTA** podría además seleccionar de forma aleatoria o de otro modo a su entera discreción, contratos por debajo del umbral de **$10,000,000.00** para asegurar que promuevan la competencia en el mercado y no sean incompatibles con el Plan Fiscal aprobado, al amparo con las Secciones 104(c) y (k) y 204(b)(5) de la Ley PROMESA.

La **SEGUNDA PARTE** reconoce y acepta que de la información presentada a la **JUNTA** no ser completa, precisa y correcta, ésto constituirá causa suficiente para anular este Contrato y la **SEGUNDA PARTE** tendrá la obligación de inmediatamente reembolsar a la **PRIMERA PARTE** la totalidad de cualquier cantidad, pago o beneficio recibido bajo el Contrato.

EVR

CUADRAGÉSIMA SEGUNDA: <u>CERTIFICACIÓN DE CUMPLIMIENTO CON LA ORDEN EJECUTIVA OE2021-029 DE 27 DE ABRIL DE 2021, EMITIDA POR EL HONORABLE GOBERNADOR DE PUERTO RICO, PEDRO R. PIERLUISI</u>. La **PRIMERA PARTE** certifica que la **SEGUNDA PARTE** fue seleccionado como proveedor de los servicios profesionales descritos en este Contrato de conformidad con lo dispuesto en la Orden Ejecutiva 2021-029 o cualquier enmienda subsiguiente a la misma cuando sea de aplicabilidad. Así mismo, **AMBAS PARTES** certifican que conocen las disposiciones de dicha Orden Ejecutiva y que toda contratación cubierta por ésta que no haya seguido los procesos y requisitos allí establecidos será rescindida.

CUADRAGÉSIMA TERCERA: <u>CERTIFICACIÓN DE TRANSFERENCIA DE HABILIDADES Y CONOCIMIENTOS TÉCNICOS</u>. El Plan Fiscal Certificado requiere que todo contrato de servicios profesionales disponga de una transferencia adecuada de habilidades y conocimientos técnicos al personal pertinente de la **PRIMERA PARTE** en la medida que dicho contrato contemple servicios profesionales recurrentes que pueden ser realizados por personal de la **PRIMERA PARTE** debidamente capacitado. A esos efectos, la **SEGUNDA PARTE** certifica que:

N/A Transferirá de manera adecuada sus habilidades y conocimientos técnicos al personal pertinente de la **PRIMERA PARTE** según estipulado en este Contrato.

N/A No está obligado a transferir sus habilidades y conocimientos técnicos, debido a que los servicios que contempla este Contrato no son de carácter recurrente, por lo que no pueden ser realizados por el personal existente de la **PRIMERA PARTE**.

____ No está obligado a transferir sus habilidades y conocimientos técnicos, debido a que los servicios que contempla este Contrato son de carácter especializado y/o requieren independencia para poder realizarse, según definido por el Código de Conducta de la Junta de Supervisión y Administración Financiera, por lo que no pueden ser realizados por el personal existente de la **PRIMERA PARTE**.

CUADRAGÉSIMA CUARTA: <u>DECLARACIÓN COMO PERSONA JURÍDICA</u>: La **SEGUNDA PARTE** certifica que:

N/A Al momento de suscribir este contrato es una corporación debidamente registrada y autorizada para emitir acciones públicamente. Certifica, además, que las acciones emitidas a su nombre y en circulación se intercambian en una bolsa de valores debidamente regulada;

O

____ Al momento de suscribir el presente contrato no es una corporación con acciones intercambiadas públicamente en una bolsa de valores debidamente regulada. Certifica, además, que previo a suscribir este contrato ha cumplimentado el formulario de **"Certificación sobre Personas Jurídicas"** y se lo ha suministrado a la **PRIMERA PARTE**.

CUADRAGÉSIMA QUINTA: NOTIFICACIÓN. Cualquier notificación que deban hacerse **LAS PARTES** en relación al presente **ACUERDO**, se enviará por escrito y se entenderá que la misma fue efectiva al momento de su entrega personal o por correo certificado y electrónico a las siguientes direcciones:

DEPARTAMENTO DE SALUD
P.O. Box 70184
San Juan, Puerto Rico 00983-8184

Secretaría u Oficina	Correo Electrónico	Número de Teléfono
Secretarías de Salud Ambiental (SASA)	Lcda. Mayra Toro Tirado mtoro@salud.pr.gov	(787) 765-2929 ext. 3201
Registro Demográfico	Lcda. Wanda Del C Llovet Díaz. WLlovet@salud.pr.gov	(787) 765-2929 ext. 6101
Secretaría Auxiliar de Reglamentación y Acreditación de Facilidades de Salud (SARAF)	Lcdo. Edwin León Pérez edwin.leon@salud.pr.gov	(787) 765-2929 ext.4701,4702

TECSECURE, LLC
Manuel Guerra Mondragón
CEO
151 Calle San Francisco
San Juan, P.R, 00901
(787) 231-5269
MGM@TECSECURE-INC.COM

CUADRAGÉSIMA SEXTA: ULTRAVIRES: CONFORME A NUESTRO ESTADO DE DERECHO VIGENTE Y LAS NORMAS QUE RIGEN LA CONTRATACION DE SERVICIOS, LOS COMPARECIENTES EN ESTE CONTRATO TOMAN CONOCIMIENTO DE QUE NO SE PRESTARA SERVICIO ALGUNO BAJO ESTE CONTRATO HASTA TANTO SEA FIRMADO POR AMBAS PARTES. DE LA MISMA FORMA, NO SE CONTINUARA DANDO SERVICIOS BAJO ESTE CONTRATO A PARTIR DE SU FECHA DE VENCIMIENTO, EXCEPTO QUE A LA FECHA DE VENCIMIENTO EXISTA YA UNA ENMIENDA FIRMADA POR AMBAS PARTES. NO SE PAGARAN SERVICIOS PRESTADOS EN VIOLACION A ESTA CLAUSULA, YA QUE CUALQUIER FUNCIONARIO QUE SOLICITE Y ACEPTE SERVICIOS DE LA OTRA PARTE EN VIOLACION A ESTA DISPOSICION, LO ESTA HACIENDO SIN AUTORIDAD LEGAL ALGUNA, POR LO QUE LA AGENCIA NO TENDRA LA OBLIGACION DE PAGAR SERVICIOS QUE NO HAN SIDO CONTRATADOS.

EN TESTIMONIO DE LO CUAL, LAS PARTES contratantes suscriben este contrato obligándose así formalmente a cumplir con todas sus cláusulas y condiciones.

En San Juan, Puerto Rico, hoy 1 de Julio de 2022

Por: Lcdo. Esdras Vélez
Principal Oficial Ad

SEGUNDA PARTE
Seguro Social Patronal: 660-72-5242

PRIMERA PARTE
Seguro Social Patronal: 660-43-7470

Este contrato fue presentado para registro en la Oficina del Contralor el _____ de _____ de _____.

TECSECURE INC.

PLAN DE CONTINGENCIA

PLATAFORMA WEB RENOVACIONESONLINE

Autor: Tecsecure Inc.

Versión: 5.0

Actualizado Fecha: 27 septiembre 2022

Documento en constante revision

Copyright © 2022, TECSECURE INC. All Rights Reserved

Autor: Tecsecure Inc.

Versión: 5.0

Actualizado Fecha: 27 septiembre 2022

Documento en constante revision

LISTADO DE RIESGOS

RIESGO	CATEGORÍA	PROBABILIDAD	RESPONSABLE	ACCIÓN CORRECTIVA	MEDIDA PREVENTIVA
Falla de disco duro de servidores.	Hardware	Baja	Rackspace	Cambio de disco duro.	Cada 6 meses revisar el estado de discos duros en los servidores. Si la vida útil está próxima a terminar, realizar cambio de disco duro inmediatamente.
Poco espacio en disco duro de servidores.	Hardware	Baja	Rackspace	Aumento de capacidad en disco, agregando un nuevo disco al rack de discos.	Cada 6 meses revisar el espacio disponible de discos duros en los servidores.
Falla en servicio de servidor web nginx.	Software	Baja	Rackspace	Reiniciar servicio de nginx en los servidores.	Monitoreo diario del estado del servidor web nginx.
Falla en servicio de base de datos mysql enterprise.	Software	Baja	Rackspace	Reiniciar servicio de mysql enterprise.	Monitoreo diario del estado del servidor mysql enterprise.
Falla en respaldos de archivos del sistema en servidor.	Software	Baja	Rackspace	Generar inmediatamente un respaldo de archivos del día actual.	Monitoreo diario de generación de respaldos de archivos de sistema.
Falla en respaldos de base de datos en servidor.	Software	Baja	Rackspace	Generar inmediatamente un respaldo de base de datos del día actual.	Monitoreo diario de generación de dos parciales y uno full respaldos de las base de datos.
Falla general en acceso a plataforma renovacionesonline.com sin causa conocida.	Software	Baja	Rackspace	Contactar a soporte de Rackspace para análisis de posibles causas y soluciones inmediatas.	Monitoreo diario de todos los servicios básicos de software necesarios para mantener online la plataforma web.

Copyright © 2022, TECSECURE INC. All Rights Reserved

Falla en pago de servicios en plataforma al utilizar tarjeta de crédito o cheque electrónico.	Software	Baja	Accepta	Contactar a soporte de Accepta (payment gateway) análisis de posibles causas y soluciones inmediatas.	Monitoreo diario de estado de los servicios online para transacciones de Accepta.
Falla en alguna funcionalidad o regla de negocio de la plataforma web.	Software	Baja	Equipo Desarrollo Tecsecure	Contactar a soporte de renovacionesonline indicando el error encontrado, y toda la información posible del error, con el objetivo de que el equipo de desarrollo genere lo más pronto posible una solución.	Luego de implementar funcionalidades en la plataforma, se lleva a cabo un testeo completo de la funcionalidad. En general, la plataforma web genera archivos de logs de errores cuando se genera realmente un error, los cuales son revisados diariamente.

Copyright © 2022, TECSECURE INC. All Rights Reserved

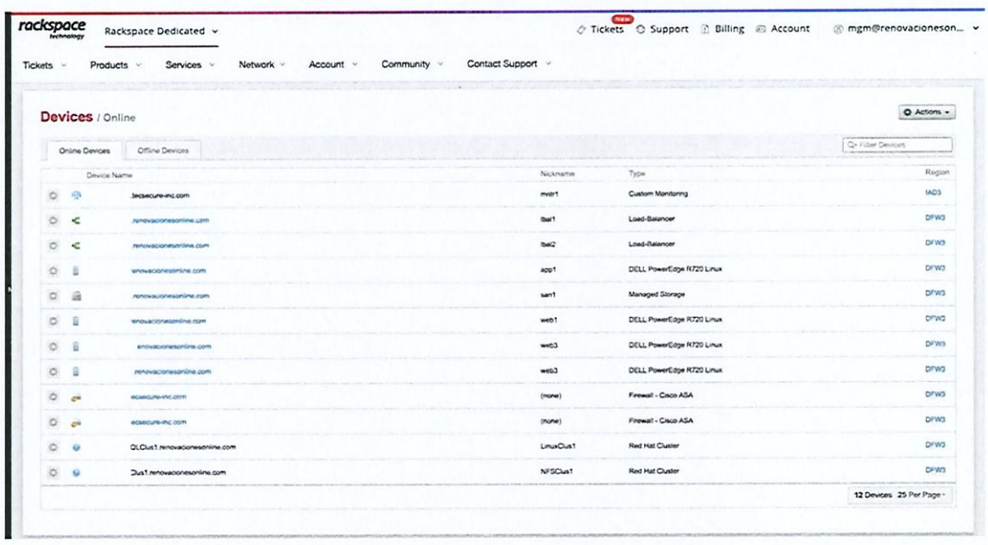
La plataforma se compone de 2 servidores de base de datos MySQL ENTERPRISE los cuales se encuentran trabajando bajo configuración de clúster de alta disponibilidad entregando los servicios de: MySQL y NFS. El servicio de MySQL entregara la base de datos sobre la cual funciona la plataforma y el servicio de NFS habilitara los folders de sitio web y carpetas home de usuario para el funcionamiento del correo electrónico.

Se cuenta además con 2 servidores que realizan el procesamiento de la capa de aplicación de Renovaciones Online con los servicios de: Webserver Nginx, PHP-FPM, Servicio de correo electrónico (Postfix y Dovecot) así como el sistema de Renovaciones Online bajo framework CakePHP.

NOTA: El nuevo software NO tendrá nombre será un White Label reemplazará con una versión en LARAVEL listo para el 2022 con unos cambios y adelantos en procesos de datos y formularios.

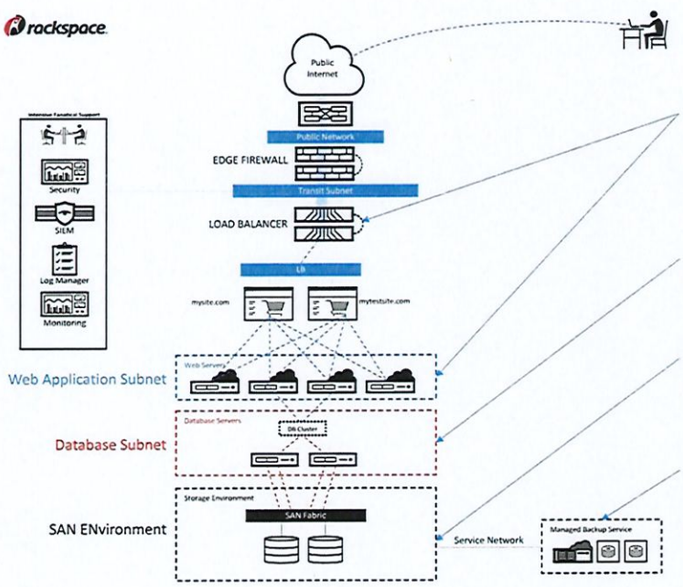
Se agrega también un componente adicional, un servicio de Load Balancer, el cual se configura por encima de los servidores web para otorgar un balanceo de carga de usuarios entre ambos servidores web distribuyendo las sesiones entre ambos equipos.

Con el objetivo de mejorar el funcionamiento y optimizar la plataforma Renovaciones Online se desarrolla una arquitectura de servicios distribuyendo entre 4 servidores



Copyright © 2022, TECSECURE INC. All Rights Reserved

DISENO DE NUESTRA INFRAESTRUCTURA



Balanceador de cargas
La infraestructura cuenta con mayor disponibilidad la capa de presentación, ya que más de 1 servidor sostiene la rotación. En este caso el balanceador recibirá las peticiones web y determinara el mejor servidor en base a carga para atender las peticiones (Normalmente los servidores web, son sitios con un código estáticos lo cual permite tener más de una copia en diferentes servidores)

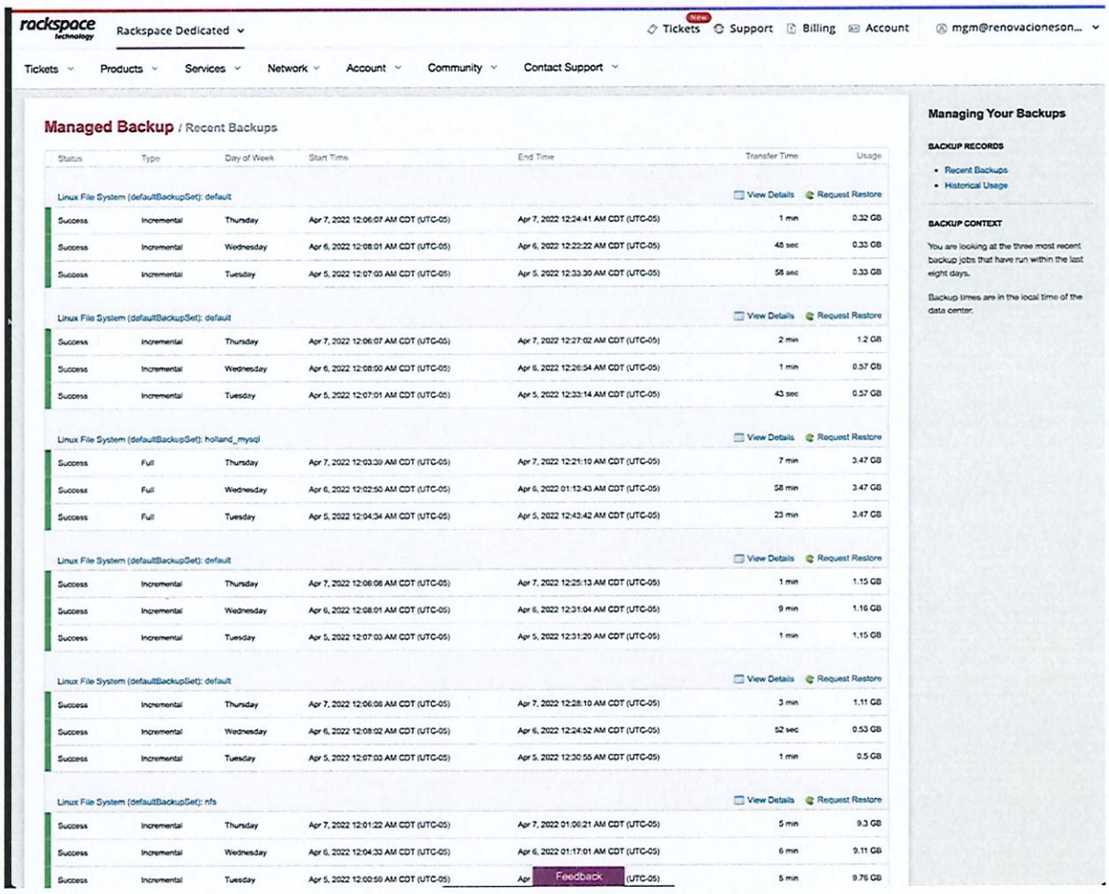
Cluster configuración ACTIVO/PASIVO
Configuración de 2 servidores conectados a un almacenamiento externo. Si uno de los servidores físicos falla, el otro toma su lugar sin interrupción para los aplicativos y/o conexiones de usuario

Almacenamiento desacoplado SAN
Esto permitirá tener la más alta disponibilidad, ya que estos dispositivos son altamente redundantes y de gran escalabilidad, lo que permitirá consumir almacenamiento, conforme nuestras bases de datos crezcan

Respaldos administrados
El respaldo administrado nos brinda la capacidad de tener copias de nuestro información en un medio externo a la infraestructura. La rotación mínima que ofrecemos es 2 semanas de retención (respaldo incremental diario/respaldo full semanal)

Copyright © 2022, TECSECURE INC. All Rights Reserved

BACKUP ES DIARIO



Copyright © 2022, TECSECURE INC. All Rights Reserved

rackspace technology®

RACKSPACE US, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE DATA CENTER HOSTING SERVICES SYSTEM

FOR THE PERIOD OF OCTOBER 1, 2020, TO SEPTEMBER 30, 2021

Attestation and Compliance Services

schellman
Quality, above all.

Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To Rackspace US, Inc.:

Scope

We have examined Rackspace US, Inc.'s ("Rackspace") accompanying assertion titled "Assertion of Rackspace US, Inc. Service Organization Management" ("assertion") that the controls within Rackspace's data center hosting services system ("system") were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Rackspace uses various subservice organizations for data center hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Rackspace, to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Rackspace is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved. Rackspace has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Rackspace is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Rackspace's data center hosting services system were effective throughout the period October 1, 2020, through September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Irving, Texas
December 3, 2021

rackspace technology.

ASSERTION OF RACKSPACE US, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Rackspace US, Inc.'s ("Rackspace") data center hosting services system ("system") throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Rackspace's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE DATA CENTER HOSTING SERVICES SYSTEM

Company Background

Rackspace Technology, Inc ("Rackspace") began operations in December 1993 to provide managed web hosting services to businesses on tools including Amazon Web Services (AWS), Google, VMware, Microsoft, Openstack®, and others. Today, Rackspace serves over 300,000 customers in 33 data centers worldwide. Currently, Rackspace employs over 6,500 people (Rackers) around the world. Rackspace integrates industry leading technologies and practices for each customer's specific need and delivers it as a service via the company's commitment to Fanatical Experience®.

Description of Services Provided

Rackspace serves a broad range of customers with diverse hosting needs and requirements. Rackspace is segmented into business units. They include data center hosting services (including Legacy Datapipe), Managed Colocation, Cloud, Fanatical Experience® for technologies, e-mail, and apps. Managed Colocation serves clients that have significant in-house expertise and only require support around physical infrastructure. Rackspace Hybrid Hosting offers a combination of hosting services that enables customers to use managed hosting and cloud services under one account. Rackspace Fanatical Experience® for technologies includes in-house expertise in support of AWS, VMware, Microsoft, OpenStack, and others. Cloud Hosting serves clients scalable information technology (IT)-enabled capabilities using Internet technologies.

Data center hosting services offerings come in the following forms:

- Dedicated servers for high-performance workloads
- VMware managed environments
- Multi-cloud connectivity with scalability via third party cloud services
- Database management
- Dedicated directly attached storage (DAS), storage area network (SAN), backup and network attached storage (NAS)
- Secure network infrastructure management

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

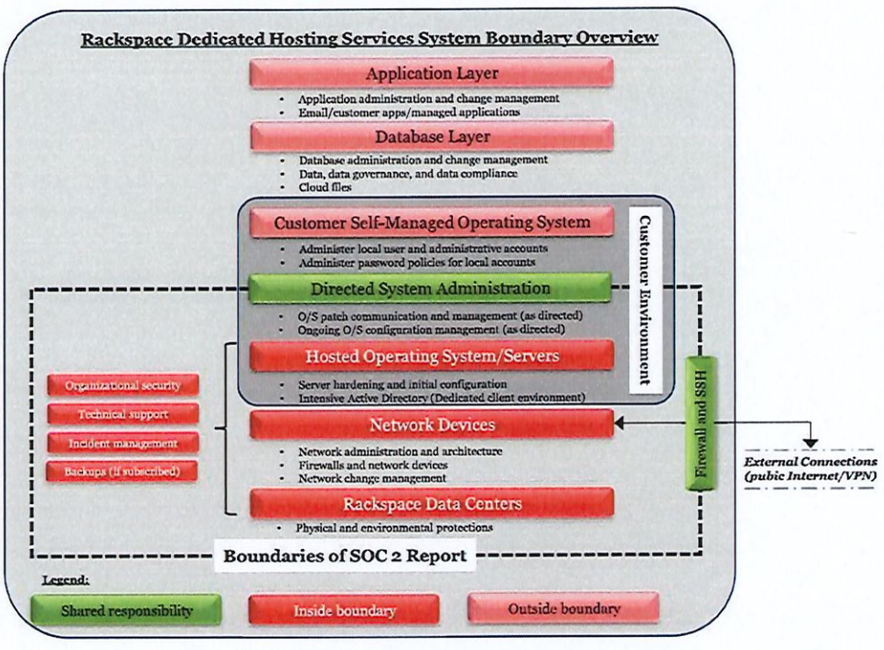
This report covers the data center hosting services system at the following data centers (in-scope data centers):

Physical Location			
Data Center	**Location**	**Ownership Type**	**Vendor**
DFW3	Dallas, Texas	Leased	Digital Reality
FRA1	Frankfurt, Germany	Leased	Digital Reality
FRA2	Frankfurt, Germany	Leased	Equinix
HKG5	Hong Kong, China	Leased	Digital Reality
IAD3	Ashburn, Virginia	Leased	Digital Reality

Physical Location			
Data Center	**Location**	**Ownership Type**	**Vendor**
IAD4	Ashburn, Virginia	Leased	Equinix
LON3	Slough, United Kingdom	Owned/Operated	Rackspace
LON5	Crawley, United Kingdom	Leased	Digital Reality
LON7	London, United Kingdom	Leased	Global Switch
MCI1	Kansas City, Missouri	Owned/Operated	Rackspace
NYC1 / NYC2	Somerset, New Jersey	Owned/Operated	Rackspace
ORD1	Chicago, Illinois	Leased	Digital Reality
SHA3	Shanghai, China	Leased	Shanghai Data Solution Co. Ltd.
SIN2	Singapore	Leased	Equinix
SJC2	San Jose, California	Owned/Operated	Rackspace
SYD2	Sydney, Australia	Leased	Digital Reality
SYD4	Sydney, Australia	Leased	Equinix

This report includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the data center hosting services system at Rackspace. This report does not extend to application and business process controls, automated application controls, or hosted application key reports that may be contained on servers hosted within the data center hosting services system. Additionally, this report does not extend to the workloads (data, files, information) sent by data center hosting services system. The integrity and conformity with regulatory requirements of such data are solely the responsibilities of the applicable data center hosting services customer.

See the illustration below for a visual representation of the boundaries of the system and this report:



Principal Service Commitments and System Requirements

Rackspace designs its processes and procedures to meet its objectives for the data center hosting services system. Those objectives are based on the service commitments that Rackspace makes to its customers. Security and availability commitments to customers are documented and communicated in the data center hosting services product terms and standardized contracts.

Security and availability commitments are standardized and include, but are not limited to, the following:

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security	• System access is granted to authorized individuals • System administrators must complete annual security awareness training • Centralized logging and monitoring • Secure configuration management of infrastructure and servers • Preventative system maintenance and patch management • Identification and remediation of risks and vulnerabilities • Data center security controls to prevent unauthorized access to systems • Network security and network access management • Monthly vulnerability scanning of client environments • Endpoint security management for client virtual servers • Security Incident Response (IR) event detection, investigation, and response	• Identity, access, and personnel management standards and processes • Security awareness and training standards • Audit and accountability standards and processes • Secure configuration standards and configuration management processes • System maintenance and patch management processes • Physical access and environmental standards • System and communication controls and standards • Vulnerability management standards and processes • Centralized endpoint security management platform and standards • IR Plan and processes • Encryption standards • Change management procedures
Availability	• Systems are available for operation and use and monitored as committed or agreed • Ability to backup and restore systems • Disaster recovery services	• Monitoring and alerting standards and processes • Backup and recovery processes • Primary and disaster recovery architecture • Disaster recovery planning and testing processes • Physical and environmental standards

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Rackspace manages and maintains infrastructure components supporting the data center hosting services at the in-scope data centers. Rackspace is responsible for data center infrastructure services, including the following:

- Networking equipment (switches, routers, firewalls, load balancers);
- Physical and logical servers; and
- Physical and environmental security equipment at owned and operated data centers (cameras, badge readers, fire suppression).

Rackspace is responsible for the data center hosting services system's connectivity to the Internet. Rackspace is not responsible for connectivity from Rackspace's owned and leased data centers beyond this point. Rackspace data centers and Rackspace's data center hosting services system communicate between physical locations and data centers using secure protocols and links.

Rackspace supports a large number of network devices that operate to support the data center hosting services system. Network devices within the system boundaries include:

- Brocade switches
- Cisco Adaptive Security Appliance (ASA) firewalls
- F5 Networks Big-internet protocol (IP) firewalls
- Cisco routers
- Cisco Catalyst switches and Cisco Nexus switches

In supporting both the data center hosting services system as well as providing support to Rackspace customers, Rackspace has implemented a series of tools that support authentication and authorization of individuals. Technologies within the system boundaries include:

- Active Directory (AD) – Rackspace utilizes Microsoft AD to provide identity management via directory services for Rackspace employees as well as managing Microsoft server operating systems in the data center hosting services system.
- Active Directory Federation Services (ADFS) – standards-based service that allows the secure sharing of identity information between trusted business partners (federations) across an extranet.
- Cisco Access Control Server (ACS) – Cisco ACS is Cisco's proprietary implementation of their authentication, authorization, and accounting tool for managing access to network components. This is used as the primary means for access control in all Cisco networking devices in the data center hosting services system (e.g., ASA firewalls, Catalyst/Nexus switches, routers).
- SailPoint IdentityIQ (IIQ) – governance-based identity access management (IAM) solution that provides automated access certifications, policy management, access request and provisioning, password management, and identity intelligence.
- Rivest, Shamir, Adelman (RSA) – RSA authentication manager is utilized as the means to provide tokens with rolling personal identification numbers (PIN) codes to enable multi-factor authentication in the Rackspace environment.
- NextGen Bastion Hosts – Balabit shell control box appliances are utilized to provide application layer filtering and proxying of connections into in-scope environments, enforcing multi-factor authentication and creating isolation between in-scope and out-of-scope environments.
- Password Safe – a password management system that is used to securely store, organize, and manage privileged account information and passwords.

Other Tools and / or Services Supporting Infrastructure Components

Rackspace provides tools and services for customers based upon their request and direction. Some of these tools include:

- CORE - A custom developed system playing a critical service management and asset management repository role for Rackspace. All assets are tracked in CORE as well as critical security information (such as passwords for service accounts and other sensitive data regarding system configuration and management).
- CrowdStrike Falcon Intel - provides next-generation antivirus, endpoint detection and response, and cyber threat intelligence.
- Intrusion Detection System (IDS) - Palo Alto network devices are utilized primarily to perform advanced traffic inspection (inclusive of both network layer and application layer inspection) to detect malicious attacks over network connections.
- Splunk - security information and event management (SIEM) system that provides real-time visibility across the information security systems and alerts Rackspace employees based on predefined event triggers.
- MyRackspace Customer Portal - publicly facing web application where Rackspace customers may login to access account information regarding their Rackspace services as well as request updates to their environment (e.g., request firewall rule change, service request, configuration changes).
- Managed Backup - the managed backup environment is a collection of servers in each data center utilized to provide data backup services for customers. The servers responsible for the primary service run the Commvault application and are referred to as a CommCell. The process of data backup of a client is initiated by the CommServe (the central management server within a CommCell) via ServiceNet on a schedule, at which time the client negotiates a channel to the designated media agent and begins streaming data. The media agent (a server designed to transport data from client servers to target data storage) delivers the data across ServiceNet to the designated storage media.
- Rackspace Virtual Infrastructure - includes the management components of the virtualized infrastructure hosting service. This environment uses the VMware NSX distributed firewall to enforce strict isolation between components of the environment. There is a shared management plane (VMNet) network that connects managed hypervisors to this environment. Hypervisors have no IP connectivity to any other network segments. Hypervisors are additionally prohibited from communicating unnecessarily with each other on management interfaces. The above environment is deployed as a fully standalone environment across all Rackspace data centers, with lab / test environments also deployed as standalone, isolated, instances of this infrastructure. Access to the environment is supported via either remote desktop protocol (RDP) or secure shell (SSH) bastion servers, which only allow access from the NextGen bastion infrastructure. Once connected, engineers are able to connect to management interfaces on the vCenter servers. For management, the vCenter servers connect to, and manage, hypervisors via a dedicated management network called VMNet. Devices on this network only have IP addresses to management interfaces, ensuring the management plane is fully isolated. Switch port access control lists on the ServiceNet switches also enforce separation of this network.

People

Personnel involved in the operation and use of the system are:

- The Rackspace leadership team – actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
- The board of directors – consists of members independent from management and has established subcommittees to provide oversight and monitoring of key risk areas (e.g., audit committee, compensation committee, and compliance committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives.

- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- IT personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service deliver infrastructure.

Procedures

Access Requests and Access Revocation to the Corporate Network Infrastructure and Customer Environments

The technology and engineering services (TES) team is responsible for security administration functions, including the provisioning and deprovisioning of employee's logical access accounts in internal Rackspace systems.

The global data center infrastructure (GDCI) team administers access to network infrastructure. Network infrastructure is categorized in two sets, Rackspace's network infrastructure (shared infrastructure) and customer's network infrastructure. The GDCI team manages Rackspace's network infrastructure, whereas the network security (NetSec) team manages the customer's network infrastructure.

New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval. Human Resources is the only division authorized to request corporate network accounts for new employees. The request is initiated by adding a job position within the global people system (GPS) to reflect the hire of a new employee. The corporate AD synchronizes with the GPS system on a nightly basis to determine newly hired employees in need of a network account. Upon receiving AD credentials, the new employee's manager is responsible for initiating an access request for any elevated or administrative access. Users request access to elevated or administrative rights through the SailPoint tool, which are then reviewed and approved / rejected. Following approval through SailPoint, an automated workflow will add users to the approved group, thereby allowing access. User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.

In the event an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts the TES department to modify the transferred employee's access rights to those that are commensurate with the employee's new position and responsibilities.

Access, Authentication and Authorization to the Corporate Infrastructure

The stability of the Rackspace network (shared infrastructure and customer infrastructure) is essential to meeting the company's delivery of uptime and reliability commitments to customers. Rackspace takes measures to ensure that employees with access to the network infrastructure have appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself.

Rackspace has established a minimum password baseline configuration for its corporate AD and production server operating systems that is compliant with the Rackspace authentication standard to further restrict access to the production environment.

Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into each network. Access to the Rackspace network is restricted to authorized personnel only. A VPN is restricted to authorized employees with a valid multi-factor authentication (MFA) token over an encrypted VPN connection.

Administrative access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services. Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS. User activity is controlled and restricted by defining granular authorization privileges based on corporate AD groups. User access privileges to in-scope production environments are reviewed on a quarterly basis to help ensure that access to in-scope systems is authorized. Within the quarterly review, users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed.

Access, Authentication and Authorization to Customer Environments

Employee access to customer environments is restricted through several layers of authentication mechanisms and systems. Systems restricting access to customer devices operate a role-based access functionality to provide appropriate segregation of duties within the company's workforce. CORE is the company's customer service platform, and while most of the Rackspace personnel have access to this system, access to see sensitive information regarding customer devices is restricted to user accounts accessible by authorized personnel.

Access to hosting environments is restricted by only allowing connections from bastion servers through the use of firewall rules. Bastion servers operate as gateways, logging devices, and provide a layer of security between Rackspace infrastructure and the customer infrastructure; bastion servers enable the delivery of Rackspace services while logging protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific AD access group. Bastions provide security to customer environments by restricting access, ensuring the Rackspace infrastructure interfacing with the customer environment is secure. Rackspace personnel authenticate to a bastion server prior to authentication and connection to customer devices. Authentication to bastion servers requires a Rackspace employee to have an active account within the corporate AD.

Data center hosting services system customer devices are managed within two forests, separate from the Rackspace corporate AD network domain:

- Intensive AD: This multi-domain forest is used to authenticate Rackspace employees into the data center hosting services customer environments.
- Global Rackspace (RS) AD: This single-domain forest is connected to the Intensive AD and is used to authenticate customers into their individual environments. Global RS AD consists only of customer accounts.

In order to access a customer environment, Rackspace employees must have an active account within the corporate AD to access dedicated bastion servers. Then, utilizing their Intensive AD credentials, Rackspace employees can either access a customer environment within Intensive AD or through a parent-child trust, within the Global RS AD.

Customer environments are appropriately segregated from other customers through use of organizational units (OUs) within the Intensive and Global RS ADs.

Rackspace has established a minimum password baseline configuration for its Intensive and Global RS AD systems. Rackspace employees gain access to the customer environments using customer network passwords that are configured to expire after 10 hours. Users with administrative privileges to customer devices are provisioned credentials within the Intensive AD and specific AD groups. New user accounts within the Intensive AD are created based on a person's job function and / or manager approval.

Data center hosting services customers purchase hardware from Rackspace and are given read only access to allow full transparency into their own environment. Data center hosting services customers who have elected to use their own hardware are given full administrative control to this infrastructure. Customer firewalls and other network devices delineate the boundary between Rackspace, customer environments, and shared infrastructure. Rackspace manages customer environments following strict security guidelines and policies as to not risk compromise of system and prevent overlap within the shared infrastructure. Rackspace fully manages the administration of shared infrastructure and Rackspace customers retain full administrative rights and control of their environments. The customer is considered the primary system administrator of their environment. The customer is considered the primary system owner of their environment as changes are not made without their documented approval within a ticket. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment. A firewall rule set can be modified by authorized Rackspace employees with terminal access controller access control system (TACACS) clearance which is checked by Cisco ACS software. These commands are authorized and accounted for via ACS.

Customer environments are isolated from one another via the use of virtual networks (VLAN) to logically separate customer traffic. VLANs are used to logically segment customers on the Rackspace network into different broadcast domains to ensure packets are switched only between ports that are designated on the same VLAN, ensuring segmentation of networks amongst Rackspace customers.

Physical Security

Rackspace uses vendors for the physical security controls at leased data centers. Rackspace maintains direct monitoring controls, including annual risk assessments, a review of third-party reports, and periodic touchpoints with the operators of the data centers to provide coverage over the physical and environmental controls performed at those data centers related to Rackspace's service commitments and system requirements and, as a result, the vendors are not deemed subservice organizations and complementary subservice organization controls that are not assumed in the design of Rackspace's controls.

Rackspace implements various physical security mechanisms to protect its personnel, hardware, network, and data from damage or loss due to unauthorized access.

Documented policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews these policies and procedures on an annual basis. Physical access to the data center facilities is documented and granted based on manager approval. The Rackspace data center manager will revoke access when physical access is no longer needed due to termination of employment or services.

Management performs a review of physical access to data center facilities on at least a semi-annual basis to help ensure that access is restricted to authorized personnel.

Access to Rackspace owned data centers is restricted through the use of biometric authentication devices (e.g., hand geometry and /or iris scanner) and keycard / badge devices. Personnel are required to display their identity badges when onsite at Rackspace facilities and visitors to the data center are required to be escorted at all times. Additional physical safeguards are in place to restrict access to Rackspace owned data centers including security guards, alarm systems, and closed-circuit television (CCTV) monitoring.

Encryption and Data Destruction

The global enterprise security (GES) cryptography policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted. To reinforce the objective to secure data, the secure file transfer standard and the physical media handling standard define mandatory security measures for when full encryption of removable media is required. Rackspace encrypts connections to customer portals using SSL or TLS.

Confidential data is sanitized and removed prior to disposal of removable media that is flagged for reuse or disposal at the LON3, SJC2, NYC1, and MCI1 data centers.

Change Management

A structured change management process is documented within the Rackspace Technical Change Management policy and this policy is reviewed and approved annually by the chief operating officer (COO). The purpose of this policy is to mitigate potential risk and customer impact associated with technical changes to the Rackspace production technical infrastructure.

A change is any change made to the production technical infrastructure which has the potential to impact more than one internal or external customer. This includes, but is not limited to, changes to hardware, networking, and applications. Rackspace employees who make global changes to the production technical infrastructure, are expected to abide by this policy.

The change management process requires that changes that impact or have the potential to impact more than one customer are recorded and reviewed in an IT Service Management (ITSM) tool. Changes are planned, tested when technically feasible, evaluated for risk, prioritized, approved, and implemented in a controlled and consistent manner.

Prior to submitting a change, a change requester is required to review the change using the risk level assessment to determine if the risk level is low, medium, or high. The risk level determines the level of approval, the corresponding communications, and other actions required by the Racker proposing the change. The assessment

consists of a risk analysis of five different dimensions: potential impact, planned impact, resiliency, past history, and likelihood.

Technical infrastructure changes with a medium risk rank can be escalated to the change sponsor for implementation approval, and technical infrastructure changes with a high risk are escalated to the change sponsor and to the change management board for implementation approval. After the change management board has reviewed changes and approved where necessary, the change is implemented. Once maintenance has been completed, if unexpected issues or failures arising during the implementation process are analyzed and reported to the change management board.

Rackspace has contractual Service Level Agreements (SLAs) in place that requires external customers receive at least a 72-hour notification for scheduled non-emergency maintenances and up to a 72-hour notice for emergency maintenances. Customers are notified via customer portal and / or other communication channels and are provided information on the effects of the changes to their operations so that they can take appropriate action.

Data Backup and Disaster Recovery

Processing capacity is monitored by data center personnel via the data center operations metrics dashboard. Additionally, data center capacity utilization is reviewed on a monthly basis by data center leadership.

Capacity management (power consumption) for customers is a view of customer environments that provides real time and trending information based on data gathered from the customer environment. The intent is to have the ability to provide a customer with a holistic view of their environment from network through storage to provide insight to the customer about capacity in their environment. Rackspace utilizes redundant routing and switching equipment for its core network infrastructure to protect against availability issues.

Rackspace has developed and maintains a process to address its business continuity plan throughout the organization. This plan addresses the information security requirements needed for the company's continuity in a disaster scenario. It plans for the maintenance and / or restoration of operations to ensure availability of information and continuity of critical business processes. More specifically, a data center business continuity plan (BCP) exists and provides the global business continuity plan for Rackspace data centers to manage significant disruptions to its operations and infrastructure.

Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements. Rackspace regularly tests and updates its business continuity plans to confirm that they are up to date and effective. Tests include full walkthroughs of plans onsite to train staff on emergency events and to ensure plans are adequate in the case of an emergency. Tests are recorded, saved, and used as learning exercises for future tests or emergencies.

Natural disasters have the potential to disrupt data centers and systems and data housed within these systems. Backups are scheduled and performed for customers who have subscribed to the backup service. Backup utility software is used to schedule and perform backups of data on customer servers. Rackspace works with customers to establish a customized backup schedule that is specific to each customer's implementation and operations. In addition, the backup utility software performs backups according to the predefined schedule determined by the customer. Failures are monitored and e-mail alerts are generated to send to backup administrators.

Periodic tests of the restoration process are performed at customer request for data restoration. In the event of a data restoration request, the customer will create a ticket and specify the details of the data that is required to be restored. Upon successful completion of the restoration, the ticket is closed.

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace utilizes an automated disc failure alert process in order to mitigate the risk of faulty media.

Environmental Security

Environmental protections, software, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors where chilled water systems are used as coolant.

Data center operations utilize tools to monitor and evaluate environmental conditions and threats. These tools include fire detection and suppression systems to prevent and mitigate the risk of loss of data and equipment due to a fire. Additionally, data centers are equipped with uninterruptible power supplies (UPS) systems and diesel generators to mitigate data loss due to power failures and / or fluctuations.

Incident Response

Rackspace has a global security operations center (GSOC) team responsible for the identification, tracking, documentation, resolution, and communication of incidents. The incident management team facilitates the remediation and communication efforts for any incident affecting the company's products or infrastructure. Resources are engaged to help restore disrupted services and mitigate the possible adverse effects incidents can have on business operations. Leaders are provided with incident status information to make decisions and direct resources to maintain operations.

Incident response processes exist to respond to and document problems and incidents including security and operational disruptions, establish point(s) of contact and a threshold of incident levels, and are available to personnel through the intranet.

The GSOC has implemented several layers of security protection and defense mechanisms within the Rackspace network. The GSOC department is composed of three teams for proactive and reactive purposes: defensive infrastructure, threat and vulnerability analysis (TVA) and IR. The defensive infrastructure team deploys GSOC security sensors and collectors throughout the network. This team monitors, maintains, and provides maintenance for all security equipment globally and ensure the GSOC is equipped to handle the latest threats based on emerging and existing technology. The TVA is responsible for evaluating the infrastructure and operating systems that support internal applications for the services offered to customers. Additionally, the TVA team provides threat intelligence for the GSOC, and Rackspace based on key relationships and vulnerability assessments performed throughout the year. Finally, the IR team monitors, detects, and responds to cyber security events. The IR team will search for malicious activity based on threat intelligence, investigate major events, and is responsible for educating Rackspace employees on safe and secure business practices.

The incident management team manages the communication to Rackspace customers and employees regarding physical, network, and other incidents that could result in a degraded ability to service customers. Once an incident occurs, a ticket is created to track the event, a communication is sent to applicable Rackspace personnel and customers (as necessary) and upon resolution the ticket is closed. Escalation procedures are determined and communicated to the customer (as necessary). Incident management event details include the impacted system, incident origin, incident start date and time, impact type (awareness, down, degraded), and severity level. Once an incident management event is created, a communication e-mail is sent to applicable Rackspace personnel for notification and status update(s). When an incident is resolved, the ticket is closed documenting the time of the resolution. In the event of a customer impacting incident, escalation procedures are in place and communicated through the customer portal and / or other communication channels / processes, to ensure customers are notified.

Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities. Vulnerability scans of Rackspace infrastructure are performed in accordance with the defined security policy. Remediation plans are documented and tracked in accordance with the defined security policy.

System Monitoring

In addition, there are several mechanisms and controls in place to safeguard network security and availability. For example, the GSOC team has implemented an IDS to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks. An access control system is used to log administrator activity to network devices. Logged activity includes username, successful / unsuccessful login attempts, and timestamp. Logs are retained for one year and are available for review in case of an incident or suspicious activity. Also, Rackspace has implemented an endpoint protection solution to monitor potential threats.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer Information	Rackspace records and keeps track of customer activity in relation to the types of services customers and their users use, the configuration of their environments, and performance metrics related to service requests and the use of the services.	Confidential
User / Account Data	User accounts created for customers for use in their respective data center hosting services environments is stored in Rackspace managed systems. This data includes usernames, full customer names, and organizational information. This information is required to provision and provide services and does not include any personally identifiable information (PII), protected health information (PHI), or other sensitive data. This collection is permitted under the master service agreement (MSA) and associated product terms.	
Log Information	Rackspace collects log data from management systems and customer environment systems. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.	
Metadata	Rackspace stores metadata consisting primarily of tags associated with customer environment information. Metadata enable customer data such as infrastructure metrics, application performance management (APM) and logs to be filtered and grouped. Metadata should not contain personal data as part of the intended use of the service.	

Subservice Organizations

The data center hosting services provided by Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution were not included within the scope of this examination.

The aforementioned data center hosting providers are responsible for providing physical safeguarding of IT infrastructure, to help ensure unauthorized access to the IT infrastructure does not occur. In addition, these data center hosting service providers are responsible for providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution, alone or in combination with controls at Rackspace, and the types of controls expected to be implemented at Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Digital Realty, Equinix, Global Switch, and Shanghai Data Solution	Applicable Trust Services Criteria
Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution are expected to implement controls to ensure that the approval, removal, and periodic review of access for their personnel and the physical security over the leased data center facilities is maintained including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.	CC6.4 CC6.5
Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution are expected to implement environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the data center hosting services system.

bsi.

CYBER ESSENTIALS

This is to certify that

Rackspace Limited

Building 5 Hyde Park Millington Road Hayes UB3 4AZ

Has been assessed
by Jun Woo Lee for BSI Group
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials

Scope: Rackspace Ltd Perimeter Network

Certification date: December 12th, 2019

Recommended re-assessment date: December 12th, 2020

Certificate no.: 2605478153906878

CREST

This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

bsi.

CYBER ESSENTIALS PLUS

This is to certify that

Rackspace Limited

Building 5 Hyde Park Millington Road Hayes UB3 4AZ

Has been assessed
by Jun Woo Lee for BSI Group
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials PLUS

Scope: Rackspace Ltd End User Devices

Certification date: December 12th, 2019

Recommended re-assessment date: December 12th, 2020

Certificate no.: 6745865092649595

CREST

This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
8/18/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
EASTERN AMERICA INSURANCE AGENCY P. O. BOX 193900 RIO PIEDRAS PR 00919-3900	PHONE (A/C, No, Ext):	FAX (A/C, No):
	E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : AIG Insurance Company - Puerto Rico	31674
INSURED TECSECURE INC. PMB 272 B5 CALLE TABONUCO STE 216 GUAYNABO PR 00968-	INSURER B :	
	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$
	☐ CLAIMS-MADE ☐ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$
							MED EXP (Any one person)	$
							PERSONAL & ADV INJURY	$
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$
	☐ POLICY ☐ PRO-JECT ☐ LOC						PRODUCTS - COMP/OP AGG	$
	☐ OTHER:							$
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$
	☐ ANY AUTO						BODILY INJURY (Per person)	$
	☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
	☐ UMBRELLA LIAB ☐ OCCUR						EACH OCCURRENCE	$
	☐ EXCESS LIAB ☐ CLAIMS-MADE						AGGREGATE	$
	☐ DED ☐ RETENTION $							$
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N						☐ PER STATUTE ☐ OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? ☐ (Mandatory in NH)	N / A					E.L. EACH ACCIDENT	$
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$
							E.L. DISEASE - POLICY LIMIT	$
A	Cyber Edge			230-1000582-3	07/23/2022	07/23/2023	Aggregate	$2,000,000
							Deductible	$35,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

DEPARTAMENTO DE SALUD
OFICINA DE SEGUROS Y RIESGOS
APARTADO 70184
SAN JUAN PR 00936-8184

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
Tanya Sanchez

© 1988-2015 ACORD CORPORATION. All rights reserved.

The ACORD name and logo are registered marks of ACORD

bsi.

CYBER ESSENTIALS PLUS

This is to certify that

Rackspace Limited

Building 5 Hyde Park Millington Road Hayes UB3 4AZ

Has been assessed
by Jun Woo Lee for BSI Group
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials PLUS

Scope: Rackspace Ltd End User Devices

Certification date: December 12th, 2019
Recommended re-assessment date: December 12th, 2020
Certificate no.: 6745865092649595

CREST

This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

bsi.

CYBER ESSENTIALS

This is to certify that

Rackspace Limited

Building 5 Hyde Park Millington Road Hayes UB3 4AZ

Has been assessed
by Jun Woo Lee for BSI Group
against the Cyber Essentials Scheme Test Specification

Level of certification: Cyber Essentials

Scope: Rackspace Ltd Perimeter Network

Certification date: December 12th, 2019
Recommended re-assessment date: December 12th, 2020
Certificate no.: 2605478153906878

CREST

This Certificate confirms that the organisation named was assessed against the Cyber Essentials Requirements dated June 2014, and at the time of testing, the organisation's ICT defences were assessed to meet the Requirements. Cyber Essentials Certification indicates that the organisation has implemented a sensible baseline of organisational cyber security only, and implies no guarantee of effective defence against commodity cyber attacks circumventing this baseline. Organisations are recommended to define and understand the risks to their organisation and take all appropriate action to mitigate or reduce any issues, which may require a greater degree of rigour or technical investment than is required for Cyber Essentials alone.

RACKSPACE US, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE DATA CENTER HOSTING SERVICES SYSTEM

FOR THE PERIOD OF OCTOBER 1, 2020, TO SEPTEMBER 30, 2021

Attestation and Compliance Services

Proprietary & Confidential
Reproduction or distribution in whole or in part without prior written consent is strictly prohibited.

schellman

INDEPENDENT SERVICE AUDITOR'S REPORT

To Rackspace US, Inc.:

Scope

We have examined Rackspace US, Inc.'s ("Rackspace") accompanying assertion titled "Assertion of Rackspace US, Inc. Service Organization Management" ("assertion") that the controls within Rackspace's data center hosting services system ("system") were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Rackspace uses various subservice organizations for data center hosting services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Rackspace, to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Rackspace is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved. Rackspace has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Rackspace is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Rackspace's data center hosting services system were effective throughout the period October 1, 2020, through September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Irving, Texas
December 3, 2021

rackspace technology.

ASSERTION OF RACKSPACE US, INC. SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Rackspace US, Inc.'s ("Rackspace") data center hosting services system ("system") throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Rackspace's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Rackspace's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE DATA CENTER HOSTING SERVICES SYSTEM

Company Background

Rackspace Technology, Inc ("Rackspace") began operations in December 1993 to provide managed web hosting services to businesses on tools including Amazon Web Services (AWS), Google, VMware, Microsoft, Openstack®, and others. Today, Rackspace serves over 300,000 customers in 33 data centers worldwide. Currently, Rackspace employs over 6,500 people (Rackers) around the world. Rackspace integrates industry leading technologies and practices for each customer's specific need and delivers it as a service via the company's commitment to Fanatical Experience®.

Description of Services Provided

Rackspace serves a broad range of customers with diverse hosting needs and requirements. Rackspace is segmented into business units. They include data center hosting services (including Legacy Datapipe), Managed Colocation, Cloud, Fanatical Experience® for technologies, e-mail, and apps. Managed Colocation serves clients that have significant in-house expertise and only require support around physical infrastructure. Rackspace Hybrid Hosting offers a combination of hosting services that enables customers to use managed hosting and cloud services under one account. Rackspace Fanatical Experience® for technologies includes in-house expertise in support of AWS, VMware, Microsoft, OpenStack, and others. Cloud Hosting serves clients scalable information technology (IT)-enabled capabilities using Internet technologies.

Data center hosting services offerings come in the following forms:

- Dedicated servers for high-performance workloads
- VMware managed environments
- Multi-cloud connectivity with scalability via third party cloud services
- Database management
- Dedicated directly attached storage (DAS), storage area network (SAN), backup and network attached storage (NAS)
- Secure network infrastructure management

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

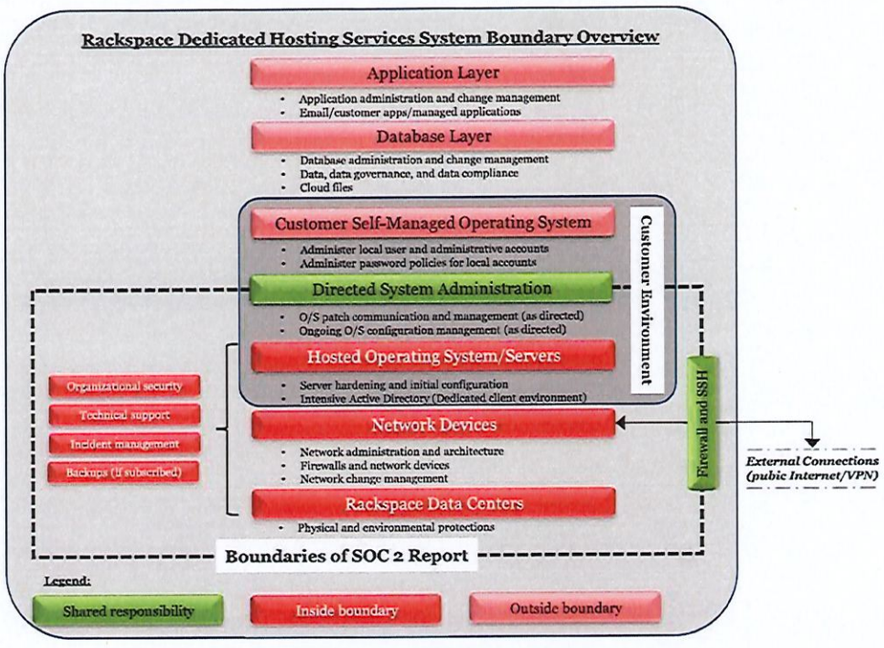
This report covers the data center hosting services system at the following data centers (in-scope data centers):

Physical Location			
Data Center	**Location**	**Ownership Type**	**Vendor**
DFW3	Dallas, Texas	Leased	Digital Reality
FRA1	Frankfurt, Germany	Leased	Digital Reality
FRA2	Frankfurt, Germany	Leased	Equinix
HKG5	Hong Kong, China	Leased	Digital Reality
IAD3	Ashburn, Virginia	Leased	Digital Reality

Physical Location			
Data Center	**Location**	**Ownership Type**	**Vendor**
IAD4	Ashburn, Virginia	Leased	Equinix
LON3	Slough, United Kingdom	Owned/Operated	Rackspace
LON5	Crawley, United Kingdom	Leased	Digital Reality
LON7	London, United Kingdom	Leased	Global Switch
MCI1	Kansas City, Missouri	Owned/Operated	Rackspace
NYC1 / NYC2	Somerset, New Jersey	Owned/Operated	Rackspace
ORD1	Chicago, Illinois	Leased	Digital Reality
SHA3	Shanghai, China	Leased	Shanghai Data Solution Co. Ltd.
SIN2	Singapore	Leased	Equinix
SJC2	San Jose, California	Owned/Operated	Rackspace
SYD2	Sydney, Australia	Leased	Digital Reality
SYD4	Sydney, Australia	Leased	Equinix

This report includes the components, infrastructure, network devices, infrastructure software, and physical data center facilities for the data center hosting services system at Rackspace. This report does not extend to application and business process controls, automated application controls, or hosted application key reports that may be contained on servers hosted within the data center hosting services system. Additionally, this report does not extend to the workloads (data, files, information) sent by data center hosting services system. The integrity and conformity with regulatory requirements of such data are solely the responsibilities of the applicable data center hosting services customer.

See the illustration below for a visual representation of the boundaries of the system and this report:



Principal Service Commitments and System Requirements

Rackspace designs its processes and procedures to meet its objectives for the data center hosting services system. Those objectives are based on the service commitments that Rackspace makes to its customers. Security and availability commitments to customers are documented and communicated in the data center hosting services product terms and standardized contracts.

Security and availability commitments are standardized and include, but are not limited to, the following:

Principal Service Commitments and System Requirements		
Trust Services Category	**Service Commitments**	**System Requirements**
Security	• System access is granted to authorized individuals • System administrators must complete annual security awareness training • Centralized logging and monitoring • Secure configuration management of infrastructure and servers • Preventative system maintenance and patch management • Identification and remediation of risks and vulnerabilities • Data center security controls to prevent unauthorized access to systems • Network security and network access management • Monthly vulnerability scanning of client environments • Endpoint security management for client virtual servers • Security Incident Response (IR) event detection, investigation, and response	• Identity, access, and personnel management standards and processes • Security awareness and training standards • Audit and accountability standards and processes • Secure configuration standards and configuration management processes • System maintenance and patch management processes • Physical access and environmental standards • System and communication controls and standards • Vulnerability management standards and processes • Centralized endpoint security management platform and standards • IR Plan and processes • Encryption standards • Change management procedures
Availability	• Systems are available for operation and use and monitored as committed or agreed • Ability to backup and restore systems • Disaster recovery services	• Monitoring and alerting standards and processes • Backup and recovery processes • Primary and disaster recovery architecture • Disaster recovery planning and testing processes • Physical and environmental standards

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Rackspace manages and maintains infrastructure components supporting the data center hosting services at the in-scope data centers. Rackspace is responsible for data center infrastructure services, including the following:

- Networking equipment (switches, routers, firewalls, load balancers);
- Physical and logical servers; and
- Physical and environmental security equipment at owned and operated data centers (cameras, badge readers, fire suppression).

Rackspace is responsible for the data center hosting services system's connectivity to the Internet. Rackspace is not responsible for connectivity from Rackspace's owned and leased data centers beyond this point. Rackspace data centers and Rackspace's data center hosting services system communicate between physical locations and data centers using secure protocols and links.

Rackspace supports a large number of network devices that operate to support the data center hosting services system. Network devices within the system boundaries include:

- Brocade switches
- Cisco Adaptive Security Appliance (ASA) firewalls
- F5 Networks Big-internet protocol (IP) firewalls
- Cisco routers
- Cisco Catalyst switches and Cisco Nexus switches

In supporting both the data center hosting services system as well as providing support to Rackspace customers, Rackspace has implemented a series of tools that support authentication and authorization of individuals. Technologies within the system boundaries include:

- Active Directory (AD) – Rackspace utilizes Microsoft AD to provide identity management via directory services for Rackspace employees as well as managing Microsoft server operating systems in the data center hosting services system.
- Active Directory Federation Services (ADFS) – standards-based service that allows the secure sharing of identity information between trusted business partners (federations) across an extranet.
- Cisco Access Control Server (ACS) – Cisco ACS is Cisco's proprietary implementation of their authentication, authorization, and accounting tool for managing access to network components. This is used as the primary means for access control in all Cisco networking devices in the data center hosting services system (e.g., ASA firewalls, Catalyst/Nexus switches, routers).
- SailPoint IdentityIQ (IIQ) – governance-based identity access management (IAM) solution that provides automated access certifications, policy management, access request and provisioning, password management, and identity intelligence.
- Rivest, Shamir, Adelman (RSA) – RSA authentication manager is utilized as the means to provide tokens with rolling personal identification numbers (PIN) codes to enable multi-factor authentication in the Rackspace environment.
- NextGen Bastion Hosts – Balabit shell control box appliances are utilized to provide application layer filtering and proxying of connections into in-scope environments, enforcing multi-factor authentication and creating isolation between in-scope and out-of-scope environments.
- Password Safe – a password management system that is used to securely store, organize, and manage privileged account information and passwords.

Other Tools and / or Services Supporting Infrastructure Components

Rackspace provides tools and services for customers based upon their request and direction. Some of these tools include:

- CORE - A custom developed system playing a critical service management and asset management repository role for Rackspace. All assets are tracked in CORE as well as critical security information (such as passwords for service accounts and other sensitive data regarding system configuration and management).
- CrowdStrike Falcon Intel - provides next-generation antivirus, endpoint detection and response, and cyber threat intelligence.
- Intrusion Detection System (IDS) - Palo Alto network devices are utilized primarily to perform advanced traffic inspection (inclusive of both network layer and application layer inspection) to detect malicious attacks over network connections.
- Splunk - security information and event management (SIEM) system that provides real-time visibility across the information security systems and alerts Rackspace employees based on predefined event triggers.
- MyRackspace Customer Portal - publicly facing web application where Rackspace customers may login to access account information regarding their Rackspace services as well as request updates to their environment (e.g., request firewall rule change, service request, configuration changes).
- Managed Backup - the managed backup environment is a collection of servers in each data center utilized to provide data backup services for customers. The servers responsible for the primary service run the Commvault application and are referred to as a CommCell. The process of data backup of a client is initiated by the CommServe (the central management server within a CommCell) via ServiceNet on a schedule, at which time the client negotiates a channel to the designated media agent and begins streaming data. The media agent (a server designed to transport data from client servers to target data storage) delivers the data across ServiceNet to the designated storage media.
- Rackspace Virtual Infrastructure - includes the management components of the virtualized infrastructure hosting service. This environment uses the VMware NSX distributed firewall to enforce strict isolation between components of the environment. There is a shared management plane (VMNet) network that connects managed hypervisors to this environment. Hypervisors have no IP connectivity to any other network segments. Hypervisors are additionally prohibited from communicating unnecessarily with each other on management interfaces. The above environment is deployed as a fully standalone environment across all Rackspace data centers, with lab / test environments also deployed as standalone, isolated, instances of this infrastructure. Access to the environment is supported via either remote desktop protocol (RDP) or secure shell (SSH) bastion servers, which only allow access from the NextGen bastion infrastructure. Once connected, engineers are able to connect to management interfaces on the vCenter servers. For management, the vCenter servers connect to, and manage, hypervisors via a dedicated management network called VMNet. Devices on this network only have IP addresses to management interfaces, ensuring the management plane is fully isolated. Switch port access control lists on the ServiceNet switches also enforce separation of this network.

People

Personnel involved in the operation and use of the system are:

- The Rackspace leadership team – actively supports information security within Rackspace through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.
- The board of directors – consists of members independent from management and has established subcommittees to provide oversight and monitoring of key risk areas (e.g., audit committee, compensation committee, and compliance committee). Each of these committees have defined charters which supports the committee's authority and outlines objectives.

- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- IT personnel – responsible for risk management and identification, monitoring, and compliance of security issues and incidents throughout the service deliver infrastructure.

Procedures

Access Requests and Access Revocation to the Corporate Network Infrastructure and Customer Environments

The technology and engineering services (TES) team is responsible for security administration functions, including the provisioning and deprovisioning of employee's logical access accounts in internal Rackspace systems.

The global data center infrastructure (GDCI) team administers access to network infrastructure. Network infrastructure is categorized in two sets, Rackspace's network infrastructure (shared infrastructure) and customer's network infrastructure. The GDCI team manages Rackspace's network infrastructure, whereas the network security (NetSec) team manages the customer's network infrastructure.

New users with administrative access to the network and users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS policies are created based on job function and manager approval. Human Resources is the only division authorized to request corporate network accounts for new employees. The request is initiated by adding a job position within the global people system (GPS) to reflect the hire of a new employee. The corporate AD synchronizes with the GPS system on a nightly basis to determine newly hired employees in need of a network account. Upon receiving AD credentials, the new employee's manager is responsible for initiating an access request for any elevated or administrative access. Users request access to elevated or administrative rights through the SailPoint tool, which are then reviewed and approved / rejected. Following approval through SailPoint, an automated workflow will add users to the approved group, thereby allowing access. User privileges to in-scope systems that are assigned to terminated employees are revoked as a component of the employee termination process.

In the event an employee's job responsibilities change or the employee transfers to a new department, the individual's manager contacts the TES department to modify the transferred employee's access rights to those that are commensurate with the employee's new position and responsibilities.

Access, Authentication and Authorization to the Corporate Infrastructure

The stability of the Rackspace network (shared infrastructure and customer infrastructure) is essential to meeting the company's delivery of uptime and reliability commitments to customers. Rackspace takes measures to ensure that employees with access to the network infrastructure have appropriate level of knowledge and experience to make configuration changes with minimal security risks and service disruptions to the network itself.

Rackspace has established a minimum password baseline configuration for its corporate AD and production server operating systems that is compliant with the Rackspace authentication standard to further restrict access to the production environment.

Employees can access internal resources by initiating the connection from Rackspace's offices, data centers, or by remotely connecting into each network. Access to the Rackspace network is restricted to authorized personnel only. A VPN is restricted to authorized employees with a valid multi-factor authentication (MFA) token over an encrypted VPN connection.

Administrative access to networking devices is controlled via the use of an access control system that provides authentication, authorization, and accountability services. Rackspace secures access to core networking infrastructure utilizing inherent access control functionality in Cisco ACS. User activity is controlled and restricted by defining granular authorization privileges based on corporate AD groups. User access privileges to in-scope production environments are reviewed on a quarterly basis to help ensure that access to in-scope systems is authorized. Within the quarterly review, users with the ability to create or modify configurations on in-scope hypervisors, firewalls, network devices, and Cisco ACS configurations are reviewed.

Access, Authentication and Authorization to Customer Environments

Employee access to customer environments is restricted through several layers of authentication mechanisms and systems. Systems restricting access to customer devices operate a role-based access functionality to provide appropriate segregation of duties within the company's workforce. CORE is the company's customer service platform, and while most of the Rackspace personnel have access to this system, access to see sensitive information regarding customer devices is restricted to user accounts accessible by authorized personnel.

Access to hosting environments is restricted by only allowing connections from bastion servers through the use of firewall rules. Bastion servers operate as gateways, logging devices, and provide a layer of security between Rackspace infrastructure and the customer infrastructure; bastion servers enable the delivery of Rackspace services while logging protecting the customer environment. Each Rackspace data center has its own set of bastion servers and access is restricted to members of a specific AD access group. Bastions provide security to customer environments by restricting access, ensuring the Rackspace infrastructure interfacing with the customer environment is secure. Rackspace personnel authenticate to a bastion server prior to authentication and connection to customer devices. Authentication to bastion servers requires a Rackspace employee to have an active account within the corporate AD.

Data center hosting services system customer devices are managed within two forests, separate from the Rackspace corporate AD network domain:

- Intensive AD: This multi-domain forest is used to authenticate Rackspace employees into the data center hosting services customer environments.
- Global Rackspace (RS) AD: This single-domain forest is connected to the Intensive AD and is used to authenticate customers into their individual environments. Global RS AD consists only of customer accounts.

In order to access a customer environment, Rackspace employees must have an active account within the corporate AD to access dedicated bastion servers. Then, utilizing their Intensive AD credentials, Rackspace employees can either access a customer environment within Intensive AD or through a parent-child trust, within the Global RS AD.

Customer environments are appropriately segregated from other customers through use of organizational units (OUs) within the Intensive and Global RS ADs.

Rackspace has established a minimum password baseline configuration for its Intensive and Global RS AD systems. Rackspace employees gain access to the customer environments using customer network passwords that are configured to expire after 10 hours. Users with administrative privileges to customer devices are provisioned credentials within the Intensive AD and specific AD groups. New user accounts within the Intensive AD are created based on a person's job function and / or manager approval.

Data center hosting services customers purchase hardware from Rackspace and are given read only access to allow full transparency into their own environment. Data center hosting services customers who have elected to use their own hardware are given full administrative control to this infrastructure. Customer firewalls and other network devices delineate the boundary between Rackspace, customer environments, and shared infrastructure. Rackspace manages customer environments following strict security guidelines and policies as to not risk compromise of system and prevent overlap within the shared infrastructure. Rackspace fully manages the administration of shared infrastructure and Rackspace customers retain full administrative rights and control of their environments. The customer is considered the primary system administrator of their environment. The customer is considered the primary system owner of their environment as changes are not made without their documented approval within a ticket. By outsourcing the hosting to Rackspace, the customer has delegated responsibility for managing the infrastructure components of their environment. A firewall rule set can be modified by authorized Rackspace employees with terminal access controller access control system (TACACS) clearance which is checked by Cisco ACS software. These commands are authorized and accounted for via ACS.

Customer environments are isolated from one another via the use of virtual networks (VLAN) to logically separate customer traffic. VLANs are used to logically segment customers on the Rackspace network into different broadcast domains to ensure packets are switched only between ports that are designated on the same VLAN, ensuring segmentation of networks amongst Rackspace customers.

Physical Security

Rackspace uses vendors for the physical security controls at leased data centers. Rackspace maintains direct monitoring controls, including annual risk assessments, a review of third-party reports, and periodic touchpoints with the operators of the data centers to provide coverage over the physical and environmental controls performed at those data centers related to Rackspace's service commitments and system requirements and, as a result, the vendors are not deemed subservice organizations and complementary subservice organization controls that are not assumed in the design of Rackspace's controls.

Rackspace implements various physical security mechanisms to protect its personnel, hardware, network, and data from damage or loss due to unauthorized access.

Documented policies and procedures are in place to guide employees in the granting, controlling, and monitoring of physical access to and within the data center. Management reviews these policies and procedures on an annual basis. Physical access to the data center facilities is documented and granted based on manager approval. The Rackspace data center manager will revoke access when physical access is no longer needed due to termination of employment or services.

Management performs a review of physical access to data center facilities on at least a semi-annual basis to help ensure that access is restricted to authorized personnel.

Access to Rackspace owned data centers is restricted through the use of biometric authentication devices (e.g., hand geometry and /or iris scanner) and keycard / badge devices. Personnel are required to display their identity badges when onsite at Rackspace facilities and visitors to the data center are required to be escorted at all times. Additional physical safeguards are in place to restrict access to Rackspace owned data centers including security guards, alarm systems, and closed-circuit television (CCTV) monitoring.

Encryption and Data Destruction

The global enterprise security (GES) cryptography policy prohibits the transmission of classified data over the Internet or other public communications paths unless it is encrypted. To reinforce the objective to secure data, the secure file transfer standard and the physical media handling standard define mandatory security measures for when full encryption of removable media is required. Rackspace encrypts connections to customer portals using SSL or TLS.

Confidential data is sanitized and removed prior to disposal of removable media that is flagged for reuse or disposal at the LON3, SJC2, NYC1, and MCI1 data centers.

Change Management

A structured change management process is documented within the Rackspace Technical Change Management policy and this policy is reviewed and approved annually by the chief operating officer (COO). The purpose of this policy is to mitigate potential risk and customer impact associated with technical changes to the Rackspace production technical infrastructure.

A change is any change made to the production technical infrastructure which has the potential to impact more than one internal or external customer. This includes, but is not limited to, changes to hardware, networking, and applications. Rackspace employees who make global changes to the production technical infrastructure, are expected to abide by this policy.

The change management process requires that changes that impact or have the potential to impact more than one customer are recorded and reviewed in an IT Service Management (ITSM) tool. Changes are planned, tested when technically feasible, evaluated for risk, prioritized, approved, and implemented in a controlled and consistent manner.

Prior to submitting a change, a change requester is required to review the change using the risk level assessment to determine if the risk level is low, medium, or high. The risk level determines the level of approval, the corresponding communications, and other actions required by the Racker proposing the change. The assessment

consists of a risk analysis of five different dimensions: potential impact, planned impact, resiliency, past history, and likelihood.

Technical infrastructure changes with a medium risk rank can be escalated to the change sponsor for implementation approval, and technical infrastructure changes with a high risk are escalated to the change sponsor and to the change management board for implementation approval. After the change management board has reviewed changes and approved where necessary, the change is implemented. Once maintenance has been completed, if unexpected issues or failures arising during the implementation process are analyzed and reported to the change management board.

Rackspace has contractual Service Level Agreements (SLAs) in place that requires external customers receive at least a 72-hour notification for scheduled non-emergency maintenances and up to a 72-hour notice for emergency maintenances. Customers are notified via customer portal and / or other communication channels and are provided information on the effects of the changes to their operations so that they can take appropriate action.

Data Backup and Disaster Recovery

Processing capacity is monitored by data center personnel via the data center operations metrics dashboard. Additionally, data center capacity utilization is reviewed on a monthly basis by data center leadership.

Capacity management (power consumption) for customers is a view of customer environments that provides real time and trending information based on data gathered from the customer environment. The intent is to have the ability to provide a customer with a holistic view of their environment from network through storage to provide insight to the customer about capacity in their environment. Rackspace utilizes redundant routing and switching equipment for its core network infrastructure to protect against availability issues.

Rackspace has developed and maintains a process to address its business continuity plan throughout the organization. This plan addresses the information security requirements needed for the company's continuity in a disaster scenario. It plans for the maintenance and / or restoration of operations to ensure availability of information and continuity of critical business processes. More specifically, a data center business continuity plan (BCP) exists and provides the global business continuity plan for Rackspace data centers to manage significant disruptions to its operations and infrastructure.

Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements. Rackspace regularly tests and updates its business continuity plans to confirm that they are up to date and effective. Tests include full walkthroughs of plans onsite to train staff on emergency events and to ensure plans are adequate in the case of an emergency. Tests are recorded, saved, and used as learning exercises for future tests or emergencies.

Natural disasters have the potential to disrupt data centers and systems and data housed within these systems. Backups are scheduled and performed for customers who have subscribed to the backup service. Backup utility software is used to schedule and perform backups of data on customer servers. Rackspace works with customers to establish a customized backup schedule that is specific to each customer's implementation and operations. In addition, the backup utility software performs backups according to the predefined schedule determined by the customer. Failures are monitored and e-mail alerts are generated to send to backup administrators.

Periodic tests of the restoration process are performed at customer request for data restoration. In the event of a data restoration request, the customer will create a ticket and specify the details of the data that is required to be restored. Upon successful completion of the restoration, the ticket is closed.

To ensure that backups are being performed and not skipped due to bad media or equipment, Rackspace utilizes an automated disc failure alert process in order to mitigate the risk of faulty media.

Environmental Security

Environmental protections, software, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. Data centers are equipped with sensors to detect environmental hazards, including smoke detectors and floor water detectors where chilled water systems are used as coolant.

Data center operations utilize tools to monitor and evaluate environmental conditions and threats. These tools include fire detection and suppression systems to prevent and mitigate the risk of loss of data and equipment due to a fire. Additionally, data centers are equipped with uninterruptible power supplies (UPS) systems and diesel generators to mitigate data loss due to power failures and / or fluctuations.

Incident Response

Rackspace has a global security operations center (GSOC) team responsible for the identification, tracking, documentation, resolution, and communication of incidents. The incident management team facilitates the remediation and communication efforts for any incident affecting the company's products or infrastructure. Resources are engaged to help restore disrupted services and mitigate the possible adverse effects incidents can have on business operations. Leaders are provided with incident status information to make decisions and direct resources to maintain operations.

Incident response processes exist to respond to and document problems and incidents including security and operational disruptions, establish point(s) of contact and a threshold of incident levels, and are available to personnel through the intranet.

The GSOC has implemented several layers of security protection and defense mechanisms within the Rackspace network. The GSOC department is composed of three teams for proactive and reactive purposes: defensive infrastructure, threat and vulnerability analysis (TVA) and IR. The defensive infrastructure team deploys GSOC security sensors and collectors throughout the network. This team monitors, maintains, and provides maintenance for all security equipment globally and ensure the GSOC is equipped to handle the latest threats based on emerging and existing technology. The TVA is responsible for evaluating the infrastructure and operating systems that support internal applications for the services offered to customers. Additionally, the TVA team provides threat intelligence for the GSOC, and Rackspace based on key relationships and vulnerability assessments performed throughout the year. Finally, the IR team monitors, detects, and responds to cyber security events. The IR team will search for malicious activity based on threat intelligence, investigate major events, and is responsible for educating Rackspace employees on safe and secure business practices.

The incident management team manages the communication to Rackspace customers and employees regarding physical, network, and other incidents that could result in a degraded ability to service customers. Once an incident occurs, a ticket is created to track the event, a communication is sent to applicable Rackspace personnel and customers (as necessary) and upon resolution the ticket is closed. Escalation procedures are determined and communicated to the customer (as necessary). Incident management event details include the impacted system, incident origin, incident start date and time, impact type (awareness, down, degraded), and severity level. Once an incident management event is created, a communication e-mail is sent to applicable Rackspace personnel for notification and status update(s). When an incident is resolved, the ticket is closed documenting the time of the resolution. In the event of a customer impacting incident, escalation procedures are in place and communicated through the customer portal and / or other communication channels / processes, to ensure customers are notified.

Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities. Vulnerability scans of Rackspace infrastructure are performed in accordance with the defined security policy. Remediation plans are documented and tracked in accordance with the defined security policy.

System Monitoring

In addition, there are several mechanisms and controls in place to safeguard network security and availability. For example, the GSOC team has implemented an IDS to detect and act upon the detection of anomaly network behavior due to unauthorized software or malicious attacks. An access control system is used to log administrator activity to network devices. Logged activity includes username, successful / unsuccessful login attempts, and timestamp. Logs are retained for one year and are available for review in case of an incident or suspicious activity. Also, Rackspace has implemented an endpoint protection solution to monitor potential threats.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer Information	Rackspace records and keeps track of customer activity in relation to the types of services customers and their users use, the configuration of their environments, and performance metrics related to service requests and the use of the services.	Confidential
User / Account Data	User accounts created for customers for use in their respective data center hosting services environments is stored in Rackspace managed systems. This data includes usernames, full customer names, and organizational information. This information is required to provision and provide services and does not include any personally identifiable information (PII), protected health information (PHI), or other sensitive data. This collection is permitted under the master service agreement (MSA) and associated product terms.	
Log Information	Rackspace collects log data from management systems and customer environment systems. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.	
Metadata	Rackspace stores metadata consisting primarily of tags associated with customer environment information. Metadata enable customer data such as infrastructure metrics, application performance management (APM) and logs to be filtered and grouped. Metadata should not contain personal data as part of the intended use of the service.	

Subservice Organizations

The data center hosting services provided by Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution were not included within the scope of this examination.

The aforementioned data center hosting providers are responsible for providing physical safeguarding of IT infrastructure, to help ensure unauthorized access to the IT infrastructure does not occur. In addition, these data center hosting service providers are responsible for providing environmental safeguards (e.g., power supply, temperature control, fire suppression, etc.) against certain environmental threats.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution, alone or in combination with controls at Rackspace, and the types of controls expected to be implemented at Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution to achieve Rackspace's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Digital Realty, Equinix, Global Switch, and Shanghai Data Solution	Applicable Trust Services Criteria
Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution are expected to implement controls to ensure that the approval, removal, and periodic review of access for their personnel and the physical security over the leased data center facilities is maintained including proximity cards, security guards, biometric scanners, alarm systems, and CCTV monitoring.	CC6.4 CC6.5
Digital Realty Trust, Equinix, Global Switch, and Shanghai Data Solution are expected to implement environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the data center hosting services system.

GOBIERNO DE PUERTO RICO
Departamento de Salud
Oficina de Asesores Legales

25 de septiembre de 2022

A LOS ASESORES LEGALES

Lcdo. Miguel A. Verdiales Morales
Principal Asesor Legal del Secretario
Director Interino
Oficina de Asesores Legales

SOBRE CONTRATOS DE TECNOLOGÍA DE INFORMACIÓN

El 31 de mayo de 2022, el Departamento de Salud fue auditado por la Oficina del Contralor (TI-22-11). En dicha auditoría se señala la necesidad de establecer controles efectivos con relación a los contratos de tecnología de información, específicamente aquellos de servicios de tecnología en la nube.

A tenor con lo cual, corresponde a los asesores legales asegurarse que la contratación propuesta cumple con las disposiciones legales aplicables a este tipo de contratación. Hacemos referencia y anejamos para su beneficio las recomendaciones que nos permiten asegurar que se incluya en dicha contratación las cláusulas requeridas por la reglamentación aplicable y proteger los mejores intereses del Departamento de Salud, a saber:

1. Establecer procedimientos para informar incidentes, obtener respuesta por parte del proveedor y otras funciones de seguridad en colaboración con el proveedor.
2. Establecer los medios para que la configuración y versiones del sistema operativo, si aplica, puedan mejorarse según la evolución y cambios de necesidad.
3. Establecer acuerdos de niveles de servicio donde se establezcan los niveles de respuesta de los proveedores en cualquier incidente y las penalidades asociadas al no cumplimiento de los niveles de servicio o la disponibilidad estipulados.
4. Roles y responsabilidades relacionadas a la implantación, operación y apoyo de la solución de tecnología en la nube.
5. Plan de migración de datos en caso de que sea necesario cambiar de proveedor.
6. Plan de respaldo de datos ("back up") recurrente.
7. Plan para la Recuperación de Desastres y Continuidad de las Operaciones.
8. Plan de adiestramiento y capacitación periódica a usuarios.
9. Certificación de revisión de seguridad (SOC-2)
10. Certificado ISO-27001-cumple con los estándares establecidos por ISMS, procesos de seguridad están ajustados para mantenerse al día con los cambios de amenazas de seguridad, vulnerabilidad e impactos adversos.

11. Propiedad exclusiva del Estado Libre Asociado de Puerto Rico sobre los datos y su uso.
12. Disponibilidad, integridad y confidencialidad de los datos.

Se incluye, además, como parte de este memorando: Carta Circular Núm. 140-16 de OGP sobre Normas Generales sobre la implantación de sistemas, compra de equipos y programas y uso de tecnología de la información para los organismos gubernamentales. Esta circular mantiene las políticas con respecto a la tecnología particularmente lo dispuesto sobre revisión de contratos de tecnología (ATI-017).

Estas normas son de estricto cumplimiento.

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Oficina de Gerencia y
Presupuesto

Hon. Alejandro García Padilla
Gobernador

Luis F. Cruz Batista
Director

7 de noviembre de 2016

CARTA CIRCULAR NÚM. 140-16

Secretarios, Jefes de Agencia, Directores, Departamentos, Oficinas, Agencias, Corporaciones Públicas y demás Instrumentalidades de la Rama Ejecutiva del Gobierno del Estado Libre Asociado de Puerto Rico.

Luis F. Cruz Batista
Director

NORMAS GENERALES SOBRE LA IMPLANTACIÓN DE SISTEMAS, COMPRA DE EQUIPOS Y PROGRAMAS Y USO DE LA TECNOLOGÍA DE INFORMACIÓN PARA LOS ORGANISMOS GUBERNAMENTALES

TRASFONDO

La Ley 147 de 18 de junio de 1980, según enmendada, conocida como "Ley Orgánica de la Oficina de Gerencia y Presupuesto", persigue, entre otras disposiciones, aumentar la efectividad, la eficiencia y la economía en el funcionamiento de los organismos gubernamentales, así como promover la óptima utilización de sus recursos. Conforme a ello, como parte de las facultades y deberes de la Oficina de Gerencia y Presupuesto (OGP) se encuentra coordinar y ampliar los esfuerzos gubernamentales para promover la integridad y eficiencia en el manejo de fondos públicos, desarrollar y establecer estándares, políticas, normas y procedimientos para guiar a las agencias en el establecimiento de controles y en la observación de prácticas de sana administración. A tales fines, la OGP emite normas y directrices a los organismos públicos mediante cartas circulares y memorandos generales.

Por otra parte, La Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico", establece que la OGP tendrá la facultad para instrumentar, establecer y emitir la política pública a seguir y las normas que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales con el objetivo primordial de lograr la interconexión de los organismos para facilitar y agilizar los servicios al pueblo. Asimismo, la Ley establece que la OGP podrá establecer políticas a nivel gubernamental.

Consciente de que el acceso a la información es un instrumento democrático de incalculable valor, que le brinda transparencia, agilidad y eficiencia, y facilita la atribución de responsabilidad en la gestión gubernamental, el Gobierno del Estado Libre Asociado de Puerto Rico ha emprendido acciones concretas en esta dirección, las cuales forman parte de las iniciativas tomadas para lograr mayor acceso a la información, mayor eficiencia en la obtención de documentos en poder del Gobierno y mayor capacidad de almacenaje y velocidad. Tales esfuerzos tienen el objetivo de acelerar los efectos positivos que los

PO Box 9023228, San Juan, PR 00902-3228
Tel: 787.725.9420 Fax: 787.725.3521
www.ogp.pr.gov

cambios en la sociedad de la información derivan, gestionando el desarrollo y mantenimiento de las redes y portales de internet del Gobierno y de las agencias e instrumentalidades. El desarrollo de las tecnologías de la información a nivel gubernamental requiere de normas y políticas uniformes que sirvan de apoyo operacional y legal a la adquisición de equipos y contratación de servicios, las operaciones diarias de las agencias relativas a la informática, de manera que la aplicación de las tecnologías promueva la efectiva interconexión de los sistemas a nivel gubernamental y la eficiencia. Lo anterior con el objetivo de mejorar la calidad de los servicios que se prestan a los ciudadanos.

Actualmente, se encuentran vigentes varias Guías o Políticas sobre diversos asuntos de tecnologías de información gubernamental. Con el fin de reafirmar o aclarar su aplicabilidad, actualizar su contenido y facilitar su manejo e implementación, se deroga la Carta Circular Núm. 77-05 y se emite la presente Carta Circular. Tal esfuerzo nos permite servirle mejor a Puerto Rico.

BASE LEGAL

La Ley 151-2004, *supra*, adopta como política pública la incorporación de las tecnologías de información a los procedimientos gubernamentales, a la prestación de servicios y a la difusión de información, mediante una estrategia enfocada en el ciudadano, orientada a la obtención de logros y que fomente activamente la innovación. Asimismo, dispone que será la OGP la entidad responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental, a la vez que ofrecerá asesoramiento a las agencias actualizará y desarrollará las transacciones gubernamentales electrónicas, y se asegurará del funcionamiento correcto de las mismas.

Por otra parte, la Ley 147, *supra*, establece como facultades y deberes de la OGP desarrollar y establecer estándares, políticas, normas y procedimientos para guiar a las agencias en el establecimiento de controles y en la observación de prácticas de sana administración.

OBJETIVO

La política pública del Estado Libre Asociado de Puerto Rico es facilitar y agilizar los procesos operacionales de los numerosos organismos de la Rama Ejecutiva, aumentar la eficiencia y efectividad en la prestación de los servicios gubernamentales al público y viabilizar la interconexión tecnológica entre los organismos y agencias. La mecanización de los sistemas de información requiere regular el uso apropiado de sus componentes y equipos e implantar las medidas necesarias para garantizar la confidencialidad de la información. Conforme a lo anterior, resulta necesario establecer las políticas necesarias para garantizar la adquisición y el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen.

Mediante esta Carta Circular se fijan las normas fundamentales que deben seguir las agencias al establecer sus controles y procedimientos, de manera que se atiendan adecuadamente los recursos, los procesos de compras e implementación de soluciones o tecnología nueva, así como el uso y manejo de los sistemas de información. Las agencias deben velar por el cumplimiento de estas normas en todos los asuntos relacionados a la tecnología de la información del Estado Libre Asociado de Puerto Rico. Esta Carta Circular se acompaña con 17 Políticas o Guías sobre diversos asuntos de tecnologías de información. Tales

Políticas forman parte integral de esta Carta Circular y se pueden acceder a través de la página electrónica de la OGP, en la dirección www.ogp.pr.gov.

APLICABILIDAD

Esta Carta Circular será aplicable a todos los organismos o instrumentalidades y entidades de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, tales como departamentos, juntas, comisiones, administraciones, oficinas, subdivisiones y corporaciones públicas, conforme a lo dispuesto en la Ley Núm. 151-2004, *supra.*

DISPOSICIONES NORMATIVAS

1. Por la presente se adoptan las siguientes políticas:

   a. **Política Núm. ATI-001, Legado Estratégico Anual Tecnológico (LEAN-Tech):** establece la norma y el procedimiento a seguir por las agencias al someter sus planes y proyectos tecnológicos a la aprobación de la Oficina de Gerencia y Presupuesto (OGP), Área de Tecnologías de Información (ATI).
   b. **Política Núm. ATI-002, Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites"):** establece las políticas concernientes al desarrollo y el mantenimiento de los sitios "web" de las agencias.
   c. **Política Núm. ATI-003, Seguridad de los Sistemas de Información**: dispone directrices sobre controles adecuados en los sistemas electrónicos de información para garantizar confidencialidad, integridad y disponibilidad.
   d. **Política Núm. ATI-004, Servicios de Tecnología:** directivas generales que permitirán a las agencias conocer los servicios de tecnología que ofrece la OGP, así como las condiciones y responsabilidades que éstas tendrán que cumplir para recibir los servicios.
   e. **Política Núm. ATI-005, Geotecnologías:** establece estándares y guías para las actividades relacionadas a la información geográfica y geotecnológica.
   f. **Política Núm. ATI-006, Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales**: describe responsabilidades y requisitos que las entidades gubernamentales deben cumplir con respecto al desarrollo, implementación y publicación de transacciones electrónicas o formularios electrónicos accesibles por Internet.
   g. **Política Núm. ATI-007, Disposiciones de equipo y licencias**: describe los mecanismos que las entidades gubernamentales establecerán para asegurarse de que se disponga apropiadamente del equipo de tecnologías de información, así como de los programas que tuviesen los mismos instalados, si alguno.
   h. **Política Núm. ATI-008, Uso de sistemas de información, de la Internet y del Correo Electrónico**: define y detalla el uso aceptable de la información que se maneja a través de los sistemas de información gubernamentales y las herramientas de Internet y Correo Electrónico.
   i. **Política Núm. ATI-009, Integración de Sistemas Financieros:** establece los fundamentos que serán requeridos a entidades gubernamentales que requieran desarrollar o adquirir aplicaciones de Nóminas, Finanzas o Recursos Humanos.

j. **Política Núm. ATI-010, Adquisición de Equipo para Sistemas Computarizados de Información:** específica los estándares mínimos que toda adquisición de equipo debe seguir para asegurar que la procura de equipo tecnológico apoye la gestión de Gobierno Electrónico.
k. **Política Núm. ATI-011, Mejores Prácticas de Infraestructura Tecnológica:** establece las buenas prácticas que toda agencia adscrita a la Rama Ejecutiva de Gobierno de Puerto Rico debe seguir al adquirir e implementar componentes en su infraestructura tecnológica.
l. **Política Núm. ATI-012, Tecnologías en la Nube:** establece las guías principales para la adopción de servicios y tecnologías en la nube.
m. **Política Núm. ATI-013, Marco Referencial de Adquisición Tecnológica Gubernamental:** establece las prácticas que toda agencia adscrita a la Rama Ejecutiva de Gobierno de Puerto Rico tienen que seguir al adquirir bienes o servicios tecnológicos.
n. **Política Núm. ATI-014, Manejo de *Firewalls*:** establece el requerimiento de que toda agencia tenga, al menos, u dispositivo o conjunto de dispositivos conocido como *firewall.*
o. **Política Núm. ATI-015, Programa de Continuidad Gubernamental:** consiste de directrices generales que permitirán a las agencias establecer un programa adecuado para garantizar la continuidad operacional de las funciones críticas que la agencia maneja.
p. **Política Núm. ATI 016, Interfaz de Programación:** establece las guías principales para el desarrollo y la adopción de interfaces de programación de aplicaciones.
q. **Política Núm. ATI 017, Revisión de Contratos de Tecnologías:** establece las normas aplicables a la contratación de bienes y servicios de informática en el Estado Libre Asociado de Puerto Rico.

2. Las agencias y entidades de la Rama Ejecutiva serán responsables de seguir e incorporar las disposiciones de las presentes políticas al uso de los sistemas de información.

3. Para las transacciones electrónicas desarrolladas por la OGP, es indispensable que las agencias cumplan con los requerimientos de información que se le hace para cada solicitud, y mantengan un estándar de calidad en el tiempo de respuesta al ciudadano.

4. Para las transacciones electrónicas desarrolladas y desplegadas en los sitios de las agencias, será responsabilidad exclusiva del jefe de agencia y de los funcionarios que éste delegue, asegurar que las transacciones efectuadas se realicen en estricta conformidad con las leyes, reglamentos, políticas y normas aplicables.

5. Cuando una agencia cumpla parcialmente, o deje de cumplir las disposiciones contenidas en esta Carta y las políticas que emanan de ella, la OGP podrá revocarle los beneficios, privilegios y servicios que ofrece a través del Área de Tecnologías de Información Gubernamental.

6. Las agencias y/o los oficiales encargados de los asuntos de tecnología de la información tendrán la obligación de acceder con regularidad al Portal de la OGP, y visitar el Área de Tecnología e Información. En la misma se publicarán las comunicaciones, memorandos, boletines y cualquier otro relativo a la operación de las áreas de tecnología de información del gobierno.

VIGENCIA

Las disposiciones de esta Carta Circular comenzarán a regir inmediatamente.

CLÁUSULA DEROGATORIA

Esta Carta Circular deroga la Carta Circular 77-05 de 8 de diciembre de 2004 y las guías emitidas a su amparo. Asimismo, las guías que acompañan la presente Carta Circular sustituyen o derogan cualquier documento análogo previamente emitido que resulte incompatible y/o redundante, y que no haya sido adoptado por la OGP.

ANEJOS

Política Núm. ATI-001
Política Núm. ATI-002
Política Núm. ATI-003
Política Núm. ATI-004
Política Núm. ATI-005
Política Núm. ATI-006
Política Núm. ATI-007
Política Núm. ATI-008
Política Núm. ATI-009
Política Núm. ATI-010
Política Núm. ATI-011
Política Núm. ATI-012
Política Núm. ATI-013
Política Núm. ATI-014
Política Núm. ATI-015
Política Núm. ATI 016
Política Núm. ATI 017

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-001

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: Legado Estratégico Anual Tecnológico (LEAN-Tech)

DESCRIPCIÓN

Esta Política establece la norma y el procedimiento a seguir por las agencias al someter sus planes y proyectos tecnológicos a la aprobación de la Oficina de Gerencia y Presupuesto (OGP), Área de Tecnologías de Información (ATI).

La misma deroga y sustituye la Política Núm. TIG-001, conocida como Legado Estratégico Anual tecnológico (LEAN-Tech), revisada el 4 de abril de 2013.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.,* Art. 6, inciso (l), (i) y (iii). Asimismo, está autorizada a requerir la información y los documentos que entienda necesarios para la incorporación de procesos y servicios gubernamentales al Gobierno Electrónico. *Id.,* Art. 6, inciso (a). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se

actualizan las políticas concernientes a la norma y el procedimiento a seguir por las agencias al someter sus planes y proyectos tecnológicos a la OGP.

POLÍTICA

Se adopta como política pública establecer el deber y la responsabilidad de las agencias del Estado Libre Asociado de Puerto Rico de preparar un Legado Estratégico Anual Tecnológico (LEAN-Tech) donde se describa la situación actual de la agencia y lo que se espera alcanzar durante el año fiscal con respecto a la adquisición y desarrollo de recursos tecnológicos. Todo proyecto sometido por las agencias deberá estar alineado con lo dispuesto en la Ley Núm. 151-2004, *supra,* y enmarcado en el contexto de los planes estratégicos y sus políticas.

PROCEDIMIENTO

Cada Jefe de agencia, en colaboración con el Director de Sistemas de Información u Oficial Principal de Informática (OPI) de la agencia, es responsable de preparar el Legado Estratégico Anual Tecnológico (LEAN- Tech) exponiendo la estrategia a seguir en el área tecnológica de acuerdo a la visión y misión de la agencia, y que a la vez esté orientado al desarrollo de un gobierno electrónico.

El LEAN-Tech constará de los planes anuales de informática, los planes anuales relacionados a automatización de procesos y las iniciativas que continúen del año anterior como los proyectos de Tecnología de Información, TI, entiéndase un sistema nuevo, la migración a una nueva versión o la modificación sustancial de un sistema en producción. Anualmente, cada agencia informará sus actividades con respecto al manejo y administración de los recursos de tecnología. Se incluirán todos los proyectos, las actividades y tareas relacionadas a presupuesto, compras, desarrollo, organización, directriz, adiestramiento y control asociado a los recursos de tecnología de información en la agencia utilizando el Perfil del Proyecto. La OGP sólo atenderá solicitudes de autorización de contratos relativos a proyectos, actividades o tareas que estén incluidos en el LEAN-Tech.

La información será recopilada en el LEAN-Tech que estará accesible en el Portal del Gobierno en https://lean.pr.gov y debe ser sometida en o antes del 30 de junio de cada año.

EXENCIONES

Ninguna

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Jefe de Agencia - Se refiere al Director, Administrador, Secretario o Jefe que dirige una agencia.

OPI - Oficial Principal de Informática

LEAN - Plan Anual de Administración de Recursos Tecnológicos, Base de Datos

ANEJOS

Ninguno

REFERENCIAS

Manual del Usuario del Legado Estratégico Anual Tecnológico (LEAN-Tech)
Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"

ANTECEDENTE

Política Núm. TIG-001, conocida como Legado Estratégico Anual Tecnológico (LEAN-Tech) revisada el 4 de abril de 2013

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-002

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 noviembre de 2016

TEMA: Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites")

DESCRIPCIÓN

Cada agencia es responsable del desarrollo y mantenimiento de las páginas de Internet, a los fines de que las mismas ofrezcan al ciudadano y a las empresas privadas una alternativa virtual para la búsqueda de información sobre los servicios que se ofrecen. Esta política va dirigida a mejorar la distribución y el alcance de la información de los servicios ofrecidos por el gobierno a los ciudadanos, así como también a adelantar la encomienda de proveer un gobierno electrónico.

La misma deroga y sustituye la Política Núm. TIG-002, conocida como Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites"), revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.,* Art. 6, inciso (l), (i) y (iii). Se requiere a las agencias desplegar una página electrónica en la Internet. *Id.,* Art. 7, incisos (a) y (b). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes al desarrollo y el mantenimiento de los sitios "web" de las agencias del Estado Libre Asociado de Puerto Rico.

POLÍTICA

Toda página, sitio o portal que una agencia desarrolle ya sea interna o externamente, así como las páginas ya publicadas, cumplirán con los siguientes requisitos y condiciones:

1. Enlace al Portal de Gobierno del Estado Libre Asociado de Puerto Rico: A tenor con la integración y difusión inmediata en caso de emergencia o de índole de interés general, se proveerá por parte de OGP, un código HTML para que se implante la barra superior de PR.gov. Dicho código debe estar integrado en todas las secciones de la página web sin excepción.

2. Como medida de eficiencia programática, se exige que todo diseño "web" sea trabajado de modo responsivo ("Responsive Web Design") para que permita un ajuste automático de la programación de la página al dispositivo por el cual se visita. Esta medida pretende evitar incurrir en programación adicional para las unidades móviles y tabletas. Además, permite aumentar la usabilidad y universalidad de su portal.

3. Todo sitio o portal incorporará páginas "web" con la siguiente información: misión; visión; base legal; estructura organizacional; localización geográfica de las oficinas centrales, regionales y locales; horarios; números de teléfonos; información de contacto; servicios ofrecidos; condiciones para recibir los servicios; e información concerniente a compras y subastas.

4. El contenido de la(s) página(s) será revisado por la persona encargada de comunicaciones, por delegación expresa del Jefe de Agencia con el propósito de asegurar la integridad y veracidad de la información presentada a la ciudadanía. La agencia es responsable de toda información que se publique y de las posibles consecuencias de publicar información incorrecta o falsa.

5. Existen tres modalidades de diseño e implantación de una Plataforma de Manejo de Contenido. La utilización de estas modalidades dependerá de la evaluación de los retos, las estrategias, el presupuesto y los recursos que decida asignar para dicho desarrollo:

    a. *Desarrollo interno con el equipo del Área de Tecnologías de Información*: si la agencia no cuenta con los recursos necesarios para la creación de su portal cibernético puede solicitar los servicios de desarrollo del grupo de portales de ATI. En cuyo caso, el desarrollo del portal será sujeto al Procedimiento Estándar de Operación para la creación de páginas web establecido por ATI.
    b. *Desarrollo interno por parte de la agencia gubernamental*: la entidad asignará una persona encargada dentro de la propia agencia para la creación de la página "web". En este caso, ATI ofrecerá su peritaje durante el proceso de diseño, creación e implementación para garantizar que se cumplan con los requisitos mínimos necesarios de accesibilidad, seguridad, integridad de la data y navegación.
    c. *Desarrollo con contratista externo*: la agencia será responsable de llevar a cabo un proceso de Solicitud de Propuestas de donde se seleccionará al proveedor que ofrezca la mejor alternativa de costos y a la misma vez, garantice el estricto cumplimiento con los requisitos de diseño, desarrollo, prueba, transferencia de conocimiento, mantenimiento y publicación que sean promulgados por OGP al igual que las leyes y reglamentos establecidas al respecto. La OGP, a través de ATI, ofrecerá su peritaje durante el proceso de diseño, creación e

implementación para que cumplan con los requisitos mínimos necesarios sin limitarse a accesibilidad, seguridad, integridad de la data y navegación.

6. Con el propósito de facilitar el proceso de publicación de información en la Internet cada agencia establecerá las políticas, los procedimientos y las responsabilidades internas para la creación y el mantenimiento de información de las páginas "web" de la agencia. Dichas políticas deberán estar alineadas con las políticas y reglamentación establecidas por ATI, y con cualquier otra normativa aplicable.

7. Con el propósito de que las agencias publiquen páginas que garanticen acceso a personas con impedimentos y aumentar la disponibilidad de la información presentada, las páginas estarán diseñadas conforme a las disposiciones de la Ley Núm. 229-2003, según enmendada, conocida como la "Ley para Garantizar el Acceso de Información a las Personas con Impedimentos". Esta ley establece que toda página electrónica estará diseñada para presentar información en formatos alternos. Asimismo, el referido estatuto dispone para que se utilice, en estas páginas, el lenguaje universal a ser leído por programas de asistencia tecnológica. Con el propósito de cumplir con esta ley, se establece lo siguiente:

   a. *Descripción en imágenes y animaciones*: debe utilizarse el código HTML ALT para describir la función de cada elemento visual en la página. Por ejemplo, ALT="descripción del gráfico".
   b. *Documentos en formato PDF*: Cuando se creen los documentos en formato PDF, se deben verificar que los mismos puedan ser copiados como texto y no creados como imagen. También pueden ser grabados con la opción OCR, para que los documentos en PDF puedan ser legibles por programas especializados como los lectores de pantalla de los no videntes.
   c. *"Scripts, applets y plug-ins":* hay que ofrecer contenido alternativo si las funciones actuales nuevas no son accesibles por este tipo de solución.
   d. *Eliminación de animaciones en Adobe Flash*: Por motivos de compatibilidad y seguridad, se solicita ir eliminando el uso de animaciones en Adobe Flash y optando por alternativas modernas, tales como HTML5.
   e. *Uso de encabezados, listas y estructuras consistentes*: Se habrá de utilizar el "Cascading Style Sheet" (CSS) para dar formato a la página "web", en la medida de lo posible. Sugerimos que se implemente la modalidad de "breadcrumbs", facilitando así al usuario la navegación del portal.
   f. *Mapa*: Se debe incluir un "sitemap" con las secciones principales del portal de forma tal que el usuario pueda acceder de forma rápida y organizada al material de interés. Asimismo, este mapa le ayudará para la actualización de las secciones correspondientes al portal de la agencia.

8. Las páginas "web" que se publiquen observarán el cumplimiento estricto con las disposiciones de la Ley Núm. 55-2012, conocida como la "Ley de Derechos Morales de Autor de Puerto Rico".

9. Las páginas "web" que se publiquen observarán el cumplimiento estricto con la Ley Núm. 78-2011, según enmendada, conocida como el "Código Electoral de Puerto Rico para el Siglo XXI", particularmente con aquellas disposiciones sobre gastos de difusión pública del Gobierno durante el año en que se celebre una elección general y hasta el día siguiente a la fecha de la celebración de la misma; así como la reglamentación que se adopte en virtud de dicha Ley.

10. Bancos de datos y recopilación de datos: toda la información de los ciudadanos que se recopile en la página "web" de la agencia debe cumplir con la política de privacidad y uso establecida en el portal del Gobierno del Estado Libre Asociado de Puerto Rico. Ningún desarrollo "web" debe incurrir en un nuevo registro de usuario con solicitud de información sensitiva, como es el seguro social. Cada agencia es responsable de solicitar a ATI la información sobre los registros compartidos para lograr reducir la cantidad de registros de usuario. Será requisito el obtener autorización de ATI para que nuevas páginas "web" utilicen un registro de usuario. ATI se asegurará del cumplimiento con los estándares de diseño, acceso, manejo, disposición y utilización de dicha información.

11. Todo proceso de desarrollo, implementación y mantenimiento debe ir acompañado de la documentación pertinente al proyecto. La documentación debe incluir todo el proceso de diseño e integración de los componentes junto al análisis de las pruebas de aceptación y uso, previo a la publicación del portal. Además, se debe incluir todo protocolo pertinente para el mantenimiento del portal cibernético donde se deberán especificar los procesos de respaldo ("backup") y el restablecimiento, en la eventualidad de cualquier caída o pérdida de contenido. Dicha documentación debe almacenarse en la agencia correspondiente y estar disponible para revisión de ATI de ser requerida.

12. Todo portal debe identificar y establecer iniciativas para la creación de "Web API's", de forma tal que se utilicen tecnologías novedosas que simplifiquen la prestación de servicios a través de otros portales en el Internet y la comunicación intragencial.

13. Las páginas "web" utilizadas para procesar las transacciones electrónicas están sujetas a la Política de Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales (ATI-006) y a la Política de Seguridad de los Sistemas de Información (ATI-003).

PROCEDIMIENTO

Según establece la Carta Circular Núm. 138-2016 de 12 de octubre de 2016, "Guías para Evaluar las Páginas de Internet del Gobierno", ATI evaluará periódicamente el contenido, el diseño y la utilidad de las páginas "web" publicadas. Para evaluar dichas páginas "web" y establecer los criterios mínimos que estas páginas deben cumplir, ATI utilizará el documento denominado "Evaluación de Página de Internet Gobierno". El equipo de trabajo de ATI notificará oportunamente los resultados de estas revisiones para que las agencias tomen conocimiento y adopten las medidas correctivas que sean necesarias.

EXENCIONES

Ninguna

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

"Breadcrumb" – Historial de navegación.

HTML5 – siglas del inglés de "Hyper Text Mark up Language"; refiérase a, lenguaje usado para estructurar y presentar el contenido para la web de forma ágil y que permite mayor sofisticaciónen el contenido.

Interfaz de programación ("Web API") – Significa el conjunto de funciones que permite la comunicación entre aplicaciones y representan la capacidad de comunicación entre componentes de "software." Éstas permiten la comunicación a través del Internet por una entidad externa con aplicaciones internas, con el objetivo de permitir el libre acceso, de manera segura, a entidades autorizadas, con información del Estado Libre Asociado de Puerto Rico.

OCR – siglas del inglés de "Optical Character Recognition"; refiérase a, la capacidad de reconocer imágenes y/o caracteres en un papel y convertirlos en datos digitales.

PDF - sigla del inglés de "Portable Document Format"; refiérase a, formato de documento portátil, el que constituye un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto)

Plataforma de Manejo de Contenido – Significa el desarrollo global o programa que permite acceder al Portal de Gobierno por medio de un navegador de Internet y el cual provee diversos niveles de privilegios para la edición, la publicación y el acceso a información relevante y pertinente.

Sitio "Web" – Significa una dirección virtual en la "World Wide Web".

Sitio "Web" Agencial – Significa el conjunto de páginas "web" que representan a una agencia del Estado Libre Asociado de Puerto Rico.

W3C – Significa el "World Web Consortium", el cual es el líder promoviendo estándares y guías de la Internet. Esta organización tiene múltiples grupos y comités que promueven las mejores prácticas en las áreas relacionadas al uso de la "web".

"Webmaster" – Significa un profesional informático encargado de la administración de los servicios de un sitio "web".

"Webmaster" Agencial – Significa el "webmaster" reconocido como la persona enlace entre la OGP y la agencia en que labora.

"Web Hosting" – Significa el espacio virtual para la publicación de las páginas "web", las estáticas o las dinámicas basado en la plataforma de manejo de contenido del Portal del Gobierno.

ANEJOS

Carta Circular Núm. 138-2016 de 12 de octubre de 2016, "Guías para Evaluar las Páginas de Internet del Gobierno", y su Anejo I, Formulario titulado "Evaluación de Página de Internet Gobierno".

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Ley Núm. 229-2003, según enmendada, conocida como "Ley para Garantizar el Acceso a Información a las Personas con Impedimentos"
Ley Núm. 55-2012, conocida como "Ley de Derechos Morales de Autor"
Ley Núm. 78-2011, según enmendada, conocida como "Código electoral de Puerto Rico para el Siglo XI"
Carta Circular Núm. 138-2016 de 12 de octubre de 2016, "Guías para Evaluar las Páginas de Internet del Gobierno"
Política Núm. ATI-06, sobre de Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales, revisada el 7 de noviembre de 2016
Política Núm. ATI-03, sobre Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016

ANTECEDENTES

Política Núm. TIG-002, conocida como Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites", revisada el 12 de septiembre de 2007.

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Oficina de Gerencia y
Presupuesto

Hon. Alejandro García Padilla
Gobernador

Luis F. Cruz Batista
Director

Evaluación de las Páginas de Internet del Gobierno

Agencia Evaluada: _____ Fecha: _____

Evaluador (a): _____ Puesto: _____

Instrucciones Generales	
Este documento representa los aspectos más relevantes e importantes que debe tener toda página electrónica del gobierno. Los criterios a evaluarse serán los siguiente:	
Contenido	Lo que está comprendido en la Información. Incluye el ámbito, la extensión y significado de la misma. El mismo tiene que estar acorde con la audiencia que utilizará la información.
Utilidad	Determina cuán práctica y fácil de entender es la página para el usuario.
Diseño	Formato estructurado a través del cual se organiza la información de manera atractiva, lógica y útil para el usuario.
El (la) evaluador (a) deberá indicar con una "X" si el requisito presentado:	
Cumple	El requisito está presente en la página y está funcionando en su totalidad.
En Proceso	El requisito comenzó a trabajarse o está esperando por aprobación
No Cumple	El requisito no está contemplado en la página o está presente, pero no cumple con lo requerido.
Nota: Previo al inicio de la evaluación, (uno o dos días antes), el (la) evaluador (a) realizará una prueba para determinar disponibilidad (Reactivo #3 dentro de la categoría de Utilidad). Esta consistirá en acceder la página por tres ocasiones durante un mismo día. Deberá hacer un lapso mínimo de tres horas entre cada intento. Para que la página cumpla, ésta tiene que haber estado disponible durante las tres ocasiones. Si se pudo acceder a la página en dos ocasiones, se puede catalogar "En Proceso". Finalmente si la página estuvo disponible una sola vez o en ningún momento, se catalogará como "No Cumple" y se hará la anotación en las observaciones donde indique lo ocurrido para que se tomen las medidas correctivas necesarias.	

PO Box 9023228, San Juan, PR 00902-3228
Tel: 787.725.9420 Fax: 787.725.3521
www.ogp.pr.gov

Contenido	Cumple	En Proceso	No Cumple
1. La página principal contiene distintos enlaces a través de los cuales se puedes acceder			
a. Base Legal de la Agencia			
b. Facultades que tiene la Agencia			
c. Misión y Metas de la Agencia[1]			
d. Descripción de las distintas unidades de la Agencia			
e. Historia de la Agencia			
f. Comunicados de prensa, actividades, subastas			
g. Oportunidades de empleo que ofrece la Agencia[2]			
2. La página provee			
a. Teléfono de los puestos contacto en la Agencia			
b. Dirección física y postal de la Agencia			
c. Correo electrónico de oficiales de contacto de la Agencia			
d. Dirección electrónica del administrador de la Página			
3. La información está organizada en forma:			
a. Lógica (Ej. Los datos tienen una secuencia esperada)			
b. Estructurada (Ej. No se pasa de una tema a otro sin una secuencia lógica; los temas están agrupados por relación)			
c. Precisa (Ej. Se exponen los temas de forma directa y evitando desviaciones o ambigüedad)			
4. La información de página			
a. Es Legible (Ej. Tamaño, color y tipo de letra es entendible)			
b. Está escrita en un lenguaje sencillo			
c. Está libre de errores ortográficos			
5. Los títulos o subtítulos presentados en la página principal están relacionados con el contenido esbozado en los enlaces.			
6. La página le provee al usuario una orientación completa sobre los servicios y la ayuda que la Agencia puede proveerle.			
7. Al acceder un enlace para el servicio, se ofrece la información completa sobre los requisitos necesarios para obtener el mismo.			

[1] La misión y metas de la Agencia deberían presentarse tal y como se describen en el documento de Presupuesto de la Oficina de Gerencia y Presupuesto. De haber discrepancias, verificar con la Agencia la razón de dicha diferencia.

[2] Si la página no tiene una sección sobre oportunidades de empleo en la Agencia, entonces tiene que proveer un enlace que lleve al (la) usuario (a) a la sección de empleos que aparece en el Portal del Gobierno dentro del enlace de " Nuestro Gobierno". De no contar con plazas disponibles, la página deberá establecerlo y la fecha de la última actualización de la misma.

8. La página presenta información de índole informativa e investigativa para el enriquecimiento del usuario.			
9. Las imágenes que se presentan son apropiadas, inclusivas y libre de prejuicio.[3]			
10. Los artículos mencionados en la página están acompañados con sus referencias y bibliografía.			
11. Cumple con los requisitos de información Artículo 7(b) Ley 151-2004			
12. La página provee enlaces a otros portales que puedan complementar la información presentada.			
13. Se incluye la fecha de edición y revisión de la página.			

Observaciones :

Utilidad	**Cumple**	**En Proceso**	**No Cumple**
1. La página se accede:			
a. Fácilmente			
b. Con rapidez			
2. Los enlaces se acceden con facilidad.			
3. Disponibilidad de la página[4]			

[3] Por ejemplo, si se van a incorporar imágenes de la ciudadanía, las mismas deben apelar a todo tipo de ciudadano sin importar edad, raza, clase social, sexo, etc.

[4] Previo al inicio de la evaluación, (uno o dos días antes), el (la) evaluador (a) realizará una prueba para determinar disponibilidad (Reactivo #3 dentro de la categoría de Utilidad). Esta consistirá en acceder la página por tres ocasiones durante un mismo día. Deberá hacer un lapso mínimo de tres horas entre cada intento. Para que la página cumpla, ésta tiene que haber estado disponible durante las tres ocasiones. Si se pudo acceder a la página en dos ocasiones, se puede catalogar "En Proceso". Finalmente si la página estuvo disponible una sola vez o en ningún momento, se catalogará como "No Cumple" y se hará la anotación en las observaciones donde indique lo ocurrido para que se tomen las medidas correctivas necesarias.

4. La cantidad de imágenes y gráficas es adecuada (Ej. No reduce rapidez de la búsqueda para el usuario ni la rapidez de la página misma).			
5. Se provee versión de impresión (por tema) para que el usuario puede imprimir la información que desee.			
6. Se provee un icono que permite enviar información de la página o la página misma a otra persona.			
7. La información contenida en la página principal le permite al usuario saber donde encontrar la información que necesita.			
Observaciones :			

Diseño	Cumple	En Proceso	No Cumple
1. La información contenida en el portal se presenta en forma:			
a. Ordenada (Ej. Enlaces organizados por orden alfabético)			
b. Atractiva (Ej. El color del texto motiva su lectura)			
2. El color del texto permite una lectura manejable (Ej. El color es agradable a la vista, el contraste de colores no cansa la vista).			
3. El fondo de la página ("Background") no interfiere con el contenido de la misma.			
4. El formato facilita el acceso a la información.			
5. La página contiene herramientas de ayuda (ventana de ayuda o buscador, ect) para que el visitante pueda conseguir la información que necesita. [5]			
6. Se utilizan recursos gráficos (gráficas, imágenes, sonidos, ect) para facilitarle al lector el entendimiento de la información.			
7. La página no contiene imágenes pesadas que confundan al lector (Ej. Imágenes en movimiento continuo)			
8. La página cuenta con un registro (counter) que permite identificar la cantidad de usuarios que visitan la misma.			

[5] El (la) evaluador (a) realizará un mínimo de tres pruebas para determinar la eficiencia del buscador. Para ello. Escribirá palabras claves que están relacionadas con información presentada en la página y verificará que con las mismas se pueda encontrar el enlace correspondiente.

9. La página cuenta con enlaces al final de cada pantalla accedida para facilitarle al visitante el regreso al inicio de la página.			
10. La página se adapta en diseño al dispositivos que se esté utilizando para visualizarla.("Responsive Web Design")			
11. La página contiene información de referencia en formatos fáciles de imprimir (EJ. PDF o HTML) para beneficio del visitante.			
12. La página provee el acceso necesario para descargar (download) programas tales como "Acrobat" cuando son necesarios para ver la información.			
13. Las gráficas y demás materiales visuales están acompañados con textos alternos que expliquen su contenido, de forma que cualquier "software" de lectura (Ej. Para no videntes) pueda leer la información.			
14. Todos los enlaces de tipo gráficos o de imágenes están documentados para que la persona pueda determinar a donde lo llevará dicho enlace aunque no puede ver la imagen.			
15. Toda la información transmitida con color, también está disponible sin color (Ej. A través del contenido o que pueda verse en blanco y negro).			
16. Los códigos de color no son la única forma de transmitir información, indicar una acción, marcar una respuesta o distinguir un elemento visual.			
17. Los archivos de multimedia tienen subtítulos y narraciones de audio sincronizadas.			
18. La información contenida en la página está formateada para que sea compatible con formatos alternativos (Ej. Braille, texto ASCII, grabaciones de audio, etc)			
19. Las página que contienen más de tres gráficas o animaciones (Animated gif JAVA, etc) tienen la opción de que se pueda acceder la misma sólo en textos (Text Only).			
20. Los sonidos de la página se identifican de alguna manera visual (Ej. Escribiendo en textos una descripción del sonido o su significado).			
Observaciones:			

Observaciones adicionales sobre Aspectos Positivos e Innovadores encontrados en la página de la Agencia:
Ejemplo: Se provee para que el usuario pueda adaptar el tamaño de la letra en la página.

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-003

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

DESCRIPCIÓN

Esta Política consiste de directrices generales que permitirán a las agencias establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan.

La misma deroga y sustituye la Política Núm. TIG-003, conocida como Seguridad de los Sistemas de Información, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.*, Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos. Asimismo, aplica a cualquier otro organismo gubernamental que no sea una agencia, en cuanto a aquellos particulares que se disponga.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualiza la política concerniente a la seguridad de los sistemas de información.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico deberá seguir las siguientes políticas de seguridad en sus sistemas de información. Los usuarios de los Servicios de la Red Interagencial que no sean agencias (i.e. municipios) están sujetos al cumplimiento de las secciones E, J y K de esta política para poder hacer uso de los Servicios de la Red Interagencial. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables para cumplir la política aquí delineada.

A. Análisis de Riesgos

1. Cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa. Para ello deberá llevar a cabo análisis de riesgos que incluya:

    a. Inventario de activos de sistemas de información que incluya el equipo, los programas (ver sección de Definiciones) y los datos. Todos los activos deberán ser clasificados de acuerdo al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

    b. Identificar las posibles amenazas contra los sistemas de información (i.e. robos, desastres naturales, fallas, virus, acceso indebido a los datos, etc.) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer con qué se van a proteger los activos identificados anteriormente.

B. Continuidad

1. El análisis de riesgo será la base para desarrollar un Plan de Continuidad que incluya un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones.

2. Establecer procedimientos de resguardo (*backup*) recurrentes de la información, de programas y de sistemas esenciales.

3. Las facilidades de sistemas de información deberán estar colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otros desastres.

C. Políticas de Seguridad Adicionales

1. Las políticas de seguridad de este documento son solo el fundamento para unas políticas más detalladas desarrolladas por cada agencia. Será responsabilidad de cada agencia el desarrollar políticas específicas de seguridad tomando en cuenta las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Las políticas desarrolladas por la OGP para su uso interno podrán ser utilizadas como modelos iniciales en el desarrollo de las políticas específicas de cada agencia.

2. Las políticas aquí establecidas no podrán ser invalidadas por las políticas particulares desarrolladas en cada agencia.

D. Leyes y Reglamentos

Las políticas y procedimientos de seguridad deberán estar de acuerdo a la legislación y los reglamentos vigentes que apliquen.

E. Controles Generales

1. Las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados (i.e. virus, spyware, adware y updates automáticos).

2. La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que se adquiera o desarrolle la agencia para facilitar las operaciones de la agencia y/o mejorar el servicio a los ciudadanos.

3. La información y los programas de aplicación en las operaciones de la agencia deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos o acceder a las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

4. Todos los mecanismos de autenticación deberán incluir una contraseña combinada de números, letras y caracteres especiales, no menor de ocho (8) caracteres.

5. Cambio de contraseñas

   a. Todas las contraseñas de nivel administrativo se deben cambiar como mínimo cada cuatro (4) meses.

   b. Todas las contraseñas de usuarios se deben cambiar como mínimo cada seis (6) meses.

6. Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

7. Deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

8. Si se va a disponer de equipo que contiene información sensitiva deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las facilidades de la Agencia.

9. Las agencias deberán establecer los controles necesarios para asegurar aquellos equipos que han estado fuera de la agencia no represente un riesgo a sus sistemas. Ello incluye revisar y requerir auditorías de dichos equipos al ingresarlos a sus sistemas.

10. Las agencias deberán establecer los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde sus redes internas hacia otros sistemas de información externos.

11. Cada agencia será responsable de diseñar y mantener la seguridad de sus sistemas de información.

12. Se recomienda a las agencias realizar auditorías de seguridad al menos una vez al año.

F. Manejo de Incidentes

1. Las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluyendo límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta.

2. Todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

G. Manejo de Cambios

Cada agencia es responsable de diseñar procedimientos que permitan que los cambios a la seguridad de los sistemas sean realizados y documentados adecuadamente y que esta documentación a su vez sea asegurada.

H. Adiestramientos

1. Cada agencia es responsable de proveer adiestramientos al personal para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

2. El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y mantenerse actualizado sobre los aspectos de seguridad de sus áreas.

3. Se deben proveer mecanismos para capacitar a todos los empleados periódicamente.

I. Controles Físicos

1. El acceso a las facilidades de sistemas de información deberá estar controlado para que solo el personal autorizado pueda utilizarlas.

2. Cualquier equipo usado fuera de la agencia deberá estar autorizado por la gerencia o persona designada, y deberá haber procedimientos para controlar su utilización.

J. Internet

1. La comunicación con Internet desde adentro de la agencia deberá estar controlada por un *"firewall"*. Las agencias deberán desarrollar las políticas de uso de Internet y de correo electrónico (ver Política Núm. ATI-008, USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO) y utilizar el *firewall* (Servidor de Seguridad de Computadoras y Redes)(ver Política Núm. ATI-014, MANEJO DE LOS *FIREWALLS)* como uno de los mecanismos de control de esas políticas.

2. Las agencias establecerán controles de uso de internet para evitar el uso no adecuado del mismo. Se debe establecer como mínimo una política que bloquee el acceso a páginas pornográficas.

3. Si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la agencia (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, autorización, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.

4. Si se determina que hay datos sensitivos pasando a través de redes que no son seguras (como Internet o redes inalámbricas), se deberán tener los controles necesarios para garantizar la confidencialidad, como por ejemplo, el uso de cifrado.

5. Toda agencia que desarrolle un programa de aplicación para brindar servicios de la agencia a los ciudadanos a través de Internet deberá asegurarse de que toma en consideración los siguientes elementos en su estudio de viabilidad para la implantación del programa:

   a. Un diseño de seguridad.

   b. La integración de mejores prácticas de seguridad en programación para evitar el acceso no autorizado y/o malicioso a través de Internet.

   c. Un *"firewall"* que permita controlar el acceso al programa desde Internet.

   d. Asegurar que si el servicio que está disponible maneja datos sensitivos, sea instalado en una red alterna. En este caso, el programa deberá funcionar en una red alterna y segura que permita el acceso desde Internet y a la misma vez permita un acceso controlado a la red interna para el intercambio controlado y monitoreado de datos.

   e. Cerciorarse que si el servicio ofrecido a través de Internet maneja datos sensitivos existe implantado un sistema de detección/prevención de intrusos.

K. Servicios Suministrados por Contratistas

1. Es necesario mantener la seguridad de los sistemas de información aun cuando el manejo y el control de parte o de todos los procesos ha sido delegado a un tercero.

2. Los contratos con terceros deberán incluir la salvaguarda de los activos sensitivos, especialmente cuando los servicios contratados incluyen el manejo de estos activos fuera de las facilidades de la Agencia.

3. Si el servicio suministrado por terceros incluye que parte de los procesos corren en las instalaciones de los contratistas, deberán establecerse controles de mutuo acuerdo para proteger la información y estos acuerdos deberán ser parte del contrato.

4. Todo contrato con terceros deberá incluir la certificación de revisión de seguridad conocida como SOC-2 y la misma debe estar vigente.

EXENCIONES

Ninguna

DEFINICIONES

Adware – Es un programa que se instala inadvertidamente en una computadora y que su principal propósito es desplegar ante el usuario anuncios y propaganda pero también puede tener un comportamiento como el *spyware*.

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Autenticación – Es el proceso por el cual una persona presenta información que lo identifica ante un sistema de información y el sistema compara la información contra su base de datos para validarla.

Autorización – Es el proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.

Confidencialidad – Es la característica que se le da a una información para que pueda ser vista solamente por personas autorizadas.

Cifrado – Es el proceso por el cual unos datos se transforman en información no entendible por aquellos que no están autorizados a verlos.

Datos sensitivos – Datos que contienen información financiera, de los ciudadanos, de los recursos humanos u otra información crítica para la operación de la agencia.

Firewall (Servidor de Seguridad de Computadoras y Redes) – Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que residen en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

Integridad – Es el proceso que permite proteger información de alteraciones indebidas.

Programa – Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber **programas de sistema** que controlan el funcionamiento de las computadoras y de las redes de informática y también **programas de aplicación** que facilitan y/o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

Ransomeware – Es un programa que se instala inadvertidamente en una computadora y está diseñado para bloquear accesos a los sistemas hasta que se pague una suma de dinero.

Seguridad de Informática – Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información; protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

Sistema de Detección y Prevención de Intrusos – Es un programa que reside en una computadora o en un equipo especializado y que permite detectar ataques o intentos indebidos de acceso hacia un sistema de información.

Spyware– Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

ANEJOS

Ninguno

REFERENCIAS

Ley 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico".
Política Núm. ATI-008, sobre USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO, revisada el 7 de noviembre e de 2016
Política Núm. ATI-014, MANEJO DE LOS *FIREWALLS,* del 7 de noviembre de 2016

ANTECEDENTE

Política Núm. TIG-003, conocida como Seguridad de los Sistemas de Información, revisada el 12 de septiembre de 2007.

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-004

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: Servicios de Tecnología

DESCRIPCIÓN

Esta política consiste de directivas generales que permitirán a las agencias conocer los servicios de tecnología que ofrece la Oficina de Gerencia y Presupuesto (OGP), así como las condiciones y responsabilidades que éstas tendrán que cumplir para recibir los servicios.

La misma deroga y sustituye la Política Núm. TIG-004, conocida como Servicios de Tecnología, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, debe proveer servicios de apoyo técnico, de almacenamiento de datos y de acceso a Internet a las agencias gubernamentales. *Id.,* Artículo 5, inciso (l). La OGP tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.,* Art. 6, inciso (l), (i) y (iii). *Id.,* Art. 7, incisos (a) y (b). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a las agencias de la Rama Ejecutiva y aquellas entidades correspondientes que utilicen los servicios de la Red Interagencial del Estado Libre Asociado de Puerto Rico.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con los servicios de tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes a los servicios de tecnologías que ofrece la OGP.

POLÍTICA

Todas las agencias cubiertas por esta política deberán cumplir las normas y procedimientos relativos al uso de las tecnologías de la información que se detallan a continuación. Estas políticas tienen como meta obtener los beneficios de los adelantos en la tecnología, mejorar las relaciones interagenciales y la reducción de costos operacionales.

SOLICITUD DE SERVICIOS A LAS AGENCIAS

Los servicios aquí delineados se solicitarán a través de Apoyo Técnico (AT) de la ATI, a través del correo electrónico support@ogp.pr.gov o al teléfono (787) 725-9420, extensiones 2438, 2440 y 2457. Los tiempos de respuesta varían dependiendo de la complejidad del servicio solicitado.

1. Adiestramientos: Adiestramientos en varios temas relacionados con tecnología se ofrecerán por solicitud previa. Para detalles relacionados a fechas, disponibilidad y registros favor de comunicarse con el AT o enviar petición a support@ogp.pr.gov.

2. Licencias de programas: Servicio de distribución de licencias adquiridas bajo contratos globales. Para obtener información sobre las licencias disponibles y sus condiciones puede comunicarse a través de support@ogp.pr.gov.

3. Internet: Servicio de acceso al Internet a través de la Red Interagencial. El tipo de acceso al Internet dependerá de la localización geográfica, disponibilidad de líneas y justificación de negocios. Para solicitar este servicio debe escribir un correo electrónico a support@ogp.pr.gov o llamar al (787) 725-9420 extensiones 2438, 2440 y 2457.

4. Web Hosting: Servicios asociados al almacenaje, la conectividad y la publicación de páginas de Internet de las agencias, que estén dentro de la plataforma asignada. El servicio se obtiene a través de una petición a support@ogp.pr.gov.

5. Registro de Dominio: Servicio de registro y mantenimiento de dominios que se ofrece a las entidades gubernamentales que deseen tener una presencia en la Internet que corresponda a la política pública establecida en la Ley de Gobierno Electrónico (Ley 151 - 2004). Para solicitar este servicio debe escribir un correo electrónico a support@ogp.pr.gov o llamar al (787) 725-9420 extensiones 2438, 2440 y 2457

6. Administración de IP: Proceso de otorgar direcciones de IP a cualquier entidad gubernamental que esté conectada a la Red Interagencial. Este servicio se brinda por medio de una solicitud a support@ogp.pr.gov.

7. Administración de Antivirus: Servicio de configuración y administración de la Consola Central de Antivirus que permite revisar y actualizar la consola de antivirus de la entidad gubernamental conectada a la Red Interagencial. Este servicio lo brinda el AT.

8. Exchange Support-Office 365: Servicio de apoyo técnico a productos de MS Exchange Server relacionados con el envío y recibo de correo electrónico. Sólo se provee asistencia técnica a algunas versiones del producto de correo electrónico de MS Exchange. Para mayor información comuníquese con support@ogp.pr.gov.

9. Firewall Support (ISA): Servicio de asistencia técnica sólo a algunas versiones del "Firewall" (Servidor de Seguridad de Computadoras y Redes) del ISA Server. Para obtener la lista de estos productos y versiones apoyadas, se deberá solicitar a través de support@ogp.pr.gov.

10. Antivirus Support: Apoyo técnico a algunas versiones de los productos Symantec Antivirus Console y Symantec Mail Security for Exchange que pertenecen al paquete de productos de Symantec Antivirus.

11. Servicios "en la nube": dependiendo los términos contractuales, los cuales pueden variar. Las agencias podrán beneficiarse de usar servicios "en la nube". Dado que pueden variar, se debe cotejar con AT para conocer disponibilidad.

12. Portales: servicio de creación y administración de portales en el cual la Agencia es responsable del contenido.

PROCEDIMIENTO

A. Responsabilidades del Área de Tecnologías de Información (ATI):

Prestación e Interrupción de Servicios

1. ATI ofrece sus servicios de lunes a viernes de 7:30 AM – 5:30 PM, excepto en días feriados.

2. ATI efectuará labores de mantenimiento, procurando que el impacto de estas labores sea mínimo. Las labores de mantenimiento podrían implicar que en algunas ocasiones los servicios ofrecidos no estén disponibles. En tales situaciones, ATI notificará a las agencias mediante la cuenta de correo electrónico support@ogp.pr.gov.

3. Hasta donde sea posible, no se programarán labores de mantenimiento en las siguientes fechas críticas:

   a) Durante las últimas dos semanas antes del fin del año fiscal y del año natural.

   b) Durante las primeras dos semanas al principio del año fiscal y del año natural.

   c) Eventos que conlleven un elevado uso de la infraestructura tales como la radicación de planillas en línea entre otros.

4. ATI notificará a los Directores de Sistemas de Información de las agencias conectadas a la Red Interagencial, a través de correo electrónico y del Portal de la Oficina de Gerencia y Presupuesto en la dirección de Internet: ogp.pr.gov, el itinerario para las interrupciones planificadas y las no planificadas.

5. Los servicios incluidos en esta política podrían sufrir cambios por causas mayores fuera del alcance de ATI, así como por problemas causados por el servicio brindado por contratos externos.

6. ATI tendrá un Plan de Recuperación por Desastre para la Red Interagencial.

Seguridad

1. ATI será responsable por establecer y aplicar las políticas necesarias para garantizar la seguridad en la Red Interagencial. ATI también será responsable de toda la seguridad en cuanto a equipo (hardware), programación (software), datos y usuarios que acceden directamente la Red Interagencial. Esto incluye el hacer y retener copias de resguardo ("backup") de los datos y sistemas con la frecuencia que sea necesaria.

2. ATI vigilará el acceso de los usuarios a la Red Interagencial, lo que incluye pero no lo limita a: cuentas de acceso, acceso a servidores, acceso a equipo y programación especializada. Para hacer esto adecuadamente, ATI utilizará los mecanismos necesarios para detectar, prever y reportar accesos no autorizados a la red (ver Política de Seguridad ATI-003).

3. ATI tendrá una base datos donde documentará la información de los usuarios que acceden sus sistemas. Está información incluirá quiénes pueden accederlos y el tipo de acceso que tienen.

4. ATI será responsable de la administración y actualización de la Consola Central de Antivirus y el "firewall" de la Red Interagencial.

Cancelación de los Servicios

1. ATI se reserva el derecho de descontinuar los servicios a la Agencia si la conexión de la Agencia pone en peligro la seguridad e integridad de los servicios ofrecidos por ATI.

B. Responsabilidades de la Agencia:

Planificación

1. La Agencia será responsable de planificar los servicios internos que brinda, así como los métodos de apoyo a sus usuarios.

2. La Agencia, como parte de un proceso de actualización y optimización, verificará sus sistemas anualmente para identificar posibles modificaciones a los mismos. De esa manera, se garantiza un servicio de alta calidad. Estas verificaciones se utilizarán también en la creación del presupuesto anual de tecnologías.

3. La Agencia obtendrá la aprobación de ATI para proyectos de Tecnología de Información previo a su contratación.

4. La Agencia notificará a ATI de cualquier proyecto relacionado con tecnologías de información que vaya a comenzar. Esto incluye pero no se limita a: proyectos realizados con fondos estatales, federales, donaciones y otros. Estos proyectos tienen que ser registrados en la aplicación LEAN-Tech, https://lean.pr.gov. *Véase* Política Núm. ATI-001, Legado Estratégico Anual Tecnológico.

5. La Agencia será responsable de comunicar a ATI de cualquier evento crítico que genere alto volumen de uso de la Red y el periodo en el cual ocurrirá, con por lo menos quince (15) días laborables de antelación, si interesa asegurar la disponibilidad y continuidad del servicio. Para ello, se comunicará con Apoyo Técnico.

6. La Agencia deberá hacer y presentar un análisis de Costo Total de Administración en el cual se evalúe no solo los costos de adquisición, de implementación, educación y manejo de cambios sino de Administración, Mantenimiento, Política de manejo de parchos/upgrades, plan de Continuidad de Negocios y Recuperación de Desastres.

Adquisición y Manejo de Equipo

1. Todo equipo que adquiera la Agencia cumplirá con los requerimientos mínimos detallados en la Política de Adquisición de Equipo para Sistemas Computadorizados de Información (ATI-010).

2. La Agencia adquirirá todo el equipo que utilice en su red interna. Esto incluye pero no se limita a: servidores, computadoras para usuarios, "hubs", cables, impresoras, y otros.

Programación

1. La Agencia adquirirá todas las plataformas necesarias para el funcionamiento de su red interna. Las mismas deberán cumplir con las mejores prácticas de programación de la industria.

2. La Agencia será responsable de la programación que requieran las computadoras de sus usuarios.

3. La Agencia deberá seguir las recomendaciones sugeridas en la guía de Diseño y Contenido de Páginas Web, si planifica crear un sitio de Internet y cumplir con la Política de Desarrollo y Mantenimiento de Sitios Web Agenciales (ATI-002).
4. La Agencia deberá analizar y crear un plan, con el apropiado análisis de costos, de cómo compara soluciones funcionales del mercado que requieran poca adecuación, mucha adecuación y programas desarrollados totalmente y únicamente para la Agencia.

Apoyo y Mantenimiento a Sistemas Internos

1. El personal de la oficina de tecnologías de información de la Agencia será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos.

2. El mantenimiento incluirá pero no se limitará a: reparación de equipo, cambio de contraseñas, instalación de programas, mudanzas de equipo, mejoras (actualización), creación de cuentas, mantenimiento de los buzones de correo electrónico y otros.

3. La Agencia verificará el funcionamiento del equipo que compone sus sistemas. Ejemplos del equipo son, pero no se limitan a: controladores primarios y secundarios, "hubs", "switches" y servidores.

4. La Agencia revisará regularmente sus sistemas para verificar que estén funcionando adecuadamente.

Recuperación de Desastres

1. La Agencia será responsable de asegurar la continuidad de sus operaciones mediante un Plan de Recuperación por Desastre desarrollado de acuerdo a la Política de Seguridad (ATI-003). ATI no proveerá un Plan de Recuperación por Desastre a la Agencias.

2. El Plan de Recuperación por Desastre abarcará todo lo relacionado a programación (software), equipo (hardware), datos y facilidades físicas de la Agencia.

Comunicación y Educación a los Usuarios

1. El departamento de tecnologías de información de la Agencia le comunicará a sus usuarios aquellos asuntos establecidos en las políticas que les apliquen. Una copia de esa comunicación se colocará en un lugar accesible a todos los empleados de la Agencia.

2. El departamento de tecnologías de información de la Agencia se asegurará que sus empleados utilicen los sistemas de información de acuerdo a las políticas de sistemas de información. Para más detalles, vea la Política de Uso de Sistemas de Información, de la Internet y del Correo Electrónico (ATI-008).

Solicitudes de Servicio

1. El Oficial Principal de Informática (OPI) de la Agencia (o un representante autorizado) será la persona autorizada para generar una petición de servicio a la División de Asistencia Técnica.

2. Las solicitudes de servicios se generará por dos medios:
   a. Correo Electrónico: support@ogp.pr.gov
   b. Teléfono: (787) 725-9420 Ext. 2438, 2440 y 2457

3. Cada incidente reportado o servicio solicitado recibirá un número de caso que le permitirá a la Agencia dar seguimiento a su solicitud.

   a. En caso de que el problema o situación reportada por la Agencia esté fuera del alcance de los servicios de la División de Asistencia Técnica, se referirá la Agencia

hacia recursos externos que tengan el peritaje para resolverlo. La contratación de estos servicios será responsabilidad de la Agencia.

b. La División de Asistencia Técnica no proveerá apoyo a problemas de programación, ni de funcionamiento de servidores, ni a ningún otro equipo relacionado a los sistemas internos de la Agencia (ver sección de Servicios a Agencias, Servicios a Municipios).

Seguridad

1. La Agencia se responsabilizará por el cumplimiento de la Política de Seguridad (ATI-003) establecida por ATI. Es además responsable de toda la seguridad en cuanto a equipo (hardware), programación (software), datos y usuarios. Esto incluye el hacer copias de resguardo ("backup") de los datos y sistemas, con la frecuencia que sea necesaria.

2. La Agencia administrará el acceso de los usuarios a sus sistemas, lo que incluye pero no lo limita a: cuentas de acceso, acceso a servidores, acceso a impresoras, acceso a equipo y programación especializada. Para hacer esto adecuadamente, la Agencia utilizará los mecanismos necesarios para detectar, prever y reportar accesos no autorizados a la red (ver Política de Seguridad ATI-003).

3. La Agencia tendrá una base datos donde documentará la información de los usuarios que acceden sus sistemas. Esta información incluirá quiénes pueden accederlos y el tipo de acceso que tienen.

4. La Agencia será responsable de la administración apropiada y de la actualización del sistema contra virus y el "firewall" (Servidor de Seguridad de Computadoras y Redes), en cumplimiento con la Política de Seguridad ATI-003).

5. La Agencia se asegurará que al momento de disponer del equipo, el mismo no contenga programación y/o información confidencial o sensitiva. Antes de disponer del mismo, se hará un proceso de eliminación de programas e información, según lo describe la Política de Disposición de Equipo y Licencias, ATI-007.

Privacidad

a. La OGP-ATI sólo ofrecerá información almacenada en sus facilidades a las agencias dueñas de dicha información. Cualquier agencia que interese información que pertenece a otra agencia, deberá hacer su petición directamente a la agencia correspondiente.

CUMPLIMIENTO DE LAS POLÍTICAS

El no cumplir con las políticas relacionadas a los sistemas de información podría conllevar sanciones y/o la suspensión de los servicios recibidos.

EXENCIONES

Si una agencia desea obtener una exención para desviarse de la política aquí descrita deberá someter una justificación escrita a la OGP por conducto del Director Asociado de ATI, quien evaluará los méritos y notificará de su decisión por escrito a la Agencia.

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Apoyo Técnico - Unidad especializada responsable de dar apoyo a las agencias cuando el equipo y/o programas conectados a la Red Interagencial no funcionan adecuadamente. Esta división está ubicada en el cuarto piso del edificio donde se encuentra la Oficina de Gerencia y Presupuesto en el Viejo San Juan, Calle Cruz 254, Esquina Tetuán . Su teléfono es: (787) 725-9420 extensiones 2438, 2440 y 2457.

Firewall (Equipo de Seguridad de Computadoras y Redes) - Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que reside en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

Portal de Apoyo Interagencial - Sitio en la Internet en donde se publica información de utilidad para las agencias que incluye un Canal de Información de acceso exclusivo a la comunidad de IT. La información incluye documentos de apoyo técnico a sistemas de información, políticas, formularios y otros.

Solicitud Servicio - que requiere que la agencia complete un proceso de solicitud para recibirlo.

ANEJOS

Ninguno

REFERENCIAS

Estándares para Portales
Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-001, Legado Estratégica Anual Tecnológico (LEAN-Tech), revisada el 7 de noviembre de 2016
Política Núm. ATI-002, Desarrollo y Mantenimiento de Sitios Web Agenciales (WEB SITES), revisada el 7 de noviembre de 2016
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-007, Disposición de Equipo y Licencias, revisada el 7 de noviembre de 2016
Política Núm. ATI-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico, revisada el 7 de noviembre de 2016
Política Núm. ATI-010, Adquisición de Equipos para Sistemas Computadorizados de Información, revisada el 7 de noviembre de 2016

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-004

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: Servicios de Tecnología

DESCRIPCIÓN

Esta política consiste de directivas generales que permitirán a las agencias conocer los servicios de tecnología que ofrece la Oficina de Gerencia y Presupuesto (OGP), así como las condiciones y responsabilidades que éstas tendrán que cumplir para recibir los servicios.

La misma deroga y sustituye la Política Núm. TIG-004, conocida como Servicios de Tecnología, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, debe proveer servicios de apoyo técnico, de almacenamiento de datos y de acceso a Internet a las agencias gubernamentales. *Id.,* Artículo 5, inciso (l). La OGP tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.,* Art. 6, inciso (l), (i) y (lii). *Id.,* Art. 7, incisos (a) y (b). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a las agencias de la Rama Ejecutiva y aquellas entidades correspondientes que utilicen los servicios de la Red Interagencial del Estado Libre Asociado de Puerto Rico.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con los servicios de tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes a los servicios de tecnologías que ofrece la OGP.

POLÍTICA

Todas las agencias cubiertas por esta política deberán cumplir las normas y procedimientos relativos al uso de las tecnologías de la información que se detallan a continuación. Estas políticas tienen como meta obtener los beneficios de los adelantos en la tecnología, mejorar las relaciones interagenciales y la reducción de costos operacionales.

SOLICITUD DE SERVICIOS A LAS AGENCIAS

Los servicios aquí delineados se solicitarán a través de Apoyo Técnico (AT) de la ATI, a través del correo electrónico support@ogp.pr.gov o al teléfono (787) 725-9420, extensiones 2438, 2440 y 2457. Los tiempos de respuesta varían dependiendo de la complejidad del servicio solicitado.

1. Adiestramientos: Adiestramientos en varios temas relacionados con tecnología se ofrecerán por solicitud previa. Para detalles relacionados a fechas, disponibilidad y registros favor de comunicarse con el AT o enviar petición a support@ogp.pr.gov.

2. Licencias de programas: Servicio de distribución de licencias adquiridas bajo contratos globales. Para obtener información sobre las licencias disponibles y sus condiciones puede comunicarse a través de support@ogp.pr.gov.

3. Internet: Servicio de acceso al Internet a través de la Red Interagencial. El tipo de acceso al Internet dependerá de la localización geográfica, disponibilidad de líneas y justificación de negocios. Para solicitar este servicio debe escribir un correo electrónico a support@ogp.pr.gov o llamar al (787) 725-9420 extensiones 2438, 2440 y 2457.

4. Web Hosting: Servicios asociados al almacenaje, la conectividad y la publicación de páginas de Internet de las agencias, que estén dentro de la plataforma asignada. El servicio se obtiene a través de una petición a support@ogp.pr.gov.

5. Registro de Dominio: Servicio de registro y mantenimiento de dominios que se ofrece a las entidades gubernamentales que deseen tener una presencia en la Internet que corresponda a la política pública establecida en la Ley de Gobierno Electrónico (Ley 151 - 2004). Para solicitar este servicio debe escribir un correo electrónico a support@ogp.pr.gov o llamar al (787) 725-9420 extensiones 2438, 2440 y 2457

6. Administración de IP: Proceso de otorgar direcciones de IP a cualquier entidad gubernamental que esté conectada a la Red Interagencial. Este servicio se brinda por medio de una solicitud a support@ogp.pr.gov.

7. Administración de Antivirus: Servicio de configuración y administración de la Consola Central de Antivirus que permite revisar y actualizar la consola de antivirus de la entidad gubernamental conectada a la Red Interagencial. Este servicio lo brinda el AT.

8. Exchange Support-Office 365: Servicio de apoyo técnico a productos de MS Exchange Server relacionados con el envío y recibo de correo electrónico. Sólo se provee asistencia técnica a algunas versiones del producto de correo electrónico de MS Exchange. Para mayor información comuníquese con support@ogp.pr.gov.

9. Firewall Support (ISA): Servicio de asistencia técnica sólo a algunas versiones del "Firewall" (Servidor de Seguridad de Computadoras y Redes) del ISA Server. Para obtener la lista de estos productos y versiones apoyadas, se deberá solicitar a través de support@ogp.pr.gov.

10. Antivirus Support: Apoyo técnico a algunas versiones de los productos Symantec Antivirus Console y Symantec Mail Security for Exchange que pertenecen al paquete de productos de Symantec Antivirus.

11. Servicios "en la nube": dependiendo los términos contractuales, los cuales pueden variar. Las agencias podrán beneficiarse de usar servicios "en la nube". Dado que pueden variar, se debe cotejar con AT para conocer disponibilidad.

12. Portales: servicio de creación y administración de portales en el cual la Agencia es responsable del contenido.

PROCEDIMIENTO

A. Responsabilidades del Área de Tecnologías de Información (ATI):

Prestación e Interrupción de Servicios

1. ATI ofrece sus servicios de lunes a viernes de 7:30 AM – 5:30 PM, excepto en días feriados.

2. ATI efectuará labores de mantenimiento, procurando que el impacto de estas labores sea mínimo. Las labores de mantenimiento podrían implicar que en algunas ocasiones los servicios ofrecidos no estén disponibles. En tales situaciones, ATI notificará a las agencias mediante la cuenta de correo electrónico support@ogp.pr.gov.

3. Hasta donde sea posible, no se programarán labores de mantenimiento en las siguientes fechas críticas:

   a) Durante las últimas dos semanas antes del fin del año fiscal y del año natural.

   b) Durante las primeras dos semanas al principio del año fiscal y del año natural.

   c) Eventos que conlleven un elevado uso de la infraestructura tales como la radicación de planillas en línea entre otros.

4. ATI notificará a los Directores de Sistemas de Información de las agencias conectadas a la Red Interagencial, a través de correo electrónico y del Portal de la Oficina de Gerencia y Presupuesto en la dirección de Internet: ogp.pr.gov, el itinerario para las interrupciones planificadas y las no planificadas.

5. Los servicios incluidos en esta política podrían sufrir cambios por causas mayores fuera del alcance de ATI, así como por problemas causados por el servicio brindado por contratos externos.

6. ATI tendrá un Plan de Recuperación por Desastre para la Red Interagencial.

Seguridad

1. ATI será responsable por establecer y aplicar las políticas necesarias para garantizar la seguridad en la Red Interagencial. ATI también será responsable de toda la seguridad en cuanto a equipo (hardware), programación (software), datos y usuarios que acceden directamente la Red Interagencial. Esto incluye el hacer y retener copias de resguardo ("backup") de los datos y sistemas con la frecuencia que sea necesaria.

2. ATI vigilará el acceso de los usuarios a la Red Interagencial, lo que incluye pero no lo limita a: cuentas de acceso, acceso a servidores, acceso a equipo y programación especializada. Para hacer esto adecuadamente, ATI utilizará los mecanismos necesarios para detectar, prever y reportar accesos no autorizados a la red (ver Política de Seguridad ATI-003).

3. ATI tendrá una base datos donde documentará la información de los usuarios que acceden sus sistemas. Está información incluirá quiénes pueden accederlos y el tipo de acceso que tienen.

4. ATI será responsable de la administración y actualización de la Consola Central de Antivirus y el "firewall" de la Red Interagencial.

Cancelación de los Servicios

1. ATI se reserva el derecho de descontinuar los servicios a la Agencia si la conexión de la Agencia pone en peligro la seguridad e integridad de los servicios ofrecidos por ATI.

B. Responsabilidades de la Agencia:

Planificación

1. La Agencia será responsable de planificar los servicios internos que brinda, así como los métodos de apoyo a sus usuarios.

2. La Agencia, como parte de un proceso de actualización y optimización, verificará sus sistemas anualmente para identificar posibles modificaciones a los mismos. De esa manera, se garantiza un servicio de alta calidad. Estas verificaciones se utilizarán también en la creación del presupuesto anual de tecnologías.

3. La Agencia obtendrá la aprobación de ATI para proyectos de Tecnología de Información previo a su contratación.

4. La Agencia notificará a ATI de cualquier proyecto relacionado con tecnologías de información que vaya a comenzar. Esto incluye pero no se limita a: proyectos realizados con fondos estatales, federales, donaciones y otros. Estos proyectos tienen que ser registrados en la aplicación LEAN-Tech, https://lean.pr.gov. *Véase* Política Núm. ATI-001, Legado Estratégico Anual Tecnológico.

5. La Agencia será responsable de comunicar a ATI de cualquier evento crítico que genere alto volumen de uso de la Red y el periodo en el cual ocurrirá, con por lo menos quince (15) días laborables de antelación, si interesa asegurar la disponibilidad y continuidad del servicio. Para ello, se comunicará con Apoyo Técnico.

6. La Agencia deberá hacer y presentar un análisis de Costo Total de Administración en el cual se evalúe no solo los costos de adquisición, de implementación, educación y manejo de cambios sino de Administración, Mantenimiento, Política de manejo de parchos/upgrades, plan de Continuidad de Negocios y Recuperación de Desastres.

Adquisición y Manejo de Equipo

1. Todo equipo que adquiera la Agencia cumplirá con los requerimientos mínimos detallados en la Política de Adquisición de Equipo para Sistemas Computadorizados de Información (ATI-010).

2. La Agencia adquirirá todo el equipo que utilice en su red interna. Esto incluye pero no se limita a: servidores, computadoras para usuarios, "hubs", cables, impresoras, y otros.

Programación

1. La Agencia adquirirá todas las plataformas necesarias para el funcionamiento de su red interna. Las mismas deberán cumplir con las mejores prácticas de programación de la industria.

2. La Agencia será responsable de la programación que requieran las computadoras de sus usuarios.

3. La Agencia deberá seguir las recomendaciones sugeridas en la guía de Diseño y Contenido de Páginas Web, si planifica crear un sitio de Internet y cumplir con la Política de Desarrollo y Mantenimiento de Sitios Web Agenciales (ATI-002).
4. La Agencia deberá analizar y crear un plan, con el apropiado análisis de costos, de cómo compara soluciones funcionales del mercado que requieran poca adecuación, mucha adecuación y programas desarrollados totalmente y únicamente para la Agencia.

Apoyo y Mantenimiento a Sistemas Internos

1. El personal de la oficina de tecnologías de información de la Agencia será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos.

2. El mantenimiento incluirá pero no se limitará a: reparación de equipo, cambio de contraseñas, instalación de programas, mudanzas de equipo, mejoras (actualización), creación de cuentas, mantenimiento de los buzones de correo electrónico y otros.

3. La Agencia verificará el funcionamiento del equipo que compone sus sistemas. Ejemplos del equipo son, pero no se limitan a: controladores primarios y secundarios, "hubs", "switches" y servidores.

4. La Agencia revisará regularmente sus sistemas para verificar que estén funcionando adecuadamente.

Recuperación de Desastres

1. La Agencia será responsable de asegurar la continuidad de sus operaciones mediante un Plan de Recuperación por Desastre desarrollado de acuerdo a la Política de Seguridad (ATI-003). ATI no proveerá un Plan de Recuperación por Desastre a la Agencias.

2. El Plan de Recuperación por Desastre abarcará todo lo relacionado a programación (software), equipo (hardware), datos y facilidades físicas de la Agencia.

Comunicación y Educación a los Usuarios

1. El departamento de tecnologías de información de la Agencia le comunicará a sus usuarios aquellos asuntos establecidos en las políticas que les apliquen. Una copia de esa comunicación se colocará en un lugar accesible a todos los empleados de la Agencia.

2. El departamento de tecnologías de información de la Agencia se asegurará que sus empleados utilicen los sistemas de información de acuerdo a las políticas de sistemas de información. Para más detalles, vea la Política de Uso de Sistemas de Información, de la Internet y del Correo Electrónico (ATI-008).

Solicitudes de Servicio

1. El Oficial Principal de Informática (OPI) de la Agencia (o un representante autorizado) será la persona autorizada para generar una petición de servicio a la División de Asistencia Técnica.

2. Las solicitudes de servicios se generará por dos medios:
   a. Correo Electrónico: support@ogp.pr.gov
   b. Teléfono: (787) 725-9420 Ext. 2438, 2440 y 2457

3. Cada incidente reportado o servicio solicitado recibirá un número de caso que le permitirá a la Agencia dar seguimiento a su solicitud.

   a. En caso de que el problema o situación reportada por la Agencia esté fuera del alcance de los servicios de la División de Asistencia Técnica, se referirá la Agencia

hacia recursos externos que tengan el peritaje para resolverlo. La contratación de estos servicios será responsabilidad de la Agencia.

b. La División de Asistencia Técnica no proveerá apoyo a problemas de programación, ni de funcionamiento de servidores, ni a ningún otro equipo relacionado a los sistemas internos de la Agencia (ver sección de Servicios a Agencias, Servicios a Municipios).

Seguridad

1. La Agencia se responsabilizará por el cumplimiento de la Política de Seguridad (ATI-003) establecida por ATI. Es además responsable de toda la seguridad en cuanto a equipo (hardware), programación (software), datos y usuarios. Esto incluye el hacer copias de resguardo ("backup") de los datos y sistemas, con la frecuencia que sea necesaria.

2. La Agencia administrará el acceso de los usuarios a sus sistemas, lo que incluye pero no lo limita a: cuentas de acceso, acceso a servidores, acceso a impresoras, acceso a equipo y programación especializada. Para hacer esto adecuadamente, la Agencia utilizará los mecanismos necesarios para detectar, prever y reportar accesos no autorizados a la red (ver Política de Seguridad ATI-003).

3. La Agencia tendrá una base datos donde documentará la información de los usuarios que acceden sus sistemas. Esta información incluirá quiénes pueden accederlos y el tipo de acceso que tienen.

4. La Agencia será responsable de la administración apropiada y de la actualización del sistema contra virus y el "firewall" (Servidor de Seguridad de Computadoras y Redes), en cumplimiento con la Política de Seguridad ATI-003).

5. La Agencia se asegurará que al momento de disponer del equipo, el mismo no contenga programación y/o información confidencial o sensitiva. Antes de disponer del mismo, se hará un proceso de eliminación de programas e información, según lo describe la Política de Disposición de Equipo y Licencias, ATI-007.

Privacidad

a. La OGP-ATI sólo ofrecerá información almacenada en sus facilidades a las agencias dueñas de dicha información. Cualquier agencia que interese información que pertenece a otra agencia, deberá hacer su petición directamente a la agencia correspondiente.

CUMPLIMIENTO DE LAS POLÍTICAS

El no cumplir con las políticas relacionadas a los sistemas de información podría conllevar sanciones y/o la suspensión de los servicios recibidos.

EXENCIONES

Si una agencia desea obtener una exención para desviarse de la política aquí descrita deberá someter una justificación escrita a la OGP por conducto del Director Asociado de ATI, quien evaluará los méritos y notificará de su decisión por escrito a la Agencia.

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Apoyo Técnico - Unidad especializada responsable de dar apoyo a las agencias cuando el equipo y/o programas conectados a la Red Interagencial no funcionan adecuadamente. Esta división está ubicada en el cuarto piso del edificio donde se encuentra la Oficina de Gerencia y Presupuesto en el Viejo San Juan, Calle Cruz 254, Esquina Tetuán . Su teléfono es: (787) 725-9420 extensiones 2438, 2440 y 2457.

Firewall (Equipo de Seguridad de Computadoras y Redes) - Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que reside en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

Portal de Apoyo Interagencial - Sitio en la Internet en donde se publica información de utilidad para las agencias que incluye un Canal de Información de acceso exclusivo a la comunidad de IT. La información incluye documentos de apoyo técnico a sistemas de información, políticas, formularios y otros.

Solicitud Servicio - que requiere que la agencia complete un proceso de solicitud para recibirlo.

ANEJOS

Ninguno

REFERENCIAS

Estándares para Portales
Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-001, Legado Estratégica Anual Tecnológico (LEAN-Tech), revisada el 7 de noviembre de 2016
Política Núm. ATI-002, Desarrollo y Mantenimiento de Sitios Web Agenciales (WEB SITES), revisada el 7 de noviembre de 2016
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-007, Disposición de Equipo y Licencias, revisada el 7 de noviembre de 2016
Política Núm. ATI-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico, revisada el 7 de noviembre de 2016
Política Núm. ATI-010, Adquisición de Equipos para Sistemas Computadorizados de Información, revisada el 7 de noviembre de 2016

OGP
OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-005 **FECHA DE EFECTIVIDAD:** 7 de noviembre de 2016

TEMA: Geotecnologías: {Geodesia, Cartografía, Sistemas de Información Geográfica, Teledetección, Sistemas de posicionamiento global (GPS)}

DESCRIPCIÓN

El propósito de este documento es establecer una serie de estándares y guías para las actividades relacionadas a la información geográfica y geotecnologías. Estas ciencias engloban disciplinas tales como geodesia, cartografía, sistemas de información geográfica, teledetección y GPS.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico que, al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico", utilizan información geográfica en sus distintas manifestaciones, oficinas que poseen programas SIG, Cartografía digital, Teledetección, GPS, en sus sistemas computarizados de información, independientemente de su costo y origen de los fondos. La misma no sustituye aquellas guías y directrices para la administración del Sistema de Información Geoespacial del Estado Libre Asociado de Puerto Rico, el Mapa Multifinalitario y Multidisciplinario de Puerto Rico, y Sistema de Coordenadas Planas Estatales, a ser emitidas por la Oficina de Agrimensura de Oficina de Agrimensura de Puerto Rico, adscrita a la Oficina de Gerencia de Permisos (OGPe), de conformidad con la Ley 184-2014, conocida como "Ley del Sistema de Información Geoespacial del Estado Libre Asociado de Puerto Rico".

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información de la Oficina de Gerencia y Presupuesto es responsable por la actualización de esta política.

POLÍTICA

La siguiente política contendrá una serie de estándares y guías relacionadas a las actividades que tienen que ver con las distintas modalidades de la información geográfica, tales como **documentación de la información geográfica (metadatos), sistemas de coordenadas, códigos de áreas geográficas, niveles requeridos** de **exactitud** de los datos geoespaciales y **guía de planificación** para ***quality assurance*** de este tipo de datos.

PROCEDIMIENTO

a. **Metadatos:** Documentación de la información geográfica digital y análoga.

Los consumidores de información geoespacial deben tener una **descripción completa de los datos** que usarán. Estas descripciones son registradas mediante formularios estandarizados.

El **gobierno federal** estadounidense, a través del ***Federal Geographic Data Committee*** (FGDC): http://www.fgdc.gov ha diseñado y publicado el estándar de metadatos **FGDC-STD-001-1998,** el cual se utilizará en nuestras agencias de gobierno.

Estándar ISO para documentación de datos geográficos:

Posterior al estándar **CSDGM v2 1998,** La agencia FGDC endosó una serie de nuevos estándares (serie **ISO:19115)** de la International Organization of Standards (ISO), referentes a documentación de geodatos. Estos facilitan el intercambio de datos entre diferentes países. El estándar a adoptarse, según la agencia FGDC es el **19139:2007** y posteriormente, el **19115-3 (2015)** cuando sea terminado y publicado.

En la página web del FGDC https://www.fgdc.gov/metadata/selecting-a-geospatial-metadata-standard se exhorta a las agencias federales y locales a adoptar la familia de estándares ISO19xx.

Existe variedad de productos gratuitos para documentar o producir metadatos: El siguiente enlace muestra una lista de ejemplos de programas de distinto tipo y enfoque, gratuitos y comerciales: http://www.fgdc.gov/metadata/geospatial-metadata-tools. Para comenzar la documentación, **recomendamos** el uso de la herramienta simple para metadatos, "**TKME**" desarrollada en el **US Geological Survey.**

Para aquellos que utilizan los programas ESRI como ArcGIS Desktop, el subprograma ArcCatalog tiene una interfaz que provee todos los formularios para llenar la documentación necesaria. Otros como Intergraph, tienen herramientas para documentar.

Los aspectos más importantes para la documentación son: ***Título o nombre del geodato, periodo de actualización, pasos del proceso o metodología, sistema de referencia espacial y la evaluación de la exactitud posicional.***

b. Sistemas de coordenadas y proyecciones cartográficas:

Ley Núm. 184-2014 (*Ley del Sistema de Información Geoespacial del Estado Libre Asociado de Puerto Rico*): Esta ley establece que todas las **agencias del gobierno,** sus instrumentalidades y los municipios de Puerto Rico **utilizarán** el sistema de referencia espacial **Sistema Estatal de Coordenadas Planas,** (State Plane Coordinate System) con proyección cartográfica **Cónica Conforme de Lambert,** utilizando el **datum NAD83** o su versión más reciente y el **metro** como unidad de medida. Sus propósitos principales son: uniformar el uso de proyecciones cartográficas, y disponer lo relativo a la certificación de ubicaciones o posiciones geográficas.

El sistema de **coordenadas con proyección cartográfica oficial es el Sistema estatal de coordenadas planas con proyección Cónica Conforme de Lambert, zona 5200.** La **unidad de medida** es el **metro.** El **datum oficial** es el norteamericano de 1983 **(NAD83) en su versión más reciente, según las pautas del US National Geodetic Survey.** Las agencias pueden usar otros sistemas de coordenadas y proyecciones siempre y cuando sea para propósitos de integración de datos con agencias federales, internacionales o para publicación de geodatos para fines de cartografía web.

Entre estos sistemas están:

- **Coordenadas geográficas, sin proyección, unidades en grados decimales así como el sistema sexagesimal. Datum WGS84**
- **Proyección "Web-Mercator"** adoptada por Google Maps, Esri, Bing y otros (unidades: metros)
- Coordenadas planas con proyección **Transversal Universal de Mercator (UTM) zonas 19 y 20. Datum NAD83,** unidades: **metros.**
- **Es importante que se descarte el uso de datums anteriores al NAD83.**
- **El uso de sistemas de coordenadas arbitrarias (locales) no es aceptable.** Las agencias deberán asegurarse de recibir geodatos que estén referenciados a sistemas de coordenadas y proyecciones cartográficas estandarizadas.

c. Códigos alfanuméricos para registrar áreas geográficas:

El gobierno federal ha establecido una serie de **códigos** para registrar áreas geográficas y otros elementos que no necesariamente son superficies. Por el momento, la mayor cantidad de información se encuentra en áreas territoriales tales como municipios, barrios y divisiones de interés estadístico.

Las agencias de gobierno que registren información estadística o descriptiva por áreas geográficas establecidas, **(municipio, barrio, subbarrio, *place*)** tendrán que utilizar estos códigos. Existen otros códigos para áreas estadísticas. Para conseguir esta información, referiérase a la información publicada por el Negociado del Censo Federal para obtener estos mapas o tablas con los códigos.

d. Exactitud y planificación *quality assurance* de los datos geoespaciales:

Adaptado del documento de la Agencia Federal de Protección Ambiental (EPA) Guidance for Geospatial Data Quality

Assurance Project Plans EPA QA/G-5G, marzo, 2003

Usaremos como base para este documento, la política "CIO POLICY TRANSMITTAL 05-002" de la US Environmental Protection Agency (agosto 24, 2008). En la misma se establecen una serie de niveles de exactitud, tiers, los cuales servirán de guía para catalogar los geodatos de las agencias según estos niveles. Como parte de la documentación "metadatos" a entregar a la Oficina, el formulario de metadatos deberá tener documentado cuál es el nivel de exactitud que le aplique al geodato. A continuación los niveles de exactitud:

NIVEL	EXACTITUD	EJEMPLOS DE MÉTODOS DE COLECCIÓN HORIZONTAL	EJEMPLOS DE APLICACIÓN
NIVEL 1	Sub-métrica	Agrimensura; Posiciones usando técnica Carrier Phase Static Relative	Mensura para apoyo o asesoramiento técnico en litigaciones
NIVEL 2	1 a 5 metros	Posiciones usando técnica GPS Carrier Phase Static Relative	Definición de límites de derramamiento de contaminantes
NIVEL 3	6 – 25 metros	Posiciones usando técnica código estándar (Pseudo Range) GPS Autónomo	Localización de chimeneas, tomas de agua, centroide de una parcela urbana ≤ 300 metros²
NIVEL 4	26 – 100 metros	Uso no especificado de GPS; interpolación usando programados de SIG, fotos aéreas	Centroide del lugar, límites de una instalación grande, centroide de una parcela grande
NIVEL 5	101 – 200 metros	*Address match* en áreas urbanas	Localización preliminar de una instalación
NIVEL 6	201 – 999 metros	Centroide de parcelas muy grandes en zonas rurales	Predicción de dispersión de contaminante por aire
NIVEL 7	1,000 – 2,000 metros	Address matching para bloques censales	Geocodificación en ristra
NIVEL 8	2,001 – 5,000 metros	Centroide de bloque censal no urbano	Población a nivel de estado, algunos municipios
NIVEL 9	>5,000 metros	Centroide de Área Zip code no urbana, centroide de municipio	Cartografía generalizada
NIVEL 10	Desconocido	No aplica	Datos relativos para dar contexto

Los **niveles requeridos** son **nivel tres o menor,** dependiendo de las fuentes de información y los instrumentos a disposición.

Planificación de producción de geodatos: Se adoptará la guía de la Agencia Federal de Protección Ambiental (EPA): Guidance for Geospatial Data Quality "Assurance Project Plans EPA QA/G-5G", marzo, 2003. Esta guía provee los elementos básicos para una planificación de la calidad de la producción de datos geográficos. La guía da especial énfasis al uso de equipos de posicionamiento global (GPS) pero es adaptable a otros ámbitos de la producción de geodatos.

EXENCIONES

Ninguna

ANEJOS

Ninguno

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Ley Núm. 184-2014, "Ley del Sistema de Información Geoespacial del Estado Libre Asociado de Puerto Rico"
Federal Geographic Data Committee (FGDC): http://www.fgdc.gov
Portal Sistemas de Información Geográfica: www.gis.pr.gov
Portal Negociado del Censo Federal: www.census.gov

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-006

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: DESARROLLO, INTEGRACIÓN Y PUBLICACIÓN DE TRANSACCIONES ELECTRÓNICAS GUBERNAMENTALES

DESCRIPCIÓN

Esta política describe responsabilidades y requisitos que las entidades gubernamentales deben cumplir con respecto al desarrollo, implementación y publicación de transacciones electrónicas o formularios electrónicos accesibles por Internet.

La misma deroga y sustituye la Política Núm. TIG-006, conocida como "Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales", revisada 12 de septiembre de 2007.

BASE LEGAL

La Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico", y la Orden Ejecutiva OE-2015-023 del 14 de julio del 2015, establecen que la Oficina de Gerencia y Presupuesto (OGP) tendrá la facultad para orientar, instrumentar, establecer y emitir la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales con el objetivo primordial de lograr la interconexión de los organismos para facilitar y agilizar los servicios al pueblo. Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a todas las agencias gubernamentales del Estado Libre Asociado de Puerto Rico que utilizan la red interagencial o que publican transacciones electrónicas ya sea por medio del Portal del Gobierno o por portales propios.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas sobre desarrollo, implementación y publicación de transacciones electrónicas o formularios electrónicos accesibles por Internet.

POLÍTICA

A tono con la visión de un gobierno electrónico, las agencias son responsables de viabilizar la radicación de solicitudes de servicios a través de Internet. Toda solicitud o formulario de servicio debe ser provisto o accedido a través de los Servicios en Línea del Portal de Gobierno del Estado Libre Asociado de Puerto Rico. Toda entidad gubernamental, que a la fecha de vigencia de esta política, ofrezca servicios a través de portales propios debe proveer la información necesaria para integrar o enlazar dichos servicios al Portal del Gobierno en no más de treinta (30) días posteriores a dicha fecha.

Las entidades gubernamentales que al presente poseen la infraestructura para ofrecer servicios en línea, podrán continuar utilizando dicha infraestructura para el proceso de sus transacciones siempre y cuando cumplan con los requisitos y responsabilidades establecidos en esta política. Toda entidad que a la fecha de efectividad de esta política no tenga un sistema para manejo de solicitudes electrónicas, se verá obligado a utilizar la infraestructura sugerida por OGP. Las entidades que no poseen la infraestructura necesaria para la publicación y trámite de transacciones, deberán coordinar con la OGP, a través de ATI, el desarrollo de un plan de trabajo entre ambas agencias con el propósito de lograr la publicación de sus transacciones.

A) Esta política establece que todas las entidades gubernamentales serán responsables de:

1. Notificar a la ATI sobre toda solicitud electrónica de servicio así como todo formulario que esté disponible al ciudadano por Internet.

2. Asignar un funcionario con la suficiente autoridad para la toma de decisiones y que a la vez sea conocedor de los servicios ofrecidos por la agencia. Este funcionario será el Enlace de Servicios entre el personal de ATI y la agencia.

3. Documentar las transacciones y su ulterior implementación. Esto incluye, pero no se limita a: entrevistas, solicitud de documentación y asignación de personal según sea necesario.

4. Informar a la ATI, con seis (6) semanas de anticipación, todo cambio que afecte la disponibilidad o requerimientos de transacciones ya publicadas. Estos cambios incluyen, pero no se limitan a: el enlace donde reside la transacción, cambios en el costo de la transacción, cambios en el proceso de la transacción, de los documentos requeridos, (nótese que de acuerdo a la Orden Ejecutiva 2015-023 y su normativa implementadora, ninguna agencia podrá solicitarle a un ciudadano algún documento o certificación que el propio gobierno, incluyendo todas su agencias, tenga en su poder, que esté disponible mediante las herramientas, salvo cuando el ciudadano no autorice y/o exista legislación aplicable estableciendo lo contrario) de las instrucciones específicas o generales, y cambios de formularios.

5. Toda transacción electrónica o formulario disponible en línea estará accesible a través del Portal de Gobierno en http://www.pr.gov. Se prohíbe publicar en portales externos transacciones que no hayan sido incluidas previamente en el Portal de Gobierno.

6. Toda inversión en publicidad y/o todo anuncio que publique una agencia con respecto a transacciones o servicios en Internet, incluirá la dirección del Portal de Gobierno como medio principal de acceder la transacción.

7. Toda transacción electrónica de la entidad gubernamental incluirá, como parte del proceso, la notificación al ciudadano sobre el estatus (recibido, en proceso, etc.) en un periodo de tiempo no mayor a un (1) día laborable.

8. Toda transacción electrónica deberá estar diseñada de acuerdo con los parámetros establecidos por la Ley Núm. 229-2003, conocida como "Ley para Garantizar el Acceso de Información a las Personas con Impedimentos", y conforme al Reglamento de Accesibilidad.

B) Para ofrecer transacciones al público las entidades gubernamentales deben cumplir los siguientes requisitos:

1. Funcionales

a) En la medida que los recursos y las herramientas tecnológicas disponibles, lo permitan, cumplir con la Orden Ejecutiva OE-2015-023.
b) Del proceso o transacción requerida no poder completarse automáticamente:
   - poseer recursos humanos adiestrados, capacitados y responsables de trabajar inmediatamente las transacciones electrónicas que se reciban.
   - Poseer recursos humanos adiestrados, capacitados y responsables por el proceso de actualización de la transacción, de ser necesario.
   - El personal asignado a trabajar las solicitudes de servicio recibidas electrónicamente debe tener acceso a Internet y a una impresora.

2. Administrativos

a) Atemperar las leyes o reglamentos que presenten impedimentos para solicitar o procesar solicitudes en línea, para que las mismas permitan cumplir con la Ley de Gobierno Electrónico y la Orden Administrativa OE-2015-023.
b) Revisar los procesos desde la perspectiva de la nueva tecnología y realizar mejoras en los mismos para viabilizar el ofrecimiento del servicio en línea.

3. Técnicos

a) Utilizar el puerto 80 del protocolo "Transmisión Control Protocolo (TCP)" para aquella parte de la comunicación con el programa de aplicaciones donde la información que se intercambie con el ciudadano no es confidencial y no tiene que estar protegida.
b) Utilizar el puerto 443 del protocolo TCP para aquella parte de la comunicación con el programa de aplicaciones donde la información que se intercambie con el ciudadano es confidencial y tiene que estar protegida utilizando el estándar de "encripción" *Secure Sockets Layer* (SSL).

PROCEDIMIENTO

Las agencias tendrán treinta (30) días a partir de la fecha de publicación de esta política para notificar a la ATI sobre aquellas transacciones o formularios que ya estén disponibles en línea a través de portales propios o externos a la cuenta de apoyo técnico: support@ogp.pr.gov.

Para solicitar o notificar a la OGP la integración de una transacción al Portal de Gobierno la agencia deberá:

1. Adjuntar el/los formulario(s) correspondiente(s) a la solicitud de la transacción en formato (pdf) así como las instrucciones necesarias para completarlo de ser necesario.
2. Participar en las actividades de entrevistas, documentación y pruebas necesarias.
3. Si en la transacción existe en un portal externo o propio de la agencia (transacción tipo enlace):
    a) La(s) página(s) de la transacción en el portal en la entidad gubernamental debe incluir un botón o enlace para regresar al Portal de Gobierno. La Agencia deberá utilizar en sus páginas de transacción un desarrollo hecho por el grupo de portales de la División de Gobierno Electrónico de ATI.
    b) Toda información que aparece bajo el Portal de Gobierno con respecto a la transacción, será fiel y exacta a la de la agencia. No debe existir discrepancia entre la información o instrucciones ofrecidas en ambos portales.
    c) La entidad gubernamental proveerá a la OGP la dirección de enlace que apunta directamente a la transacción o formulario en su portal, y no a la página de bienvenida donde la entidad gubernamental la pública.
    d) Proveer el personal para las pruebas del funcionamiento de enlace.

EXENCIONES

Si una entidad gubernamental desea obtener una exención en relación al uso de la arquitectura sugerida por OGP, deberá someter una justificación por escrito al Director Asociado del Área de Tecnología de la OGP quien evaluará los méritos y notificará su decisión por escrito a la entidad gubernamental.

DEFINICIONES:

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Formulario- Documentos que completa el ciudadano en formato pdf con el propósito de solicitar un servicio en una agencia. Incluye las instrucciones y anejos pertinentes.

Puerto del protocolo TCP – Conexión lógica que describe la manera en que un programa cliente accede un servidor y viceversa.

Secure Sockets Layer (SSL)- Es un protocolo utilizado para manejar la seguridad de la información transmitida a través de Internet.

Servicio – Se refiere a los servicios que una agencia de gobierno les ofrece a los ciudadanos. Por lo general, el ciudadano debe completar un formulario para poder recibir el servicio solicitado.

Transacción – se refiere a la acción o conjunto de acciones que se realizan en una entidad gubernamental y cuyo producto final es de interés para un solicitante. Los solicitantes de una transacción pueden ser: individuos, organizaciones y corporaciones públicas o privadas.

Transacción Electrónica – se refiere a la acción o conjunto de acciones las cuales son realizadas parcial o completamente por medios electrónicos y cuyo producto final es de interés para un solicitante. Los solicitantes de una transacción pueden ser: individuos, organizaciones y corporaciones públicas o privadas.

ANEJOS

Orden Ejecutiva OE-2015-023 de 14 de julio de 2015
Carta Circular Núm. 127-15 de la Oficina de Gerencia y Presupuesto, Directrices para la Implantación de la Orden Ejecutiva Núm. 2015-23 de 14 de julio de 2015

REFERENCIAS

Ley Núm. 229-2003, según enmendada, conocida como "Ley para Garantizar el Acceso de Información a las Personas con Impedimentos".
Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Orden Ejecutiva OE-2015-023 de 14 de julio de 2015
Carta Circular Núm. 127-15 de la Oficina de Gerencia y Presupuesto, Directrices para la Implantación de la Orden Ejecutiva Núm. 2015-23 de 14 de julio de 2015

ANTECEDENTE

Política Núm. TIG-006, conocida como Desarrollo, Integración y Publicación de Transacciones Electrónicas Gubernamentales, revisada el 12 de septiembre de 2007.

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-007

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: DISPOSICIÓN DE EQUIPO Y LICENCIAS

DESCRIPCIÓN

Esta política describe los mecanismos que las entidades gubernamentales establecerán para asegurarse de que se disponga apropiadamente del equipo de tecnologías de información, así como de los programas que tuviesen los mismos instalados, si alguno. De esa manera, se cumplen los requerimientos de la Política de Seguridad y con los acuerdos incluidos en las licencias de los programas.

La misma deroga y sustituye la Política Núm. TIG-007, conocida como Disposición de Equipo y Licencias, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.,* Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, *supra*, tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes a las normas para disponer apropiadamente del equipo de tecnologías de información, así como de los programas que tuviesen los mismos instalados, si alguno.

POLÍTICA

Con el propósito de evitar el mal uso del equipo y el proteger la confidencialidad de los datos contenidos en los mismos, las entidades gubernamentales serán responsables de disponer adecuadamente de todo el equipo electrónico para el cual no se tenga uso, de conformidad con las reglas de la Administración de Servicios Generales (ASG). Además, todo equipo y/o programación así como datos almacenados pasará por un proceso intensivo de remoción de su contenido. Dicho proceso impedirá que se puedan extraer datos de los equipos una vez la entidad gubernamental determine que el equipo ya no le es necesario. Si el equipo contiene programas con licencias que no se reinstalarán en otro equipo, se le notificará al personal a cargo de las licencias de su agencia, para así mantener actualizado el inventario de las mismas.

PROCEDIMIENTO

El Oficial Principal de Informática (OPI) de la Agencia, junto con su personal autorizado y en coordinación con el Área de Propiedad, realizará el siguiente proceso para cumplir con esta política:

1. Seleccionar el método de remoción más adecuado. El OPI en coordinación con el Área de Propiedad decidirá cuál de los métodos de remoción de contenido es el más adecuado.
2. El OPI deberá mantener registros y documentación del equipo a disponerse, a través de la Oficina de Propiedad u Oficina de Administración de la agencia. Esto en conformidad con las reglas estipuladas por la Administración de Servicios Generales.
3. Si el equipo a disponerse contiene información digital almacenada en dispositivos de almacenamiento auxiliar como discos duros ("hard disk") y/o cintas magnéticas ("tapes"), u otro tipo de almacenamiento de información digital, el OPI deberá mantener resguardo ("backup") de la información.
4. Entregar las licencias que contenía el equipo: El devolver las licencias que no están en uso es uno de los requerimientos detallados en la política de Manejo de Licencias de Tecnologías. En el caso de las licencias globales adquiridas a través de OGP y que le pertenecen a OGP, las mismas se devolverán una vez se finalice el proceso de remoción de contenido del equipo. Aquellas licencias adquiridas por la agencia fuera de los contratos globales, permanecerán en la agencia como parte de su inventario de licenciamiento.
5. Transferir a otra entidad gubernamental el equipo que ya no se utilizará, luego de la remoción de su contenido: Si se está disponiendo del equipo por que es obsoleto para esta entidad gubernamental, pero se entiende que podría serle útil a cualquier otra, el mismo se le entregará al Oficial de Propiedad para que se le pueda transferir a otra entidad que pueda necesitarlo.
6. Donar el equipo que ya no se utilizará a escuelas y entidades sin fines de lucro, luego de la remoción de su contenido: Si se está disponiendo del equipo por que es obsoleto para las entidades gubernamentales, pero se entiende que podría serle útil a una escuela o entidad sin fines de lucro, el mismo se le entregará al Oficial de Propiedad para que se le pueda asignar a una escuela o entidad sin fines de lucro que pueda necesitarlo, cumpliendo con la normativa aplicable.
7. Destruir el equipo que ya no se utilizará, luego de la remoción de su contenido: Si se está disponiendo del equipo porque es obsoleto, pero se entiende que por razones de seguridad el mismo no debe transferirse o donarse, entonces la entidad gubernamental hará el proceso pertinente para destruir dicho equipo, conforme a la reglamentación de Propiedad Excedente Estatal de la Administración de Servicios Generales o la que corresponde, según la entidad gubernamental.

EXENCIONES

Ninguna

DEFINICIONES:

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra*.

Cinta Magnética – Dispositivo que consiste de una cinta de material plástico recubierta de material ferromagnético, sobre la que se almacena información. Las cintas sirven para resguardar información y se pueden almacenar en lugares dentro o fuera de la agencia.

Degaussing – Proceso en el que se utiliza un flujo magnético poderoso para eliminar los datos contenidos en un medio de almacenamiento magnético. Usualmente, el medio de almacenamiento queda inservible luego de este proceso.

Disco Duro - Dispositivo encargado de almacenar archivos e información de forma permanente y reutilizable en una computadora. Puede ser discos internos (directamente conectadas a la computadora) o externos (unidos a la computadora por puerto externos como USB).

Disposición de equipo – Es el proceso de eliminar equipo perteneciente a la agencia. El proceso de eliminar puede implicar el transferir el equipo a otra oficina u agencia, donarlo a una entidad sin fines de lucro o destruirlo.

Equipo – Incluye, pero no se limita a: computadoras, impresoras, cables, "hubs", "routers", baterías (UPS), escáneres y demás accesorios.

Licencia para programas (software) - Es un contrato entre el autor del programa y el usuario, que le permite al usuario utilizar el programa en forma legal. Las licencias contienen un acuerdo donde normalmente se estipula quiénes pueden utilizar el programa, los usos permitidos, si se pueden hacer copias del mismo, entre otras. Las compañías dedicadas a la venta de programación normalmente tienen disponibles diferentes tipos de licenciamiento, que se adaptan a las circunstancias y necesidades del cliente.

Overwriting – Proceso en el que se reemplaza con nuevos datos los datos existentes en un medio de almacenamiento. Existen programas que hacen automáticamente este proceso por medio de la sobre escritura en patrones. Este método no se debe confundir con la re-inicialización de discos ("format") o eliminación de particiones del disco con la herramienta "fdisk". El uso del "format" o el del "fdisk" no se consideran como métodos seguros de remoción de datos.

Remoción de contenido – Proceso que elimina el contenido de los medios para almacenamiento de datos (discos duros, cintas magnéticas, memorias y otros), de tal manera que dicho contenido

no pueda recuperarse en el futuro. Al momento existen diferentes métodos para la remoción de datos: "overwriting", "degaussing" y la destrucción física del medio de almacenamiento.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-003, Seguridad de los Sistemas de Información, de 7 de noviembre de 2016
Reglamento Núm. 5064 de 2 de mayo de 1994, Reglamento de Propiedad Excedente Estatal de la ASG http://www.gobierno.pr/ASG/reglamentos
Reglamento Núm. 6179 de 1 de agosto de 2000, Reglamento para Enmendar el Reglamento de Propiedad Excedente Estatal de la ASG http://www.gobierno.pr/ASG/reglamentos

ANTECEDENTES

Política Núm. TIG-007, conocida como Disposición de Equipo y Licencias, revisada el 12 de septiembre de 2007.

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-008

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO

DESCRIPCIÓN

Esta Política define y detalla el uso aceptable de la información que se maneja a través de los sistemas de información gubernamentales y las herramientas de Internet y Correo Electrónico, para así proteger al usuario y al gobierno de situaciones que pongan en peligro los sistemas y la información que contienen.

La misma deroga y sustituye la Política Núm. TIG-008, conocida como Uso de Información, de la Internet y del Correo Electrónico, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para establecer políticas de seguridad a nivel gubernamental sobre el acceso, uso, clasificación y custodia de los sistemas de información. *Id.*, Art. 5, inciso (e). Además, podrá establecer políticas dirigidas a garantizar la privacidad y protección de la información personal con relación al uso del Internet. *Id.*, Art. 5, inciso (f). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes al uso aceptable de la información que se maneja a través de los sistemas de información gubernamentales y las herramientas de Internet y Correo Electrónico.

POLÍTICA

La política pública del Estado Libre Asociado de Puerto Rico es facilitar y agilizar los procesos operacionales de los numerosos organismos de la Rama Ejecutiva, aumentar la eficiencia y efectividad en la prestación de los servicios gubernamentales al público y viabilizar la interconexión tecnológica entre los organismos y agencias. La automatización de los procesos operacionales requiere regular el uso apropiado de sus componentes y equipos e implantar las medidas necesarias para garantizar la confidencialidad de la información. Conforme a lo anterior, resulta necesario establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen.

Esta política tiene el objetivo de fijar las normas fundamentales que deben regir los controles básicos a ser establecidos por las agencias de manera que se garantice el uso adecuado de los recursos relativos a los sistemas de información. Las agencias deben promulgar políticas conforme al contenido de la presente política y velar por el cumplimiento de las mismas por parte de todo usuario de los sistemas de información del Estado Libre Asociado de Puerto Rico, incluyendo empleados, contratistas y otros autorizados a tal uso.

Normas generales aplicables al uso de los sistemas de información:

1. Cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad, y de las herramientas de Internet y correo electrónico. En ésta se indicarán los usos permitidos, los no permitidos y las sanciones o medidas disciplinarias que se aplicarían a los usuarios que incumplieran con la misma. Asimismo, será responsabilidad de cada entidad particular notificar debidamente a los empleados del contenido de la misma. Los usuarios a su vez, firmarán un documento indicando que conocen la política y que cumplirán con ella. La misma deberá estar disponible en cualquier momento para revisión o apreciación de cualquier persona civil o entidad gubernamental.

2. Los sistemas de información de las entidades gubernamentales, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y sólo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente constatándolo en documento oficial.

3. Cada entidad gubernamental debe colocar un aviso que indique al usuario o a quien acceda a su sistema de información que está accediendo a un sistema de información propiedad de esa entidad del Estado Libre Asociado de Puerto Rico y que se compromete a utilizarlo conforme a las normas establecidas.

4. Los sistemas de información y las herramientas asociadas, como el correo electrónico y la Internet, sólo podrán ser utilizados por personal debidamente autorizado. Será responsabilidad de cada entidad gubernamental definir las tareas que conllevan acceso a tal herramienta. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos de la entidad gubernamental y no es un derecho.

5. La información desarrollada, transmitida o almacenada en los sistemas de información de las agencias es propiedad de la entidad gubernamental y del Estado Libre Asociado de Puerto Rico, por lo que le aplican todas las disposiciones legales aplicables a los documentos públicos. La divulgación de tal información sin autorización está estrictamente prohibida. La alteración fraudulenta de cualquier documento en formato electrónico conllevará las sanciones aplicables a la alteración fraudulenta de documentos públicos.

6. Es responsabilidad de cada entidad gubernamental tomar las medidas necesarias para salvaguardar la confidencialidad de los datos personales de los empleados o de los ciudadanos contenidos en sus sistemas de información, conforme a la legislación aplicable.

7. Los documentos generados o contenidos en los sistemas de información de las entidades gubernamentales serán parte de los expedientes oficiales de la entidad. La destrucción de tales documentos electrónicos estará sujeta a las sanciones aplicables a la destrucción de documentos públicos.

8. El titular de los derechos relativos a las creaciones de funcionarios gubernamentales o por encargo de éstos es el Estado Libre Asociado de Puerto Rico. Los usuarios de los sistemas de información están obligados a respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.

9. Los programas y recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización del Departamento de Sistemas de Información, aunque sean programas libres de costos.

10. Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones o poderes de la entidad gubernamental.

11. Cada entidad gubernamental será responsable de establecer las normas mediante las cuales se asignan las cuentas acceso, incluyendo las medidas de seguridad aplicables tales como: claves secretas (contraseñas), controles de acceso a los servidores y sistemas para auditar su uso, la integridad y la seguridad de los datos y comunicaciones que se envían. (Ver Política de Seguridad ATI-003). Los usuarios de los sistemas deberán cumplir con todas las normas de uso y las relativas a la seguridad de la información emitidas por la entidad gubernamental. Cada usuario será individualmente responsable por el manejo adecuado de los códigos de acceso o contraseñas asignadas.

12. La correspondiente asignación de códigos de acceso no impedirá que el uso de los sistemas de información sea auditado por el personal autorizado por la agencia a tales fines, con el propósito de garantizar el uso apropiado de los recursos de la entidad gubernamental. Asimismo, los usuarios no deben tener expectativa de privacidad alguna con relación a la

información almacenada en su computadora o que sea emitida o comunicada a través de los sistemas de información del Estado Libre Asociado de Puerto Rico.

13. El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme a la legislación local y federal vigente y a las normas aplicables que rigen la conducta de los empleados.

14. Cada entidad gubernamental será responsable de verificar que el Internet y el correo electrónico estén funcionando adecuadamente. También se asegurarán que la información contenida en dichos sistemas esté protegida de accesos no autorizados. La agencia utilizará sistemas de protección contra virus y sistemas de protección contra accesos no autorizados ubicados en Servidores de Seguridad de Computadoras y Redes (*firewall*). (Ver Política de Seguridad ATI-003 y Política de Manejo de Firewalls ATI-014).

15. Las normas aquí establecidas deben interpretarse como complementarias a las normas legales de ordinario aplicables. Las entidades gubernamentales del Estado Libre Asociado se reservan la facultad de comenzar los procesos administrativos, civiles o criminales pertinentes a los actos cometidos, aunque los mismos no estén expresamente prohibidos en este documento, si dichos actos, directa o indirectamente, ponen en riesgo la seguridad, integridad y confiabilidad de la información, el equipo y los sistemas de información de la agencia. Tanto estas normas como las emitidas al amparo de esta política en las respectivas entidades gubernamentales, serán revisadas y actualizadas periódicamente, por lo que es responsabilidad de la agencia notificar al usuario el contenido de las mismas. Cualquier violación a las normas puede conllevar la revocación de cualquier privilegio de uso de los sistemas de información y deberá ser notificada al Director del Departamento de Sistemas de Información, al Director del Departamento de Recursos Humanos y al supervisor del empleado.

Normas aplicable al uso de Internet:

1. Los sistemas de comunicación y acceso a la Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.
2. Las operaciones realizadas a través de la Internet pueden generar responsabilidad por parte de las entidades gubernamentales del Estado Libre Asociado, por lo que los usuarios que tengan acceso al Internet a través de la entidad gubernamental no tienen expectativa de privacidad alguna con relación al uso y los accesos realizados a través de la Internet. La agencia se reserva el derecho a intervenir y auditar los accesos realizados por los usuarios a través de su sistema de información, el acceso a la Internet y el contenido de lo accedido.
3. La entidad gubernamental que provee acceso a la Internet no se responsabiliza por la validez, calidad, contenido o corrección de la Información contenida en la Internet.
4. Cada entidad gubernamental será responsable por velar que la conexión a la Internet se lleve a cabo conforme a la Política de Seguridad de la información y podrá monitorear el funcionamiento correcto de las mismas.

5. La publicación de información de la entidad gubernamental a través de la Internet deberá ser debidamente autorizada por el jefe de la agencia o la persona a quien éste delegue.

Normas aplicable al uso del correo electrónico:

1. El sistema de correo electrónico es propiedad de la entidad gubernamental y es parte íntegra de sus sistemas de información, por lo que la misma se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo.
2. Las operaciones realizadas por medio del correo electrónico pueden generar responsabilidad por parte de las agencias del Estado Libre Asociado, por lo que los usuarios de las cuentas de correo electrónico no tienen expectativa de privacidad alguna con relación a la información contenida en dichas cuentas. Las cuentas están sujetas a auditorias y revisiones sin previo aviso por el personal autorizado por la entidad gubernamental a tales efectos.
3. El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de la agencia. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados. Los usuarios deberán velar por el cumplimiento de las normas aplicables al comportamiento de los empleados de la entidad al momento de utilizar el correo electrónico.
4. Las entidades gubernamentales deberán establecer claramente una norma con relación a enviar por medio del correo electrónico documentos que contengan información confidencial de la agencia o que contengan información en los cuales se comenten asuntos internos de la agencia que no deben ser divulgados, conforme a las normas que rigen la conducta de los empleados. De ser necesario enviar tal información sensitiva, la misma deberá ser cifrada (*encrypted*) para evitar su divulgación. De sospecharse la interceptación o divulgación de tal información, se deberá informar al Departamento de Sistemas de Información inmediatamente, de manera que puedan tomar las medidas cautelares que procedan.
5. Cada agencia será responsable de establecer las normas mediante las cuales se asignan las cuentas de correo electrónico, incluyendo las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas, los controles de acceso al servidor, los sistemas para auditar el uso del sistema, la integridad y seguridad de los datos y las comunicaciones enviadas.
6. Las entidades gubernamentales deberán establecer claramente una prohibición con relación a obtener acceso no autorizado a las cuentas de correo electrónico, a leer, interceptar o revisar cualquier documento electrónico sin el consentimiento del remitente y del destinatario de la comunicación.
7. Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la agencia, a menos que estén autorizados a tal uso.
8. No se debe utilizar el correo personal para comunicaciones/funciones oficiales.

CUMPLIMIENTO DE LA POLÍTICA

El no cumplir con las políticas relacionadas a los sistemas de información podría conllevar sanciones y/o la suspensión de los servicios recibidos.

EXENCIONES

Ninguna.

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra*.

Antivirus - Programa que protege a los sistemas de los ataques de virus conocidos.

Cifrar (encrypt) – Proceso en el cual los datos se convierten a un formato que no puede descifrarse fácilmente por personas no autorizadas a acceder los mismos.

Contraseña – Secuencia de caracteres que se utiliza para comprobar que el usuario que está requiriendo acceso a un sistema es realmente ese usuario.

Firewall (Servidor de Seguridad de Computadoras y Redes) - Conjunto de programas que protege los recursos de una red de accesos no autorizados.

Lenguaje discriminatorio – Expresiones que podrían percibirse como ofensivas, ya sea por razones de raza, sexo, origen, nacionalidad, orientación sexual, edad, impedimento, religión o ideales políticos.

Usuario – Empleado del gobierno o contratista que tiene acceso autorizado a los sistemas.

Virus – Programa de computadora cuyo fin es hacerle daño a la computadora donde reside.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-014, MANEJO DE LOS *FIREWALLS*, del 7 de noviembre de 2016

ANTECEDENTE

Política Núm. TIG-008, conocida como Uso de Información, de la Internet y del Correo Electrónico, revisada el 12 de septiembre de 2007.

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLITICA NÚM. ATI-009

Fecha de Efectividad: 15 de diciembre de 2004
Fecha de Revisión: 7 de noviembre de 2016

TEMA: INTEGRACIÓN DE SISTEMAS FINANCIEROS

DESCRIPCIÓN

Esta política establece los fundamentos que serán requeridos a entidades gubernamentales que requieran desarrollar o adquirir aplicaciones de Nóminas, Finanzas o Recursos Humanos. Toda aplicación para estos efectos deberá proveer compatibilidad y/o integración con el módulo de Finanzas (PRIFAS) o el Sistema de Nóminas y Recursos Humanos (RHUM), según aplique, del Departamento de Hacienda.

La misma deroga y sustituye la Política Núm. TIG-009, conocida como Integración de Sistemas Financieros, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Además, tiene como función incorporar a las operaciones gubernamentales las mejores practicas del sector tecnológico y facilitar la comunicación entre la diversidad de tecnologías existentes en las instituciones del Gobierno. *Id.*, Art. 5, incisos (h) y (j). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a todas las agencias que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", requieren el desarrollo o adquisición de Sistemas de Nominas, Finanzas o Recursos Humanos.

ACTUALIZACION DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes a la integración de los sistemas financieros.

POLÍTICA

A. Entidades Gubernamentales

Todas las entidades gubernamentales tienen la responsabilidad de implementar sistemas de nóminas, finanzas o recursos humanos para optimizar y/o facilitar sus operaciones y funciones siempre que dicho sistema provea interoperabilidad y/o integración con los sistemas del Departamento de Hacienda del Estados Libre Asociado de Puerto Rico. Esta política también dispone que la agencia será responsable de:

1. Asegurar que la adquisición o desarrollo del producto cumple con las siguientes políticas:
   ATI-003 Seguridad de los Sistemas de Información
   ATI-004 Servicios de Tecnología
   ATI-010 Adquisición de Equipos para Sistemas Computadorizados de Información
   ATI-011 Mejores Prácticas de Infraestructura Tecnológica
2. Hacer los contactos, entrevistas y recopilación de la documentación necesaria en el Departamento de Hacienda para desarrollar las especificaciones de la interfase que hará la integración de datos con el(los) sistema(s) del Departamento de Hacienda.
3. Desarrollar la interfase que permite la integración de datos con los sistemas del Departamento de Hacienda.
4. Establecer controles y políticas internas para asegurar la integridad y seguridad de los datos transmitidos.
5. Coordinar y ejecutar las pruebas de la aplicación que hará interfase con el sistema del Departamento de Hacienda para asegurar el funcionamiento apropiado de la misma.
6. Si el Departamento de Hacienda hace modificaciones a sus sistemas que de alguna manera afecten el proceso en producción de transferencia de datos de la agencia hacia el Departamento de Hacienda, la agencia es responsable de realizar los cambios que correspondan al programa o proceso que realiza la interfase con el(los) sistema(s) de Hacienda.

B. Departamento de Hacienda

A su vez, el Departamento de Hacienda tendrá la responsabilidad de:

1. Autorizar el desarrollo o adquisición de sistemas financieros.
2. Verificar que los sistemas a ser desarrollados o adquiridos cumplen con los requisitos definidos para el control y manejo de información financiera de acuerdo a las nuevas prácticas definidas para sistemas de gobierno.
3. Proveer un ambiente de prueba para que las agencias puedan realizar las pruebas de interfase requerida.
4. Proveer a la agencia que lo solicite, la información necesaria para que pueda documentar, programar y poner en producción la interfase requerida.

5. Avisar a todas las agencias, con al menos treinta (30) días de anticipación, sobre todo cambio realizado en los sistemas de RHUM o PRIFAS que puedan afectar el proceso de transferencia de datos o interfase que la agencia pudiera tener programado con dichos sistemas.

CUMPLIMIENTO

Las agencias son responsables de reflejar en su Legado Estratégico Anual Tecnológico (LEAN-Tech) la adherencia y cumplimiento a la Política de Integración de Sistemas Financieros.

EXENCIONES

Si de forma excepcional una agencia desea obtener una exención para desviarse de la política aquí descrita deberá someter una justificación escrita a la OGP por conducto del Director Asociado de ATI, quien evaluará estrictamente los méritos y notificará de su decisión por escrito a la agencia.

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Integración - Es el proceso mediante el cual subsistemas o componentes producidos separadamente son combinados para trabajar coordinadamente y sin dificultadas. También puede referirse como el proceso mediante el cual productos de diferentes manufactureros son combinados para trabajar en conjunto.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-001, Legado Estratégico Anual Tecnológico (LEAN-Tech), revisada el 7 de noviembre de 2016
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-004, Servicios de Tecnología, revisada el 7 de noviembre de 2016
Política Núm. ATI-010, Adquisición de Equipo para Sistemas Computarizados de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-011, Mejores Prácticas de Infraestructura Tecnológicas, revisada el 7 de noviembre de 2016

ANTECEDENTE

Política Núm. TIG-009, conocida como Integración de Sistemas Financieros, revisada el 12 de septiembre de 2007.

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-010

FECHA DE EFECTIVIDAD: 15 de diciembre de 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: ADQUISICIÓN DE EQUIPO PARA SISTEMAS COMPUTADORIZADOS DE INFORMACIÓN

DESCRIPCIÓN

Esta política especifica los estándares mínimos que toda adquisición de equipo debe seguir para asegurar que la procura de equipo tecnológico apoye la gestión de Gobierno Electrónico. La misma deroga y sustituye la Política Núm. TIG-010, conocida como Adquisición de Equipos para Sistemas Computarizados de Información, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Además, tiene como función incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico y facilitar la comunicación entre la diversidad de tecnologías existentes en las instituciones del Gobierno. *Id.*, Art. 5, incisos (h) y (j). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a todas las agencias que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen, planifican adquirir o comprar equipo de informática o "hardware", que crean, dan acceso, procesan o tienen custodia de información del Estado Libre Asociado de Puerto Rico, independientemente de su costo y/u origen de fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes a la toda adquisición de equipo de sistemas computarizados de información.

POLÍTICA

El equipo que se adquiere como parte de los sistemas de información, es uno de los elementos fundamentales para que los sistemas funcionen en forma apropiada y eficiente. Es por esa razón que todo equipo que se adquiera deberá:

1. Tener la capacidad de integrarse a los sistemas que componen el Gobierno Electrónico (Ley de Gobierno Electrónico, Ley Núm. 151-2004, según enmendada).
2. Cumplir con las normas y requisitos de adquisición de equipo de la Administración de Servicios Generales, así como de las demás juntas de subastas del Estado Libre Asociado de Puerto Rico.
3. Cumplir con los requisitos de seguridad establecidos en la Política de Seguridad de los Sistemas de Información (ATI-003).
4. Ser de tecnología vigente y que la agencia que los adquiere cuenta o ha desarrollado un plan para adquirir la capacidad y conocimientos técnicos necesarios para obtener la óptima utilización de los mismos.
5. El sistema a adquirirse cumpla la base tecnológica requerida para su implantación (equipos, programas y personal) y se ajuste a la realidad financiera y presupuestaria del país.
6. Ser capaz de suplir las necesidades tecnológicas de las agencias del Estado Libre Asociado de Puerto Rico y permitir el ofrecimiento adecuado de los servicios e información a ofrecerse.
7. Promover el acercamiento del ciudadano a través de los Servicios en Línea.
8. Ser conforme al Plan Estratégico sometido.
9. Que no limite su uso y provea espacio de crecimiento y continuidad a las operaciones gubernamentales.

Antes de someter cualquier compra para adquisición de equipos y sistemas computarizados, la agencia debe cerciorarse de que cumple con el licenciamiento de los programas. Para más información sobre el licenciamiento asignado, puede comunicarse con el Área de Apoyo Técnico en la OGP.

EXENCIONES

Ninguna.

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra*.

Equipo computadorizado – dispositivo o máquina electrónica que recibe y procesa datos para convertirlos en información conveniente y útil. Se compone físicamente por numerosos circuitos integrados y otros muchos componentes de apoyo, extensión y accesorios, que en conjunto pueden ejecutar tareas diversas con suma rapidez y bajo el control de un programa. Dos partes esenciales constituyen estos equipos: el **"hardware"**, que es su componente físico (circuitos electrónicos, cables, gabinete, teclado, etcétera) y el **"software"**, que consta la parte intangible (sistemas operativos, programas, datos, información, etcétera) del equipo. "Hardware" y "software trabajan en conjunto para operar el equipo computadorizado.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Reglamento Núm. 3381 de 2 de diciembre de 1986, según enmendado, Reglamento de Adquisición de la ASG
Reglamento Núm. 3380 de 2 de diciembre de 1986, según enmendado, Reglamento Subastas de la ASG

ANTECEDENTE

Política Núm. TIG-010, conocida como Adquisición de Equipos para Sistemas Computarizados de Información, revisada el 12 de septiembre de 2007.

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLITICA NÚM. ATI-011

FECHA DE EFECTIVIDAD: 15 de diciembre 2004
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: MEJORES PRÁCTICAS DE INFRAESTRUCTURA TECNOLÓGICA

DESCRIPCIÓN

Esta política establece las buenas prácticas que toda agencia adscrita a la Rama Ejecutiva de Gobierno de Puerto Rico debe seguir al adquirir e implementar componentes en su infraestructura tecnológica.

La misma deroga y sustituye la Política Núm. TIG-011, conocida como Mejores Prácticas de Infraestructura Tecnológica, revisada el 12 de septiembre de 2007.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. La OGP tiene entre sus funciones el desarrollar y mantener, directamente o mediante contrato, una infraestructura capaz de suplir las necesidades tecnológicas del Gobierno, y que permita el ofrecimiento adecuado de servicios es información al ciudadano. *Id.*, Art. 5, inciso (d). A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Además, tiene como función incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico y facilitar la comunicación entre la diversidad de tecnologías existentes en las instituciones del Gobierno. *Id.*, Art. 5, incisos (h) y (j). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a toda agencia de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se

actualizan las políticas concernientes a la norma y el procedimiento a seguir por las agencias para lograr las mejores prácticas de infraestructura de tecnología.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico debe adquirir, desarrollar e implementar componentes de infraestructura tecnológica con productos de calidad y costo efectivos. La adquisición e implementación de dichos componentes también debe promover una infraestructura que provea interoperabilidad y escalabilidad a modo de mejorar las capacidades operacionales, la productividad y ejecución de las agencias resultando así en un servicio gubernamental de alta calidad. Para propósitos de este documento, el diseño de la infraestructura se dividió en cuatro componentes: Plataforma, Aplicaciones (Software), Redes y Datos/Información. A continuación, se describen cada uno de los componentes y la política a seguir a base de los principios de mejores prácticas.

Términos técnicos están descritos en la sección de Definiciones de este documento.

PLATAFORMA

La política del componente de Plataforma pretende que los dispositivos que se implementen en las agencias provean interoperabilidad y sean de uso común en la industria. Los componentes de plataforma son Servidores, Unidades de Almacenamiento y Estaciones de Trabajo (Clientes).

Política para el Componente de Plataforma

La planificación, diseño, adquisición e implementación de los dispositivos pertenecientes al componente de plataforma son guiados por los siguientes principios con el propósito de apoyar la estrategia de gobierno, sus metas y objetivos:

1. Los componentes de la plataforma deben ser capaces de apoyar los procesos administrativos y los procesos de negocio de la agencia.

2. Toda adquisición de los componentes de plataforma debe estar regida por la Política de Adquisición de Equipo para Sistemas Computarizados (ATI-010).

3. Los servidores y los dispositivos de almacenaje deben dar apoyo a los servicios esenciales en la agencia.

4. Los dispositivos adquiridos e implementados debe utilizar las tecnologías principales, las cuales se determinan por su uso y dominio en la industria.

5. Las agencias deben adquirir servidores que se adapten a sus necesidades de trabajo diario y a la vez provean para crecimiento, escalabilidad e interoperabilidad.

6. Los dispositivos de entrada de datos (teclados) y los dispositivos de salida (monitores, proyectores, bocinas, impresoras etc.) conectados a los clientes deben utilizar estándares aprobados por la IEEE y estándares de la industria para programación de controladores (*software drivers*). (*Industry de facto Standard Software Drivers*)

7. Los componentes conectados a los servidores, tales como impresoras y *ploters,* etc., deben cumplir con los estándares de la IEEE y con los estándares de la industria para programación de controladores (*software drivers*).

8. Las agencias deben adquirir soluciones de almacenamiento que atiendan las necesidades de la agencia a mediano y largo plazo.

9. El proveedor de la plataforma debe proveer los medios contractuales para que la configuración y versiones del sistema operativo puedan mejorarse según la evolución y cambios de la necesidad.

10. Los componentes de plataforma implementados deben permitir un modelo *n-tier* (niveles).

11. La infraestructura de la plataforma debe ser diseñada para permitir crecimiento, flexibilidad y adaptabilidad.

12. La infraestructura de la plataforma debe maximizar el diseño y la red en la agencia para asegurar la disponibilidad de las aplicaciones y de los servicios a los ciudadanos y usuarios.

PROGRAMACIÓN

El componente de programación pretende que la adquisición e implementación de programas para automatizar y mantener los procesos en las agencias promueva la interoperabilidad, integración, colaboración y comunicación a fin de proveer un servicio público eficiente y de alta calidad. Será de suma importancia que se dé prioridad a utilizar software que contenga la mayor funcionalidad posible y principalmente configurable y no de alta dependencia de la programación personalizada.

El componente de Programación (*software*) está definido por aplicaciones, lenguajes de programación, bases de datos, programas de productividad y programas de utilidades.

Políticas para el Componente de Programación

La planificación, diseño, adquisición e implementación de programas son guiados por los siguientes principios con el propósito de apoyar la estrategia de gobierno, sus metas y objetivos:

1. Todos los productos adquiridos o desarrollados deben ser utilizados para automatizar funciones y/o procesos en las agencias.
2. Las aplicaciones o Sistemas de Manejo de Bases de Datos deben ser diseñadas, adquiridas e implementadas para proveer crecimiento, flexibilidad, adaptabilidad.
3. Las aplicaciones deben ser diseñadas, adquiridas, desarrolladas o mejoradas de modo que la información pueda ser compartida e integrada seguramente con otros sistemas que así lo requieran.

4. Las aplicaciones, lenguajes de programación, Bases de Datos y programas de productividad deben operar entre si, ser funcionales en arquitectura de n-niveles (*n-tier*) y tener la capacidad de poder operar en navegadores de uso común en la industria si es necesario.

5. Toda aplicación comercial ó personalizada implementada debe ser documentada utilizando metodologías de desarrollo y documentación estándares o de uso común.

6. Toda aplicación comercial o personalizada que se adquiera o desarrolle debe tener maneras de controlar la creación y privilegios de los usuarios.

7. Toda aplicación que se desarrolle o adquiera debe tener una garantía que asegure que funciona apropiadamente y de acuerdo con los propósitos para los cuales fue desarrollada.

8. Toda aplicación que se desarrolle o adquiera debe incluir el plan de administración de mejoras, reparaciones, mantenimiento y capacidad para asegurar Recuperación de Desastres y Continuidad de Operación en caso de interrupción.

9. Toda aplicación que se desarrolle e que involucre programación (código hecho a la medida), dicho código será propiedad del Estado Libre Asociado de Puerto Rico y sus instrumentalidades.

DATOS/INFORMACIÓN

Al establecer una política del componente de datos e información se pretende que las agencias mantengan uniformidad de los datos utilizados en sus sistemas. Los datos/información que las agencias mantienen son vitales para la toma de decisiones tanto para la agencia como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico. Las agencias deben establecer metodologías para asegurar la integridad y confiabilidad de los datos producidos y almacenados.

Política para el Componente de Datos

1. Las agencias deben mantener uno o varios diccionarios de datos, donde se documente y explique claramente qué datos son mantenidos en sus bases de datos. Las agencias son responsable de mantener actualizada dicha información en su agencia.
2. Las agencias deben utilizar nombres significativos en sus datos y mantener uniformidad a través de distintas plataforma o sistemas en la agencia en relación al nombre que se le ha dado al dato.

3. La duplicidad de datos en un mismo sistema debe ser evitado para asegurar así integridad en los mismos.
4. Los datos producidos y mantenidos en las agencias deben ser resguardados y mantenidos con una frecuencia que este acorde con la sensibilidad de los datos y volumen de trabajo diario.
5. Las agencias deben desarrollar un plan de contingencia que contenga los elementos descritos en la Política de Seguridad (TIG-003).

RED

Al establecer una política del componente de Red se pretende que las agencias adquieran e implementen una infraestructura de red segura, escalable, basada en estándares de dominio en la industria, la cual provee la comunicación necesaria para la distribución de servicios eficientemente.

Política para el Componente de Red

1. Las redes en las agencias deben proveer la infraestructura necesaria para implementar y mantener los procesos de negocio de la agencia.
2. Las redes deben ser operacionales y confiables.
3. Las redes en las agencias deben ser diseñadas e implementadas con niveles de redundancia, tolerancia a fallas e incluyendo un plan de recuperación de desastres, basado en los requerimientos de negocio de la agencia.
4. El diseño de la red debe estar documentado.
5. El diseño e implementación de la red debe ser escalable y operable entre otras redes en la agencia u otras agencias del gobierno de ser necesario.
6. Las redes deben utilizar tecnologías probadas y de dominio en la industria.
7. Las redes deben ser diseñadas e implementadas para cumplir con la Política de Seguridad de los Sistemas de Información (TIG-003).
8. El acceso a la red debe ser implementado por medio de autenticación y autorización independientemente de su localización.

9. La adquisición de equipo o elementos de la red deben cumplir con lo estipulado en la Política de Adquisición de Equipo para Sistemas Computarizados de Información (TIG-010). Esta guía será revisada periódicamente para indicar cambios en tecnología.

CUMPLIMIENTO

Las agencias son responsables de reflejar en el Legado Estratégico Anual Tecnológico (LEAN-TECH), la adherencia y cumplimiento con la Política de Mejores Prácticas de Infraestructura Tecnológica.

EXENCIÓN

Si una agencia desea obtener una exención para desviarse de la política aquí descrita deberá someter una justificación escrita a la OGP por conducto del Director Asociado de ATI, quien evaluará los méritos y notificará de su decisión por escrito a la Agencia y a la Administración de Servicios Generales.

DEFINICIONES

AGENCIA – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

ALMACENAMIENTO – El almacenamiento usualmente es conocido como un recurso externo separado de los servidores y clientes. El almacenamiento es usualmente adquirido y manejado independientemente y a la vez compartido por múltiples servidores. Algunos tipos de almacenamiento aceptables son:

- **DAS** (*Direct Attached Storage*) - tipo de almacenamiento que se sujeta directamente a un servidor o un cliente. Las arquitecturas más comunes de este tipo de almacenamiento son los arreglos RAID y las librerías en cintas.

- **NAS** (*Network Attached Storage*) – es un tipo de almacenamiento orientado a archivos donde el dispositivo de almacenamiento está conectado a una red y el mismo provee los servicios de acceso a archivos ya sea a los servidores ó los cliente. NAS es una tecnología de estándar abierto en la industria que permite a los usuarios acceder y compartir datos sin impactar las aplicaciones o del servidor.

- **SAN** (*Storage Area Network*)- Es una implementación de almacenamiento que tradicionalmente es utilizado para redes de propósitos especiales la cual incorpora tecnologías de comunicación e interfaces de alto rendimiento para conectar los dispositivos de almacenamiento a los servidores.

- **Nube (Cloud)**- es la capacidad de utilizar de forma estática o dinámica almacenamiento de datos en Centros dedicados para el propósito de almacenamiento sean propios, adquiridos pero remotos o de terceros.

APLICACIONES – son sistemas compuestos por programación y bases de datos diseñados para automatizar funciones específicas del negocio en la agencia. Ejemplo: sistemas de nóminas, sistema de

registro de vehículos etc. Las aplicaciones pueden ser de dos tipos: aplicaciones comerciales o aplicaciones personalizadas (*custom software*)

APLICACIONES COMERCIALES - Aplicaciones desarrolladas para la venta o público general. Estas aplicaciones pueden ser personalizadas o adaptadas para distintos negocios por medio de programación de preferencias.

APLICACIONES PERSONALIZADAS - Aplicaciones diseñadas y desarrolladas a base de necesidades específicas de un negocio o de un cliente.

BASES DE DATOS – primordialmente describe sistemas de manejo de bases de datos, los cuales organizan, manejan y facilitan el acceso a los datos. Además, estos sistemas proveen seguridad adecuada para mantener integridad de los datos almacenados.

DICCIONARIO DE DATOS - Es una base de datos que guarda información sobre los datos y de bases de datos. Contiene el nombre, tipo, rango de valores posibles, fuentes y autorización para accesos para cada dato o elemento utilizado en bases de datos o archivos.

ESTACIONES DE TRABAJO (CLIENTES) - El cliente, con su sistema operativo asociado, provee la interfaz entre el usuario a las aplicaciones existentes. Los clientes pueden incluir: computadoras personales (PC), clientes finos (*thin client*), terminales controlados por sistemas centrales, interfaces de voz, dispositivos móviles de una ó múltiples funciones (*Pocket PC, PDA*, teléfonos *PDA*, etc.), dispositivos telefónicos, tarjetas inteligentes etc.

INTEROPERABILIDAD - Es la habilidad de un sistema o producto para trabajar con otros sistemas o productos sin un esfuerzo especial. Un producto alcanza interoperabilidad adhiriéndose a estándares publicados.

N-TIER (NIVELES) - Un programa *n-tier* es aquel que es distribuido entre tres o más computadoras en una red. Una estructura *n-tiers* implica la utilización de un modelo Cliente / Servidor.

PRODUCTOS PARA PROGRAMACIÓN – Son tecnologías y productos utilizados para desarrollar y mantener aplicaciones en una agencia. Se incluyen lenguajes de programación y la tecnología intermediaria *middleware* que facilita la comunicación entre aplicaciones así como también productos que permiten el intercambio de información (productos para producir informes etc.).

PROGRAMAS DE PRODUCTIVIDAD- son herramientas de programación utilizadas para promover la automatización y colaboración en las oficinas. Ejemplos: herramientas para procesamiento de palabras, hojas de cálculos, presentaciones, aplicaciones gráficas, bases de datos personales etc.

PROGRAMAS DE UTILIDADES – programas que típicamente son una extensión de un dispositivo del sistema operativo. Usualmente se refiere a un producto de programación que es clasificado como necesario para mantener, modificar y mejorar la arquitectura de plataforma o de la red.

SERVIDORES - Una computadora con su respectivo sistema operativo para proveer de servicio a las ESTACIONES DE TRABAJO (clientes).

NUBE – Servicio de aprovisionamiento de infraestructura, software, base de datos, servicios combinados con el fin de cumplir con una necesidad particular. Usualmente este tipo de servicio es provisto por terceros y el pago del servicio es basado en el uso o demanda. Como regla general el proveedor es responsable de todos los costos asociados para que el servicio funcione y establece niveles de servicios garantizados para sustentar la tarifa a cobrar.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-010, Adquisición de Equipo para Sistemas Computadorizados de Información, revisada el 7 de noviembre de 2016

ANTECEDENTE

Política Núm. TGI-11, Mejores Prácticas de Infraestructura Tecnológica, revisada el 12 de septiembre de 2007.

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-012

FECHA DE EFECTIVIDAD: 7 de noviembre de 2016

TEMA: TECNOLOGÍAS EN LA NUBE
("CLOUD COMPUTING")

DESCRIPCIÓN

El Área de Tecnologías de Información (ATI) de la Oficina de Gerencia y Presupuesto (OGP) ha identificado la adopción de Tecnologías en la Nube o "Cloud Computing" como una oportunidad para transformar el uso tecnología informática en el Estado Libre Asociado de Puerto Rico. El National Institute of Standards and Technology (NIST) define "Cloud Computing" como "un modelo para habilitar de forma conveniente, ubicua y por demanda (según sea solicitado) el acceso en red a un conjunto de recursos informáticos compartidos y configurables (ej. redes, servidores, almacenaje, aplicaciones y servicios) que pueden ser prestados de forma rápida y lanzados con un mínimo de esfuerzo de gestión o interacción de parte del proveedor del servicio"[1] (National Institute of Standards and Technologies [NIST], 2011). Esta política establece las guías principales para la adopción de servicios y tecnologías en la nube.

No obstante, la adopción y migración a Tecnologías en la Nube podrá realizarse siempre y cuando exista una solución segura, confiable y costo-efectiva. De igual forma, es responsabilidad principal de las agencias validar y asegurar que los proveedores de Tecnologías en la Nube cumplen con los aspectos de seguridad y cumplimiento requeridos por las leyes, reglamentos y guías que rigen las mejores prácticas de su negocio.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. La OGP tiene entre sus funciones el desarrollar y mantener, directamente o mediante contrato, una infraestructura capaz de suplir las necesidades tecnológicas del Gobierno, y que permita el ofrecimiento adecuado de servicios es información al ciudadano. *Id.*, Art. 5, inciso (d). A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Además, tiene como función incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico y facilitar la comunicación entre la diversidad de tecnologías existentes en las instituciones del Gobierno. *Id.*, Art. 5, incisos (h) y (j). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151,

---

[1]Mell, P., & Granee, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145). Gaithersburg, MD: National Institute of Standards and Technologies. Retrieved from: http: //csrc.nist.gov/publications/PubsSPs.html#800-145

las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a cualquier adquisición de Tecnologías en la Nube por parte de cualquier agencia, de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico. Se refiere a la adquisición de servicios de un suplidor externo al ELA.

Por lo tanto, los servicios ofrecidos por ATI a las agencias quedan excluidos de esta política. ATI podrá establecer guías, directrices y formularios específicos aplicables a los modelos de Tecnologías en la Nube, a un grupo de servicios o a cualquier proveedor de servicios, de forma que se amplíen o clarifiquen los aspectos contenidos en esta política sobre Tecnologías en la Nube; en cuyo caso, las agencias esta obligadas a dar cumplimiento a lo así provisto. .

Se considerarán y denominarán como Tecnologías en la Nube todas aquellas que operan bajo los modelos "Software as a Service" (SaaS), " Platform as a Service" (PaaS) e " Infrastructure as a Service" (IaaS). Las definiciones y modelos de Tecnologías en la Nube ("Cloud Computing") son aquellos según definidos por el National Institute of Standards and Technologies (NIST) para establecer una definición uniforme y aceptada.[2]

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación.

POLÍTICA

1. La adquisición y utilización de Tecnologías en la Nube deberá estar autorizada formalmente por los mismos mecanismos aplicables a otros servicios de informática que involucran a la ATI.

2. La solicitud de autorización de Tecnologías en la Nube deberá estar acompañada de un formulario de evaluación específico para el tipo de servicio (Evaluación de Tecnologías en la Nube).

3. La utilización de Tecnologías en la Nube deberá cumplir con todas las leyes y reglamentos de privacidad y confidencialidad aplicables a nivel estatal y federal. La agencia que adquiera los servicios de Tecnologías en la Nube será responsable por asegurar que los roles y responsabilidades relacionadas al manejo de datos y la privacidad y confidencialidad de los mismos están clara y adecuadamente definidos en el acuerdo de servicio del proveedor de Tecnologías en la Nube.

---

[2] Para mayor información sobre los modelos y características de las Tecnologías en la Nube según definidos por el National Institute of Standards and Technologies, favor de referirse al documento The NIST Definition of Cloud Computing (NIST Special Publication 800-145). Obtenido de:
http://csrc. nist.gov/publications/nistpubs/800-145/SP800-145.pdf

4. El acuerdo de servicio del proveedor de Tecnologías en la Nube deberá ser evaluado y aprobado por ATI. En su análisis, ATI podrá considerar si el servicio ya se encuentra disponible mediante contrato global suscrito por ATI, en cuyo caso la agencia de justificar la razonabilidad y costo/efectividad de la contratación directa.

5. La agencia no podrá adquirir servicios de Tecnologías en la Nube hasta que se cumpla con todos los requisitos establecidos en esta política.

GUÍAS

1. La agencia debe determinar la razón o justificación para utilizar un modelo de Tecnologías en la Nube, que pudiera incluir las siguientes, entre otras:

   a. Mayor eficiencia o efectividad en la prestación de un servicio tecnológico.

   b. La necesidad de un atributo específico de Tecnologías en la Nube (ej. elasticidad, escalabilidad, modelo basado en utilización)

   c. La necesidad de implantar un servicio tecnológico en un corto período de tiempo.

   d. La necesidad de implantar nuevos o mejores mecanismos de contingencia, recuperación de desastres o estrategias para garantizar la continuidad del negocio.

   e. Como una estrategia para establecer ambientes de desarrollo, prueba, control de calidad o cualquier otra necesidad cónsona con las mejores prácticas en el ciclo de desarrollo de software.

2. La agencia debe tener claridad en cuanto a todos los costos asociados con el ciclo de vida de la solución de Tecnologías en la Nube, no solamente la implantación.

3. La agencia debe consultar con ATI al comienzo del ciclo de evaluación de Tecnologías en la Nube para determinar si existen contratos o acuerdos existentes en el gobierno del ELA que pudieran ser aprovechados para el nuevo proyecto.

4. Al evaluar la adquisición de un servicio de Tecnologías en la Nube, la agencia, en colaboración con ATI, deberá considerar maneras de estructurar las soluciones y acuerdos de servicios o contratos de forma que faciliten la adopción de Tecnologías en la Nube en otros programas o agencias.

5. En cuanto a seguridad de informática, la agencia debe llevar a cabo un análisis de riesgo completo previo a contratar servicios de Tecnologías en la Nube:

   a. El proveedor de servicios deberá presentar evidencia de haberse sometido a un proceso de evaluación de seguridad por una entidad competente y presentar evidencia por medio de la presentación de un informe conocido como SOC ("Service Organization Control") nivel 2 que asegura a sus clientes de la utilización de sistemas que protegen sus datos. Este informe es el resultado de auditoría de seguridad, disponibilidad, integridad de procesos, privacidad y

confidencialidad. También deberá presentar que está certificado ISO 27001. Esta certificación establece que la entidad que provee servicios de computación en la nube ("Cloud computing"), cumple con los estándares establecidos por ISMS (Information Security Management Systems"). El ISMS asegura que los procesos de seguridad están ajustados para mantenerse al día con los cambios de amenazas de seguridad, vulnerabilidad e impactos adversos.

b. La agencia debe establecer procedimientos para informar incidentes, obtener respuesta de parte del proveedor y otras funciones de seguridad en colaboración con el proveedor de Tecnologías en la Nube.

c. La agencia debe establecer medidas para recuperación de desastres y garantizar la continuidad de los servicios de Tecnologías en la Nube.

d. Deben establecerse acuerdos de niveles de servicio ("Service Level/ Agreement") donde se establezcan los niveles de respuesta de los proveedores en cualquier incidente.

6. La agencia debe entender cuáles son sus roles y responsabilidades relacionadas a la implantación, operación y apoyo de la solución de Tecnologías en la Nube.

7. La agencia debe tener un plan de migración en caso que haya que cambiar de proveedor de solución de Tecnologías en la Nube o desee traer la solución a la infraestructura tecnológica de la agencia. Esto busca disminuir y evitar estar atados a un solo proveedor o tipo de tecnología garantizando la entrada y salida de la Nube.

8. Todo contrato debe tener una cláusula donde diga de forma explícita que los datos y su uso son propiedad exclusiva del Estado Libre Asociado de Puerto Rico. Para revisión sobre cláusulas contractuales, véase Política Núm. ATI-017, sobre Revisión de Contratos de Tecnología.

ASPECTOS TÉCNICOS

En aras de garantizar una adecuada implementación y colaboración entre las diferentes soluciones implementadas en la Nube, se deberá cumplir con los siguientes aspectos técnicos:

1. Se seleccionarán Tecnologías en la Nube que implementen y utilicen estándares, formatos y protocolos abiertos. En los casos donde no se provean mecanismos que implementen o utilicen dichos estándares, formatos o protocolos, se deberán establecer y garantizar mecanismos aceptados para la recuperación de los datos.

2. Se deben evaluar con prioridad aquellas Tecnologías en la Nube que proveen mecanismos para desarrollar, extender y mejorar la funcionalidad base que proveen en sus servicios.

3. Se deben evaluar con prioridad las Tecnologías en la Nube cuyos componentes y servicios estén basados o que se puedan extender utilizando tecnologías abiertas.

4. Se deben evaluar con prioridad aquellas Tecnologías en la Nube que cuentan o colaboran con proyectos para replicar la implementación de la Nube utilizando la infraestructura tecnológica propia de la agencia.

EXENCIONES

Ninguna

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Interfaz de programación ("Web API") - Conjunto de funciones que permite la comunicación entre aplicaciones y representan la capacidad de comunicación entre componentes de "software." Éstas permiten la comunicación a través del Internet por una entidad externa con aplicaciones internas del Gobierno, con el objetivo de permitir el libre acceso, de manera segura, a entidades autorizadas con información del Estado Libre Asociado.

National Institute of Standards and Technologies (NIST) - Agencia adscrita al Departamento de Comercio de los Estados Unidos que promueve el avance de la ciencia a través de la medición, los estándares y la tecnología para mejorar el desarrollo económico y la calidad de vida.

Tecnología en la Nube o "Cloud Computing" - Un modelo para habilitar de forma conveniente, ubicua y por demanda (según sea solicitado) el acceso en red a un conjunto de recursos informáticos compartidos y configurables (ej. redes, servidores, almacenaje, aplicaciones y servicios) que pueden ser provisionados de forma rápida y lanzados con un mínimo de esfuerzo de gestión o interacción de parte del proveedor de servicio.[3]

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-017, sobre Revisión de Contratos de Tecnología, del 7 de noviembre de 2016

[3]Traducción Libre. Mell, P., & Granee, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145). Gaithersburg, MD: National Institute of Standards and Technologies. Obtenido de: http: //csrc.nist.gov/publications/PubsSPs.htm1#800-145

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-013

FECHA DE EFECTIVIDAD: 1 de julio de 2006
FECHA DE REVISIÓN: 7 de noviembre de 2016

TEMA: MARCO REFERENCIAL DE ADQUISICIÓN TECNOLÓGICA GUBERNAMENTAL

DESCRIPCIÓN

Esta política establece las prácticas que toda agencia adscrita a la Rama Ejecutiva de Gobierno de Puerto Rico tienen que seguir al adquirir bienes o servicios tecnológicos. La misma deroga y sustituye la Política Núm. TIG-011, conocida como Marco Referencial de Adquisición de Tecnología Gubernamental de 1ro de julio de 2006.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. La OGP tiene entre sus funciones el desarrollar y mantener, directamente o mediante contrato, una infraestructura capaz de suplir las necesidades tecnológicas del Gobierno, y que permita el ofrecimiento adecuado de servicios es información al ciudadano. *Id.,* Art. 5, inciso (d). A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.,* Art. 6, inciso (I), (i) y (iii). Además, tiene como función incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico y facilitar la comunicación entre la diversidad de tecnologías existentes en las instituciones del Gobierno. *Id.,* Art. 5, incisos (h) y (j). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a toda agencia de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

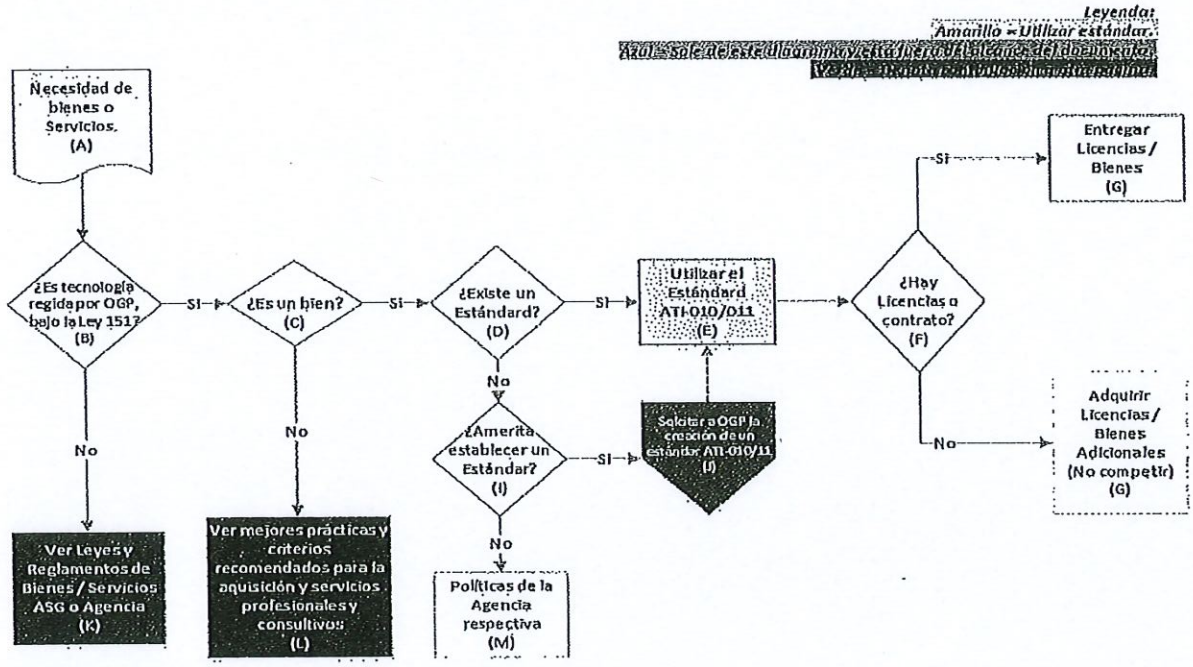
ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes al marco referencial de adquisición tecnológica gubernamental.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico debe adquirir, desarrollar e implementar componentes, licencias, aplicaciones, programas, equipos y/o productos tecnológicos con soluciones de alta calidad y probada efectividad. La adquisición e implementación de dichas soluciones también debe promover una infraestructura inter-operable y escalable a modo de mejorar las capacidades operacionales, la productividad y ejecución de las agencias resultando así en un servicio gubernamental de alta calidad. Es el propósito de la Oficina de Gerencia y Presupuesto (OGP) hacer cumplir la Ley 151-2004, *supra,* e instrumentar y emitir la política pública a seguir y las normas que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales, con el objetivo primordial de lograr un estándar tecnológico para facilitar la interconexión de las entidades gubernamentales y agilizar los servicios del pueblo de una forma eficiente y costo efectiva, según las mejores prácticas de Tecnología de Información.

Diagrama decisional de Adquisición Tecnológica Gubernamental



Nota: Referirse a las próximas secciones de esta política para descripción y definiciones.

Descripción y definiciones: Diagrama de decisión de adquisición tecnológica gubernamental

A. Necesidades de bienes o servicios: Toda Agencia o dependencia gubernamental es responsable de operar bajo un presupuesto anual aprobado, según lo establecido por Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como " Ley de Contabilidad del Gobierno del Puerto Rico". Esto requiere establecer necesidades y prioridades, asignar presupuesto y dar seguimiento a la adquisición de bienes y servicios, según las mejores prácticas establecidas por la ASG, OGP y la Oficina del Contralor.

B. ¿Es tecnología regida por OGP bajo la Ley 151-2004?: La Ley 151-2004, *supra,* faculta a la OGP a regular la adquisición de bienes y servicios tecnológicos tales como computadoras, redes, aplicaciones, programas; servidores, servicios de implantación, servicios de apoyo técnico, adiestramientos tecnológicos a usuarios o especialistas técnicos, etc. Estos deben de estar incorporados en el Legado Estratégico Anual Tecnológico, Lean-Tech, donde se describe la situación actual de la agencia y lo que se espera alcanzar durante el año fiscal (ver ATI-001). El objetivo de OGP es lograr la interoperabilidad, estandarización y costo-efectividad tecnológico en las dependencias gubernamentales, y así facilitar y agilizar los servicios al ciudadano.

C. ¿Es un bien?: Un bien es una aplicación, programa o producto el cual tiene un costo económico y está disponible comercialmente.

D. ¿Existe un estándar?: Un estándar es un producto/servicio que la OGP estableció como el indicado a ser utilizado para una funcionalidad específica. El Artículo 5 de la Ley 151, *supra,* dispone que la OGP tendrá entre sus funciones incorporar a las operaciones gubernamentales las mejores prácticas del sector tecnológico, por medio de licenciamientos y adiestramientos globales u otros esquemas ventajosas en el ámbito gubernamental. Asimismo, el Artículo 6 de dicha Ley dispone que la OGP podrá contratar servicios, programas y equipos necesarios para cumplir con la política pública establecida mediante esta Ley y en la gestión del Gobierno Electrónico, incluyendo programas globales de licenciamiento y adiestramiento. El establecer este estándar obliga a las dependencias de gobierno, todas las que la Ley 151 establece que están bajo la guía de la OGP con respecto a tecnología, a utilizar este producto/servicio para la funcionalidad especificada.

E. Utilizar el estándar: Seguir el estándar (ver letra D para más detalles). Esto garantiza que se cumplan los objetivos de funcionalidad y metas tecnológicas del gobierno de una manera eficiente e inter-operable.

F. ¿Hay licencias o contrato?: Una licencia es un contrato entre el autor de una aplicación, programa o producto y el usuario, que le permite a este utilizar la aplicación, programa o producto de forma legal. Es una buena práctica establecer contratos globales para comprar licencias o bienes y de esta forma conseguir los beneficios económicos de comprar en grandes cantidades. Comunicarse con Apoyo Técnico de ATI al (787) 725-9420 ext. 2438, 2440 ó 2457, para determinar disponibilidad de licencias y/o contratos globales, y procedimiento a seguir.

G. Entregar licencias / bienes: La OGP entregará licencias y/o bienes disponibles o ejecutará términos de contratos ya firmados para satisfacer necesidad de bienes y/o servicios. Comunicarse

con la OGP para determinar disponibilidad de licencias y/o contratos globales, y procedimiento a seguir.

H. Adquirir licencias / bienes adicionales: Cuando las licencias y/o bienes no estén disponibles pero existen contratos ya firmados, la OGP utilizará los precios ya acordados en estos contratos para solicitar licencias y/o bienes. Todos los costos deberán ser pagados por la agencia que recibe los bienes.

I. ¿Amerita establecer un estándar?: Se considerará establecer un estándar cuando se cumplan al menos dos de las siguientes condiciones:

1. La funcionalidad de este producto es común en varias dependencias del gobierno.
2. Es altamente probable que varias dependencias del gobierno necesiten este producto en el próximo año.
3. La OGP puede obtener beneficios económicos, entre otros, al negociar la adquisición de este producto de manera global para todas las dependencias del gobierno.
4. El estandarizar un producto para la funcionalidad especifica en cuestión facilitará y/o viabilizara la interoperabilidad entre sistemas inter-agenciales y/o sistemas intra-agenciales que comparten la necesidad.
5. El estandarizar un producto para la funcionalidad específica en cuestión facilitará la colaboración de recursos humanos entre agencias que están ejecutando la funcionalidad en común.
6. La adquisición del producto requiere subasta.
7. Se debe incluir en el contrato las siguientes cláusulas:
   El desarrollo e implementación de la aplicación "X" debe quedar completamente documentado, de manera que el contratista deberá entregar los códigos fuentes de los programas desarrollados.
   El contratista reconoce que cualquier diseño, modelo o producto del contrato será considerado propiedad intelectual del Estado Libre Asociado de Puerto Rico, el cual tendrá derecho absoluto sobre los mismos.

J. Solicitar a OGP la creación de un estándar: Es la responsabilidad de OGP el establecer estándares tecnológicos para bienes y servicios. Estos estándares serán el resultado de opiniones de expertos en la evaluación de tecnología y basados en requerimientos para una funcionalidad en específico y tomando en cuenta las mejores prácticas de tecnología, costo-efectividad e interoperabilidad. La creación de un estándar implica una inversión de tiempo, adiestramiento y costo. Estos factores garantizan que se cumplan los objetivos de funcionalidad y metas tecnológicas del gobierno de una manera eficiente e inter-operable.
(Referirse al diagrama: Creación de un estándar)

K. Ver leyes y reglamentos de bienes / servicios: Si el bien o servicio no está bajó la jurisdicción de OGP, ver las leyes y reglamentos de ASG, y políticas y reglamentos internos de las agencias para adquisición de bienes o servicios no tecnológicos.

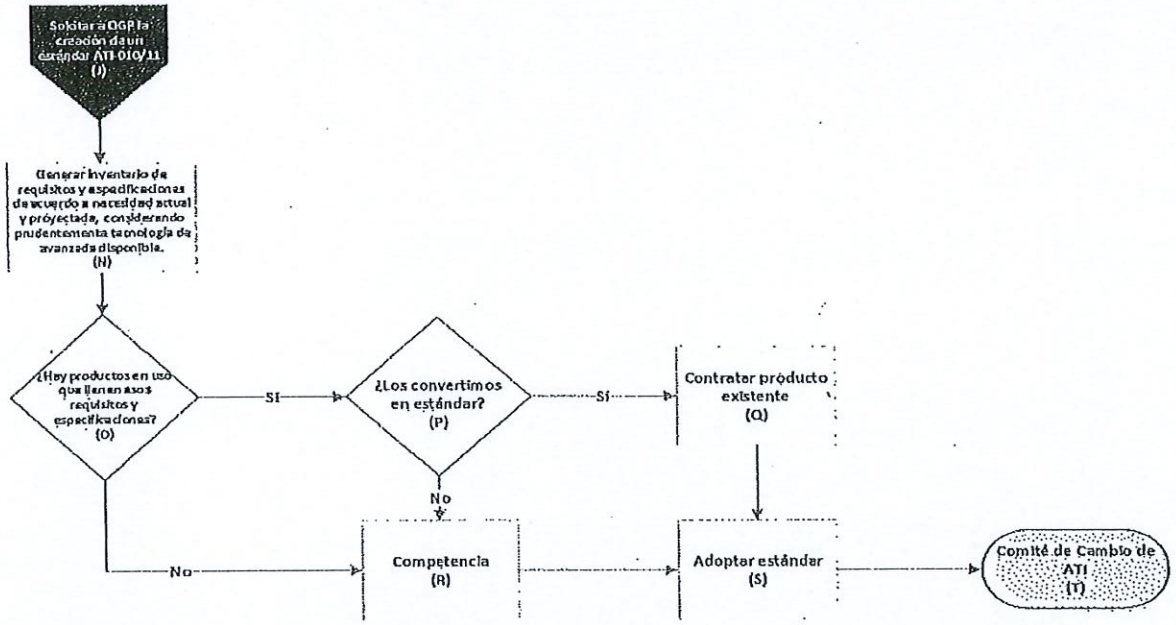
L. Ver mejores prácticas y criterios recomendados para la adquisición de servicios profesionales y consultivos: Los servicios profesionales y consultivos de proyectos de tecnología incluyen: adiestramiento, análisis, estudios, validación, pruebas, apoyo técnico, diseño y administración de

sistemas, desarrollo de programas, implantación, configuración, programación, entre otros. Estos servicios no están sujetos a las mismas reglas de competencia que los bienes. Sin embargo, la OGP recomienda los siguientes criterios de mejores prácticas cuando se contemple la adquisición de servicios tecnológicos:

1. Un mínimo de tres propuestas por escrito por cada contrato
2. Documentación clara y por escrito para casos de único licitador ("sole source")
3. Adherirse a los principios de costo-efectividad; el cosio debe ser razonable aun en casos de único licitador ("sole source")
4. Contratar servicios profesionales y consultivos de firmas de buena reputación y con experiencia previa en los trabajos a contratarse
5. Los servicios tienen que estar bien detallados en el contrato de forma tal que sea fácil y claro el establecer si el proveedor cumplió o no con los mismos.
6. Cualquier conflicto de intereses deben ser identificados y eliminados

M. Políticas de la agencia respectiva: Cuando el bien requerido no cumpla con los criterios para la creación de un estándar, se debe seguir las mejores prácticas según folleto del Contralor (ver referencias al final de esta política) y/o políticas de adquisición de bienes de la agencia pertinente.

Diagrama de OGP: Creación de un estándar



Nota: Referirse a las próximas secciones de esta política para descripción y definiciones.

N. Generar inventario de requisitos y especificaciones: El primer paso para establecer un criterio de estándar es generar las especificaciones y requisitos del producto, aplicación o programa que se requiere. Estas especificaciones y requisitos deben ser los estrictamente necesarios para obtener los resultados presentes y futuros requeridos por los posibles escenarios donde se aplicarán la

solución bajo análisis. El segundo paso es buscar información de mercado sobre la reputación, versatilidad, funcionalidad y compatibilidad de este con respecto a la arquitectura tecnológica del Gobierno de Puerto Rico. Para esto se recomienda:

1. El cumplimiento con la definición detallada de la funcionalidad deseada, que deberá ser sometida por las agencias y revisada/complementada por la OGP.
2. El producto(s) escogido(s) como estándar deberá ser líder, al momento de la selección, en su espacio de la industria. Este liderazgo deberá demostrarse a través de evaluaciones de firmas cotizadas que evalúan tecnologías (ej: Gartner, Inc., International Data Group (IDC.es), Forrester Research, Aberdeen Group, META Group,The Yankee Group, entre otros).
3. La compañía manufacturera deberá demostrar su continua inversión en el mejoramiento del producto. Esto lo demostrará sometiendo el "Product Road Map" que lo demuestre.

O. ¿Hay productos en uso que llenen esos requisitos y especificaciones?: La OGP procederá a ver si este producto, aplicación o programa ya existe en alguna dependencia del gobierno.

P. ¿Los convertimos como estándar?: Una vez determinado que el producto, aplicación o programa en uso cumple con las especificaciones y requisitos presentes y futuros, la dependencia gubernamental y su personal lo recomiendan a la OGP, y hay evidencia de que se siguió el proceso de adquisición, el mismo se convertirá en un estándar para el Gobierno de Puerto Rico.

Q. Contratar productos existentes: Luego de que se adopte el nuevo estándar, la OGP contratará el mismo utilizando las mejores prácticas de negociación. (Se requiere demostrar que hubo competencia en la adquisición inicial)

R. Competencia: Competir la adquisición de producto, aplicación o programa utilizando desde cotizaciones por escrito para compras menores hasta RFP ("Request for Proposal") para adquisición de productos, programas o aplicaciones para compras mayores. Lo importante es establecer la competencia como factor que garantice el mejor precio posible y de acuerdo a las políticas de adquisición de la OGP y las mejores prácticas establecidas y/o recomendadas por ASG y la Oficina del Contralor.

S. Adoptar estándar: Esto implica que el producto, aplicación o programa pasará de inmediato al listado virtual de estándares tecnológicos de OGP y que todas las Agencias o dependencias gubernamentales deben seguir este nuevo estándar tecnológico de OGP cuando adquieran este tipo de solución, según dispone la Ley Núm. 151 de Gobierno electrónico.

T. Comité de Cambio de ATI: Se establecerá un comité para la revisión y creación de estándares compuesto por el Director Asociado de Tecnologías de Información de OGP, el Gerente designado de la División de Operaciones, el Gerente designado de División de Apoyo Técnico y el Gerente de Infraestructura. Este comité se reunirá regularmente para revisar los estándares establecidos por OGP y hará recomendaciones al respecto.

CUMPLIMIENTO

Las agencias son responsables de reflejar en el Legado Estratégico Anual Tecnológico, Lean-Tech, la adherencia y cumplimiento con la Política de Mejores Prácticas de Infraestructura Tecnológica.

EXENCIONES

Si una agencia desea obtener una exención para desviarse de la política aquí descrita deberá someter una justificación escrita a la OGP por conducto del Director Asociado de ATI, quien evaluará los méritos y notificará de su decisión por escrito a la Agencia y a la Administración de Servicios Generales.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como "Ley de Contabilidad del Gobierno del Puerto Rico"
Política Núm. ATI-010, Adquisición de Equipo para Sistemas Computadorizados de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-011, conocida como Mejores Prácticas de Infraestructura Tecnológica, revisada el 7 de noviembre de 2016
Folleto informativo de las Mejores Prácticas para la Adquisición, Desarrollo, Utilización y Control de la Tecnología de Información (Oficina del Contralor, enero 2006)

ANTECEDENTE

Política Núm. TIG-013, conocida como Marco Referencial de Adquisición de Tecnología Gubernamental de 1ro de julio de 2006.

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-014

FECHA DE EFECTIVIDAD: 7 de noviembre de 2016

TEMA: Manejo de *Firewalls*

DESCRIPCIÓN DE LA POLÍTICA

El propósito de esta política es establecer que toda agencia debe tener, al menos, un dispositivo o conjunto de dispositivos conocido como *firewall* que controle el acceso al internet y personal capacitado para el manejo del mismo.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.*, Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos. Asimismo, aplica a cualquier otro organismo gubernamental que esté conectado a la Red Interagencial.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable por la actualización de esta política.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico deberá seguir las políticas aquí dispuestas sobre manejo de *firewall*. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos internos para cumplir la política aquí delineada.

A. Protección Mínima

1. Toda agencia debe tener un *firewall* protegiendo, como mínimo, su conexión a internet.
2. Si el *firewall* requiere algún licenciamiento, el mismo debe estar vigente.
3. Se deben hacer resguardos periódicos de la configuración del *firewall* en un sistema de almacenamiento alterno (no en el mismo dispositivo). El acceso a este resguardo debe estar restringido sólo al personal responsable de administrar el equipo.

B. Personal

1. Toda agencia debe tener personal capacitado y adiestrado en seguridad y en el manejo de *firewalls*. En caso de delegarse a un tercero, éste debe estar capacitado y certificado en seguridad y manejo de *firewalls*.
2. Típicamente el personal de sistemas de información está demasiado ocupado trabajando con asuntos de mantenimiento y soporte de los sistemas informáticos y la seguridad es un tema sumamente complejo y sensitivo que, en muchas ocasiones, requiere personal especializado. Así las cosas, en agencias donde la complejidad de la seguridad lo requiera por necesidad de cumplimiento de regulaciones federales, tales como HIPAA, SOX, FISMA y otras leyes análogas, es recomendable que exista un Oficial de Seguridad Informática, Gerente de Seguridad Informática, Especialista en Seguridad Informática o sus equivalentes, debido a los retos técnicos que, regularmente, supone la implementación de políticas y controles para tal cumplimiento.
3. Un candidato para las posiciones antes mencionadas debe tener una combinación entre educación, experiencia y adiestramiento para ser cualificado como experto en seguridad.[1]
    a. Oficial/Especialista en Seguridad Informática
        i. El candidato debe poseer al menos un bachillerato en ingeniería (computadoras, telecomunicaciones o campos relacionados), ciencias de computadoras o sistemas de información de una universidad acreditada.
        ii. Es altamente deseable que el candidato posea alguna de las siguientes certificaciones: CEH[2], OSCP[3], CHFI[4]o su equivalente.
        iii. El candidato debe tener cinco (5) o más años de experiencia en tareas relacionadas a la seguridad y al cumplimiento de regulaciones federales.
    b. Gerente de Seguridad Informática
        i. El candidato debe poseer al menos un bachillerato en ingeniería (computadoras, telecomunicaciones o campos relacionados), ciencias de computadoras o sistemas de información de una universidad acreditada.
        ii. Es altamente deseable que el candidato posea alguna de las siguientes certificaciones: CISSP[5] o su equivalente; GIAC[6]o su equivalente; CISM[7] o su equivalente.
        iii. Diez (10) años o más de experiencia en el campo de las tecnologías de información con historial sólido en seguridad de la información y en el área de cumplimiento de regulaciones federales y, al menos, cinco (5) años en experiencia gerencial.

C. Adiestramientos

1. La agencia es responsable de proveer notificaciones a toda la gerencia y los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes. A tales fines, deberán celebrar charlas periódicas, para orientar al personal de las políticas y controles de seguridad establecidos.
2. El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
4. La agencia es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

D. Reglas Mínimas

1. *Firewalls* Perimetrales
    a. Denegar todo tráfico que no esté explícitamente permitido en ambas direcciones (*inbound* and *outbound*)
    b. Permitir de salida (*outbound*) sólo los puertos que se utilizan
        i. Ejemplo
            1. Acceso a Internet
                a. DNS (UDP y TCP 53) a DNS de la red interagencial (típicamente sólo el DNS interno de la agencia es el que debe tener acceso a DNS)
                b. HTTP (80)
                c. HTTPS(443)
2. Filtros de Contenido de Internet
    a. Deben poseer, al menos, una política base que bloquee pornografía y que aplique a TODO el personal.

E. Leyes y Reglamentos

1. Las políticas y procedimientos de seguridad deberán estar de acuerdo con la legislación y reglamentación vigentes.

EXENCIONES

Ninguna

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Firewall – un dispositivo o combinación de dispositivos configurados para permitir, denegar y/o cifrar entre los diferentes segmentos de seguridad, basado en una serie de reglas u otros criterios.

FISMA – Federal Information Security Management Act, 44 USC § 3541 *et seq*. Es una legislación federal que define una plataforma comprensiva para proteger información, operaciones y activos del gobierno en contra de amenazas naturales o realizadas por el hombre. FISMA fueintegrada al "Electronic Government Act of 2002", 44 USC § 101 *et seq*.[8]

HIPAA – Health Insurance Portability and Accountability Act, Pub.L. No. 104-101, 110 Stat. 1936 (1996). La Oficina de Derechos Civiles tiene la responsabilidad de hacer cumplir la Regla de Privacidad de la Ley HIPAA, la cual protege la información de salud individualmente identificable; la Regla de Seguridad HIPAA, la cual establece los estándares nacionales para la seguridad electrónica de la información de salud protegida; la Regla de Notificación de Violación de Seguridad, la cual requiere que las entidades y los asociados de negocio cubiertos a proveer una notificación luego de una violación de seguridad de la información de salud protegida; y las disposiciones sobre confidencialidad de la Regla de Seguridad del Paciente, la cual protege la información de identidad utilizada para analizar los eventos de seguridad del paciente y mejorar la seguridad del paciente.[9]

SOX – The Sarbanes-Oxley Act, Pub. L. No. 107-204,116 Stat. 745(2002), también conocida como Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. Se puso en efecto en julio de 2002 e introdujo grandes cambios a la regulación de la gobernanza corporativa y la práctica financiera.

ANEJOS

Ninguno

REFERENCIAS

POLITICA NÚM. ATI-003, Seguridad de los Sistemas de Información, revisada el 7 de noviembre de 2016
Corporate Firewall Policy [Pdf Format].(2008). In www.shortinfosec.net.Retrieved from http://www.shortinfosec.net/2008/01/downloads.html
Ley Sarbanes-Oxley.(Jan 12, 2015).In http://www.sec.gov. Retrieved fromhttp://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

---

[1]Sample-Job-Descriptions-Complete. In https://msisac.cisecurity.org
[2]EC-Council Certified Ethical Hacker http://www.eccouncil.org/
[3]Offensive Security Certified Professional https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
[4] EC-Council Computer Hacking Forensic Investigator http://www.eccouncil.org/certification/computer-hacking-forensics-investigator
[5]Certified Information System Security Professional https://www.isc2.org/cissp/default.aspx
[6] Global Information Assurance Certification http://www.giac.org/
[7]Certified Security Information Manager http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/Pages/default.aspx
[8] http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
[9]http://health.state.tn.us/hipaa/

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-015

FECHA DE EFECTIVIDAD: 30 de septiembre de 2011
FECHA DE REVISIÓN: 12 de octubre de 2016

TEMA: PROGRAMA DE CONTINUIDAD GUBERNAMENTAL

DESCRIPCIÓN

Esta política consiste de directrices generales que permitirán a las agencias establecer un programa adecuado para garantizar la continuidad operacional de las funciones críticas que la agencia maneja. Dispone las guías que regirán el Programa de Continuidad Gubernamental con el objetivo de establecer con antelación la planificación y preparación necesaria, para minimizar pérdidas y preservar la continuidad de todas las funciones críticas de las agencias adscritas a la Rama Ejecutiva del Gobierno del Estado Libre Asociado de Puerto Rico ante la eventualidad de un incidente que pueda interrumpir sus operaciones y que pueda crear un estado de emergencia o desastre.

La misma deroga y sustituye la Política Núm. TIG-015, sobre Programa de Continuidad Gubernamental, revisada el 12 de septiembre de 2011.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. Entre otros aspectos, la OGP debe proyectar la utilidad de las tecnologías de la información para prevenir accidentes y preparar planes de contingencia que permitan al gobierno reaccionar adecuadamente en caso de crisis para el restablecimiento de sistemas y datos en caso desastre en el menor tiempo posible. *Id.*, Art. 5, inciso (m). A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.*, Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACION DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualizan las políticas concernientes al Programa de Continuidad Gubernamental.

POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Gobierno de Puerto Rico deberá seguir las siguientes políticas de continuidad establecidas. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables para cumplir la política aquí delineada.

Área de Tecnologías de Información

El Área de Tecnologías de Información (ATI) de la Oficina de Gerencia y Presupuesto, establece la estructura y formatos relacionados con los informes, programas y procedimientos que forman parte del Programa de Continuidad Gubernamental:

1. Desarrollo y estructuración de todas las políticas conducentes al establecimiento de la continuidad en todas las funciones y procesos críticos de la agencia.
2. Establecimiento de una Estructura de Continuidad en la Agencia.
3. Formato para un Análisis de Riesgos.
4. Formatos para un Análisis de Impactos.
5. Componentes de un Plan de Recuperación de Desastres (Disaster Recovery Plan - DRP).
6. Componentes de un Plan de Continuidad Gubernamental (Business Continuity Plan - BCP).
7. Formato para un Plan de Manejo de Incidentes.
8. Formato para un Programa de Manejo de Emergencias.
9. Formato para un Programa de Comunicación de Crisis.
10. Formato para un Programa de Pruebas y Ejercicios.
11. Componentes para un Programa de Concientización y Adiestramientos en continuidad.
12. Estructura de procedimientos relativos a la coordinación con otras autoridades públicas.

A. Desarrollo de Políticas de Continuidad

1. Se establece que todas las agencias deben establecer políticas de continuidad conducentes a lograr el cumplimiento con ATI.

2. Será responsabilidad de cada agencia de seguir y cumplir con la metodología de continuidad establecida tomando en cuenta las características propias de la agencia en base a sus operaciones y de los ambientes de tecnología existentes.

3. Las políticas desarrolladas por la OGP para su uso interno podrán ser utilizadas como modelos iniciales en el desarrollo de las políticas específicas de cada agencia.

B. Estructura de Continuidad

1. Es requerido que cada agencia establezca una estructura organizacional de continuidad. Los directores de las agencias serán los líderes del programa de continuidad de la agencia y serán responsables de la implantación y cumplimiento del programa en la agencia. El líder de continuidad asignará un coordinador de continuidad el cual será responsable por el desarrollo de todas las actividades y ejecución del programa de continuidad de la agencia.

2. Los miembros de la estructura de continuidad de la agencia participarán en el proceso de planificación y de toma de decisiones del programa de continuidad de la agencia.

C. Análisis de Riesgos – Risk Analysis (RA)

El Análisis de Riesgos es un informe gerencial en el cuál se establece el nivel de vulnerabilidades ante la exposición de riesgos y la efectividad de los controles existentes de la agencia. También provee información crítica para la elaboración del Programa de Manejo de Emergencias. Como parte del Programa de Continuidad Gubernamental se establece que:

1. Todas las agencias debe realizar Análisis de Riesgo dentro de un límite mínimo de tiempo de 24 meses y/o cuando se realice un cambio significativo dentro de su infraestructura operacional.

2. El desarrollo y análisis de los resultados del Análisis de Riesgos deberá ser certificado de acuerdo a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

C. Análisis de Impacto Gubernamental – Business Impact Analysis (BIA)

El Análisis de Impacto es un informe gerencial en el cual se determina los impactos cualitativos y cuantitativos a través de una interrupción en los procesos críticos. El Análisis de Impacto permite determinar los niveles de criticidad de los procesos críticos de la agencia, los requerimientos de operación y el tiempo de recuperación operacional (Recovery Time Objective – RTO) y tiempo de resguardo requerido (Recovery Point Objective - RPO). Como parte del Programa de Continuidad Gubernamental se establece que:

1. Todas las agencias deben realizar un Análisis de Impacto dentro de un límite mínimo de tiempo de 24 meses y/o cuando se realice un cambio significativo dentro de su infraestructura operacional.

2. El desarrollo y análisis de los resultados del Análisis de Impacto deberá ser certificado de acuerdo a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

D. Plan de Recuperación de Desastres – Disaster Recovery Plan (DRP)

El Plan de Recuperación de Desastres – Disaster Recovery Plan (DRP) son las tareas, actividades y procedimientos formales que ejecuta la Unidad de Tecnología y Sistemas de Información conducentes al restablecimiento de los sistemas críticos de procesamiento de la agencia ante la eventualidad de un desastre y/o contingencia. Como parte del Programa de Continuidad Gubernamental se establece que:

1. Todas las agencias debe tener implantado, ejercitado y probado su Plan de Recuperación de Desastres. El Plan de Recuperación de Desastres será actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

2. El Plan de Recuperación de Desastres deberá tener establecido las estrategias de respuesta, recuperación, reanudación y de restauración para todos los procesos críticos de la agencia tanto a nivel de las plataformas de procesamiento y de sus comunicaciones. Las estrategias de continuidad establecidas por la agencia estarán basadas en los tiempos de recuperación y resguardos (RTO/RPO) de sus procesos críticos obtenidos en el informe del Análisis de Impacto.

3. La elaboración e implantación del Plan de Recuperación de Desastres deberá ser basado conforme a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

E. Plan de Continuidad Gubernamental – Business Continuity Plan (BCP)

El Plan de Continuidad Gubernamental son las tareas, actividades y procedimientos formales que ejecuta las diferentes unidades de la agencia conducentes al restablecimiento de los sistemas críticos de procesamiento ante la eventualidad de un desastre y/o contingencia. Como parte del Programa de Continuidad Gubernamental se establece que:

1. Todas las agencias debe tener implantado, ejercitado y probado su Plan de Continuidad Gubernamental. El Plan de Continuidad Gubernamental será actualizado cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

2. El Plan de Continuidad Gubernamental deberá tener establecido las estrategias de respuesta, recuperación, reanudación y de restauración para todos los procesos críticos de las unidades de la agencia. Las estrategias de continuidad establecidas por la agencia estarán basadas en los resultados obtenidos en el informe del Análisis de Impacto.

3. El Plan de Continuidad Gubernamental deberá incluir los requerimientos mínimos de operación de cada una de las unidades de la agencia.

4. El Plan de Continuidad Gubernamental deberá incluir la documentación de los procedimientos de respuesta, recuperación, reanudación y restauración de las diferentes unidades de la agencia.

5. La elaboración e implantación del Plan de Continuidad Gubernamental deberá ser basado conforme a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

E. Plan de Manejo de Incidentes

Un Plan de Manejo de Incidentes es una serie de actividades documentadas que serán ejecutadas por los diferentes grupos de continuidad de una agencia en respuesta a un incidente que interrumpa la prestación de sus servicios por un periodo determinado de tiempo. Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. Desarrollar una estructura en la agencia para el Manejo de Incidentes.

2. Desarrollar procedimientos para detectar, reportar y responder a cualquier tipo de incidente que cause interrupción en la prestación de sus servicios.

3. Asegurarse que todos sus empleados, visitantes y contratistas ejecuten los procedimientos de manejo de incidentes establecidos.

4. La elaboración e implantación del Plan de Manejo de Incidentes deberá ser basado conforme a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

F. Programa de Manejo de Emergencias

Un Programa de Manejo de Emergencias tiene como propósito es proteger y salvaguardar vidas y responder efectivamente ante la eventualidad de un desastre. El Programa de Manejo de Emergencias debe incluir las actividades prevención y de respuesta ante desastres naturales y otros tipos en los que sea necesario activar los procedimientos de desalojo de las facilidades. Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. Desarrollar procedimientos de prevención, respuesta para cualquier tipo de desastre natural que cause interrupción en la prestación de sus servicios.

2. Asegurarse que todos sus empleados, visitantes y contratistas ejecuten los procedimientos de desalojo establecidos.

3. La elaboración e implantación del Programa de Manejo de Emergencias deberá ser basado conforme a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

G. Programa de Comunicación de Crisis

Un Programa de Comunicación de Crisis tiene como propósito definir y proveer un canal formal y claro de comunicación existente en la Agencia a Nivel Interno (Empleados, Junta de Directores), Externo (Clientes, Suplidores), Autoridades Públicas y ante los Medios de Comunicación (Prensa, Radio, Televisión y otros) ante la eventualidad de un incidente y/o desastre. El Programa de Comunicación de Crisis de las agencias deberá:

1. Asignar los portavoces oficiales de la agencia
2. Definir los Medios de Comunicación (Prensa, Radio, Televisión y otros)
3. Establecer guías para enfrentar situaciones adversas y para asegurarnos de que todo el personal y los portavoces están familiarizados con los procedimientos básicos de comunicaciones y su rol ante la eventualidad de una crisis.
4. Elaborar e implantar el Programa de Manejo de Comunicación de Crisis en base a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

H. Programa de Pruebas y Ejercicios

El Programa de Pruebas y Ejercicios describe el diseño, desarrollo, ejecución, evaluación y validación de la funcionalidad de las actividades y procedimientos de mitigación, respuesta, recuperación, reanudación y de restauración para todas las funciones y procesos críticas de negocios de la Agencia.

Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. Toda Agencia deberá realizar al menos un ejercicio y una prueba anualmente para todas sus unidades simulando escenarios de desastre o interrupción del negocio para garantizar que su Plan de Continuidad de Negocios puede ser implementado en situaciones reales de emergencia y desastres.

2. Cada Agencia deberá documentar todos los ejercicios y pruebas de continuidad de los diferentes grupos de continuidad.

3. Se elabore y se implante el Programa de Pruebas y Ejercicios en base a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

I. Programa de Concientización y Adiestramientos

El Programa de Concientización y de Adiestramiento tiene como propósito promover en sus empleados el conocimiento de todas las actividades del Programa de Continuidad de la Agencia.

Se establece en el Programa de Continuidad Gubernamental que las agencias deberán:

1. Desarrollar un Programa de Adiestramiento a Nivel Básico, Intermedio y Avanzado para todo el personal. Dichos adiestramientos serán asignados basados en la responsabilidad de continuidad a ser realizada por los empleados.

2. La elaboración e implantación del Programa de Concientización y Adiestramientos deberá ser basado conforme a las prácticas profesionales de continuidad establecidas por el Disaster Recovery Institute International (DRII).

J. Proceso de Coordinación con otras Autoridades Públicas

Se requiere que toda agencia tenga documentado todas las actividades y procedimientos de coordinación con las diferentes autoridades públicas ante la eventualidad de un incidente y/o desastre.

K. Políticas de Continuidad Adicionales

Las políticas escritas en este documento no podrán ser invalidadas por las políticas particulares desarrolladas en cada agencia.

L. Leyes y Reglamentos

Las políticas y procedimientos de continuidad deberán estar de acuerdo a la legislación y los reglamentos vigentes.

M. Personal

Cada agencia será responsable de tener el personal necesario ya sea interno o contratado para diseñar y mantener el Programa de Continuidad Gubernamental.

O. Manejo de Cambios

La agencia es responsable de diseñar procedimientos que permitan que los cambios a los procedimientos de continuidad sean realizados y documentados adecuadamente y que esta documentación a su vez sea asegurada.

EXENCIONES

Ninguna

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Análisis de Riesgos – Risk Analysis (RA) - Es un informe gerencial que determina la probabilidad y el impacto de una variedad de amenazas específicas que pueden causar la interrupción de negocios.

Análisis de Impacto – Business Impact Analysis (BIA) - Es un informe gerencial en el cual se determina la prioridad en los procesos críticos de negocios, sus impactos cualitativo y cuantitativos, los costos por interrupciones y el tiempo de recuperación necesario de los procesos críticos. Se utiliza para justificar la inversión en las estrategias de continuidad.

Amenaza - Evento que ocasiona que un riesgo se vuelva una pérdida real en los activos de la compañía

Control - Proceso o dispositivo que disminuye el efecto de una Amenaza. (Reduce el efecto, pero no puede prevenir la ocurrencia)

Desastre - Cualquier evento que crea la inhabilidad a una compañía de proveer las funciones criticas de negocios por un periodo pre-determinado de tiempo.

Emergencia - Un evento no-planificado que puede causar daños y/o muertes a empleados, clientes o al público, daños ambientales o físico a las área de operación.

Gobierno - Se refiere al Estado Libre Asociado de Puerto Rico.

Plan de Continuidad Gubernamental – Business Continuity Plan (BCP) - La planificación y preparación con la antelación de tiempo necesario para minimizar pérdidas y asegurar la continuidad de las funciones críticas de una organización ante la eventualidad de un desastre y/o contingencia

Plan de Recuperación de Desastres – Disaster Recovery Plan (DRP) - Son las tareas, actividades y procedimientos formales que ejecuta la unidad de Tecnología y Sistemas de Información conducentes al restablecimiento de los sistemas críticos de procesamiento ante la eventualidad de un desastre y/o contingencia.

Riesgo – Exposición a pérdida, lesión, peligro, potencial de pérdida.

Vulnerabilidad - Exposición a un evento que puede ocasionar la pérdida real de los activos de la compañía

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Prácticas Profesionales de Continuidad – Disaster Recovery Institute International

ANTECEDENTE

Política Núm. TIG-015, sobre Programa de Continuidad Gubernamental, revisada el 12 de septiembre de 2011.

OFICINA DE GERENCIA Y PRESUPUESTO
ESTADO LIBRE ASOCIADO DE PUERTO RICO

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-016 **FECHA DE EFECTIVIDAD:** 7 de noviembre de 2016

TEMA: INTERFAZ DE PROGRAMACIÓN
("APPLICATION PROGRAMMING INTERFACE- API")

DESCRIPCIÓN DE LA POLÍTICA

El Área de Tecnología de Información (ATI) de la Oficina de Gerencia y Presupuesto (OGP) ha identificado la necesidad de desarrollar e implementar interfaces de programación de aplicaciones (API's) para automatizar, simplificar y facilitar la prestación de servicios a la ciudadanía y la interoperabilidad entre las agencias, departamentos, oficinas e instrumentalidades del Estado Libre Asociado de Puerto Rico. Esta política establece las guías principales para el desarrollo y la adopción de interfaces de programación de aplicaciones.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.,* Art. 5, inciso (i). Además, deberá evaluar y asesorar, de acuerdo a los criterios adoptados, loso sistemas de procesamiento electrónico e interconexión del gobierno de manera que los mismos propiicies, facilite y agilicen los procesos interagenciales. *Id.,* inciso (m). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

ALCANCE

Esta política aplica a cualquier desarrollo o implantación de API's por parte de cualquier agencia, de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación.

POLÍTICA

NORMAS GENERALES

1. El desarrollo de cualquier API por parte de las agencias deberá realizarse en cumplimiento de lo aquí recomendado.

2. La agencia no podrá realizar cambios a sus API's que quebranten o interfieran con la conectividad, la compatibilidad y el funcionamiento de los sistemas en producción ya existentes (propios o de otras agencias) salvo en aquellos casos donde se esté llevando a cabo una restructuración mayor de la base de datos en cuyo caso, se llevará a cabo un proceso de divulgación por medio de mensajería electrónica a las entidades previamente autorizadas y que tengan API's en producción.

3. La agencia deberá migrar sus servicios "web" existentes de acuerdo a las guías y los aspectos técnicos detallados en la política que aquí se promulga, sin afectar la conectividad, la compatibilidad y el funcionamiento de los sistemas ya en producción.

4. La agencia que contrate servicios relacionados a bases de datos deberá exigir que se desarrolle una documentación técnica que detalle, explique y facilite la adopción y utilización de sus API's.

5. La agencia que contrate servicios de manejo de sistemas y bases de datos debe exigir el desarrollo de un API sobre dicha base de datos que cumpla con lo aquí promulgado.

6. La agencia será responsable de cumplir con las leyes y los reglamentos de privacidad y confidencialidad aplicables a nivel estatal y federal para garantizar la seguridad, el acceso, el uso y el manejo adecuado de los servicios y datos transmitidos a través de la interfaz de programación de aplicaciones.

7. La agencia deberá propiciar la automatización de los servicios, los documentos, los procesos y las necesidades de datos requeridas por otra agencia gubernamental mediante el desarrollo de interfaces de programación de aplicaciones.

8. La agencia deberá propiciar la publicación de datos y la información pública para el acceso, uso y consumo por cualquier agencia gubernamental y la ciudadanía, mediante el desarrollo de interfaces de programación de aplicaciones.

9. Todo proyecto de base de datos debe considerar la interconexión de los datos con sus respectivas dependencias y/o agencias.

GUÍAS

1. La agencia deberá establecer los mecanismos tecnológicos necesarios para garantizar el funcionamiento continuo de sus interfaces de programación de aplicaciones.

2. La agencia deberá establecer mecanismos confiables y aceptables de seguridad para poder acceder y utilizar sus interfaces de programación de aplicaciones. El ATI podrá establecer guías

y documentos técnicos que elaboren y profundicen sobre los aspectos de seguridad que deben implementar las agencias.

3. Se propiciará el desarrollo de interfaces de programación de aplicaciones que publiquen datos actualizados en tiempo real.

4. La agencia podrá desarrollar sus API's con los recursos propios de ésta e implementarlos en la infraestructura propia de la agencia. No obstante, ATI estará disponible para asistir en el desarrollo o implementación de las interfaces de programación de aplicaciones.

5. La agencia podrá implementar sus interfaces de programación de aplicaciones en la nube en cumplimiento con la Política de Tecnologías en la Nube (ATI-012).

ASPECTOS TÉCNICOS

En aras de garantizar un desarrollo adecuado y establecer una plataforma de interoperabilidad entre las diferentes agencias y sus interfaces de programación de aplicaciones, se deberá cumplir con los siguientes aspectos técnicos:

1. Se propiciará el desarrollo de interfaces de programación de aplicaciones utilizando las tecnologías y los estándares abiertos para facilitar la colaboración y el desarrollo de nuevas funcionalidades entre las diferentes agencias

2. Los cambios, las mejoras y las nuevas funcionalidades a interfaces de programación de aplicaciones existentes deberán desarrollarse utilizando un diseño que contemple el manejo de versiones ("API versioning") para no afectar la compatibilidad con los sistemas que utilizan versiones anteriores de la interfaz.

3. Los APIs desarrollados se harán disponibles en un repositorio común que proveerá la ATI en OGP.

EXENCIONES

Quedan exentos de la aplicabilidad de esta política aquellos servicios "web" ("web services") ya existentes y que sean utilizados por aplicaciones en producción por cualquier agencia o entidad gubernamental.

No obstante, los cambios, y las mejoras y futuras versiones de dichos servicios "web" deberán realizarse a tenor con esta política, sin quebrantar la compatibilidad y funcionalidad de los servicios existentes y en uso.

Las agencias deberán favorecer la migración de sus servicios "web" a tenor con esta política.

DEFINICIONES

Agencia - Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Gobierno - Se refiere al Gobierno del Estado Libre Asociado de Puerto Rico.

Interfaz de programación ("Web API" o "API") - Conjunto de funciones que permite la comunicación entre aplicaciones y representan la capacidad de comunicación entre componentes de "software." Éstas permiten la comunicación a través del Internet por una entidad externa con aplicaciones internas del Gobierno, con el objetivo de permitir el libre acceso, de manera segura, a entidades autorizadas y previamente autorizadas, con información del Estado Libre Asociado.

Servicio Web o "Web Service"- Un servicio web (en inglés, Web services) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Política Núm. ATI-012, Política de Tecnologías en la Nube, de 7 de noviembre de 2016

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN
OFICINA DE GERENCIA Y PRESUPUESTO

POLÍTICA NÚM. ATI-017 **FECHA DE EFECTIVIDAD:** 7 de noviembre de 2016

TEMA: REVISIÓN DE CONTRATOS DE TECNOLOGÍA

DESCRIPCIÓN

Esta política establece las normas aplicables a la contratación de bienes y servicios de informática en el Estado Libre Asociado de Puerto Rico.

BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar la política pública a seguir y las guías que regirán la adquisición e implantación de los sistemas, equipos y programas de información tecnológica para los organismos gubernamentales. *Id.*, Art. 6, inciso (l), (i) y (iii). Asimismo, está autorizada a requerir la información y los documentos que entienda necesarios para la incorporación de procesos y servicios gubernamentales al Gobierno Electrónico. *Id.*, Art. 6, inciso (a). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.*, Art.7, incisos (g) y (h).

ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos.

ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se promulga política concerniente a la contratación de bienes y servicios de informática.

POLÍTICA

La contratación de bienes y/o servicios de informática por parte de las agencias de la Rama Ejecutiva deberá cumplir con la normativa que se expone a continuación:

1. Los bienes o servicios propuestos deben tener algún tipo de garantía asociada a los mismos. En el caso de bienes, la garantía debe incluir un período dentro del cual el suplidor del bien es responsable de todas las reparaciones del mismo y de reemplazarlo de ser necesario. En el caso de servicios, la garantía consiste de tener que volver a prestar los servicios de éstos no ser aceptados por la agencia contratante. La agencia contratante tiene la opción de no permitir al suplidor prestar los servicios nuevamente y contratar a un tercero, así como de realizar cualquier reclamación para la devolución de prestaciones realizadas, según proceda. De una agencia entender que los servicios prestados por un proveedor fueron deficientes y por lo tanto no aceptados, informará de dicha situación a la ATI para que esta situación sea divulgada a todas las agencias.

2. En el caso de servicios críticos de infraestructura como lo son redes, Internet y telecomunicaciones, éstos tendrán una garantía de nivel de servicio y unos mínimos de disponibilidad para ser elegibles a pago o en su defecto, que hayan penalidades asociadas al no cumplimiento de los niveles de servicio o la disponibilidad estipulados.

3. En el caso de servicios de programación, todo código se debe entregar en formato electrónico en los servidores o sistemas de almacenaje de los ambientes técnicos de prueba y/o producción, así como en un medio portátil como un CO, OVO o memoria USB.

4. Toda base de datos debe tener cláusulas de control por parte de la agencia e incluir esquema de la misma y políticas para establecer desarrollo escalable de aplicaciones sobre la base de datos con cualquier suplidor externo.

5. En el caso de código web, la interfaz del usuario debe cumplir con la Política Núm. ATI-02, sobre Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites") y las estipulaciones de la Sección 508 of the Rehabilitation Act (https://www.section508.gov/).

6. En todos los casos, los suplidores deben de tomar las medidas necesarias para salvaguardar la disponibilidad, integridad y confidencialidad de los datos que sus tecnologías manejan. Además deben cumplir con todas las leyes estatales y federales aplicables a sus bienes o servicios.

7. La propiedad intelectual de cualquier código o desarrollo hecho para cualquier agencia contratante es propiedad del Estado Libre Asociado de Puerto Rico y podrá ser utilizado en cualquier otra agencia sin tener que incurrir en costos adicionales de licenciamiento para ese código o desarrollo.

8. En cualquier contratación de bienes o servicios, se requerirá el desarrollo de documentación que justifique la compra del bien o la ejecución de proyecto o la contratación de servicios.

9. En cualquier contratación de bienes o servicios, será requisito el proveer capacitación al personal de la agencia contratante y constancia de la transferencia de conocimientos del proveedor a los recursos internos de la agencia

10. En cualquier contratación el código, los procesos y sistemas envueltos, aún cuando estén bajo el control de la contraparte, están sujetos a auditoría por parte de la agencia contratante, y la Oficina del Contralor de Puerto Rico

11. En toda contratación de bienes o servicios de tecnología, se obtendrá la autorización previa de ATI. Serán de aplicación aquellos criterios generales de la contratación gubernamental de bienes o servicios, según procedan.

12. Toda contratación de bienes o servicios de tecnología deberá ser conforme a la Política Núm. ATI-010, Adquisición de Equipos para Sistemas Computarizados de Información, la Política Núm. ATI-011, Mejores Prácticas de Infraestructura Tecnológica, y/o la Política Núm. ATI-013, Marco Referencial de Adquisición Tecnológica Gubernamental, de 12 de octubre de 2016, según apliquen. Asimismo, deberá ser conforme a cualquier normativa emitida por la OGP al amparo de la Ley 151-2004, según *supra*.

13. Los contratos de tecnología que abarquen aplicaciones o desarrollos deberán contener el siguiente lenguaje:

    PRIMERA: El desarrollo e implementación de la aplicación "X" debe quedar completamente documentado. De manera que, el contratista deberá entregar los códigos fuentes de los programas desarrollados. Todo código será entregado en formato electrónico en los servidores o sistemas de almacenaje de los ambientes técnicos de prueba y/o producción, así como en un medio físico, como un CD, DVD o memoria USB. Dicha entrega resulta esencial para adiestrar a nuestro personal y facilitar el mantenimiento de las aplicaciones y sus programas. Siendo ello así, la aplicación "X" debe ser documentada en su totalidad por el contratista para el beneficio de nuestra agencia utilizando metodologías de desarrollo y documentación estándares o de uso común.

    SEGUNDA: El contratista reconoce que cualquier diseño, modelo o producto de este Contrato será considerado propiedad intelectual del Estado Libre Asociado de Puerto Rico, el cual tendrá derecho absoluto sobre los mismos. Disponiéndose que el contratista no tendrá derecho alguno sobre los productos desarrollados y la documentación completa. En vista de ello, la solución podrá ser utilizada en cualquier otra agencia o instrumentalidad pública del Estado Libre Asociado de Puerto Rico sin tener que incurrir en costos adicionales de licenciamiento por el código o desarrollo.

    TERCERA: Como parte de este Contrato, y durante la fase de implementación de la aplicación "X", el contratista se compromete a proveer adiestramientos y/o capacitación técnica a los usuarios y al personal de nuestra agencia. A esos efectos, el contratista ofrecerá los siguientes talleres: (a) _____, (b) _____, (c) _____, y (d) _____. Asimismo, el contratista brindará el siguiente apoyo durante la instalación de la solución: _____.

CUARTA: Una vez la aplicación "X" haya sido puesta en producción, el contratista proveerá el mantenimiento y las actualizaciones necesarias para garantizar la disponibilidad, continuidad e integridad de la solución. En este sentido, las partes contratantes convienen lo siguiente: (espacio de tiempo) + (remuneración). El contratista se asegurará de que nuestra agencia cuente en todo momento con la documentación completa y actualizada de la aplicación en producción.

EXENCIONES

Ninguna

DEFINICIONES

Agencia – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

Jefe de Agencia - Se refiere al Director, Administrador, Secretario o Jefe que dirige una agencia.

ANEJOS

Ninguno

REFERENCIAS

Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico"
Sección 508 del *Rehabilitation Act* of 1973
Política Núm. ATI-02, sobre Desarrollo y Mantenimiento de Sitios "Web" Agenciales ("Web Sites"), revisada el 7 de noviembre de 2016
Política Núm. ATI-010, Adquisición de Equipos para Sistemas Computarizados de Información, revisada el 7 de noviembre de 2016
Política Núm. ATI-011, Mejores Prácticas de Infraestructura Tecnológica, revisada el 7 de noviembre de 2016
Política Núm. ATI-013, Marco Referencial de Adquisición Tecnológica Gubernamental, de 7 de noviembre de 2016

GOBIERNO DE PUERTO RICO
Departamento de Salud
Oficina de Asesores Legales

25 de septiembre de 2022

A LOS ASESORES LEGALES

Lcdo. Miguel A. Verdiales Morales
Principal Asesor Legal del Secretario
Director Interino
Oficina de Asesores Legales

SOBRE CONTRATOS DE TECNOLOGÍA DE INFORMACIÓN

El 31 de mayo de 2022, el Departamento de Salud fue auditado por la Oficina del Contralor (TI-22-11). En dicha auditoría se señala la necesidad de establecer controles efectivos con relación a los contratos de tecnología de información, específicamente aquellos de servicios de tecnología en la nube.

A tenor con lo cual, corresponde a los asesores legales asegurarse que la contratación propuesta cumple con las disposiciones legales aplicables a este tipo de contratación. Hacemos referencia y anejamos para su beneficio las recomendaciones que nos permiten asegurar que se incluya en dicha contratación las cláusulas requeridas por la reglamentación aplicable y proteger los mejores intereses del Departamento de Salud, a saber:

1. Establecer procedimientos para informar incidentes, obtener respuesta por parte del proveedor y otras funciones de seguridad en colaboración con el proveedor.
2. Establecer los medios para que la configuración y versiones del sistema operativo, si aplica, puedan mejorarse según la evolución y cambios de necesidad.
3. Establecer acuerdos de niveles de servicio donde se establezcan los niveles de respuesta de los proveedores en cualquier incidente y las penalidades asociadas al no cumplimiento de los niveles de servicio o la disponibilidad estipulados.
4. Roles y responsabilidades relacionadas a la implantación, operación y apoyo de la solución de tecnología en la nube.
5. Plan de migración de datos en caso de que sea necesario cambiar de proveedor.
6. Plan de respaldo de datos ("back up") recurrente.
7. Plan para la Recuperación de Desastres y Continuidad de las Operaciones.
8. Plan de adiestramiento y capacitación periódica a usuarios.
9. Certificación de revisión de seguridad (SOC-2)
10. Certificado ISO-27001-cumple con los estándares establecidos por ISMS, procesos de seguridad están ajustados para mantenerse al día con los cambios de amenazas de seguridad, vulnerabilidad e impactos adversos.

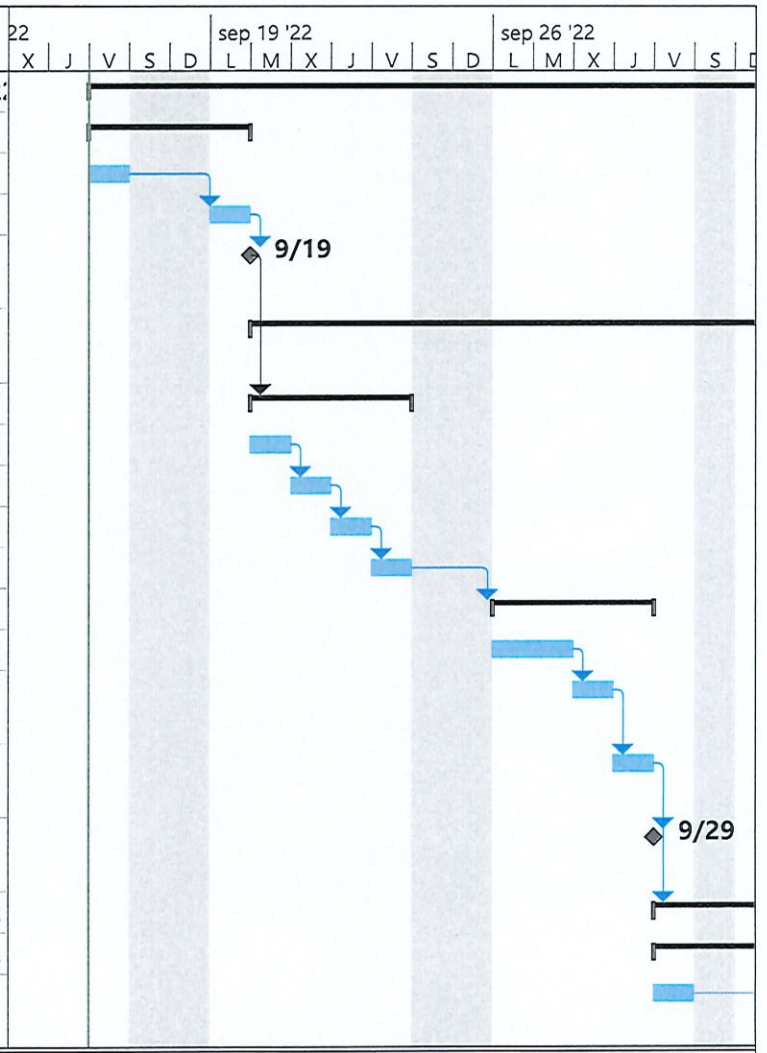
11. Propiedad exclusiva del Estado Libre Asociado de Puerto Rico sobre los datos y su uso.
12. Disponibilidad, integridad y confidencialidad de los datos.

Se incluye, además, como parte de este memorando: Carta Circular Núm. 140-16 de OGP sobre Normas Generales sobre la implantación de sistemas, compra de equipos y programas y uso de tecnología de la información para los organismos gubernamentales. Esta circular mantiene las políticas con respecto a la tecnología particularmente lo dispuesto sobre revisión de contratos de tecnología (ATI-017).

Estas normas son de estricto cumplimiento.

Anejo 3

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Pry-Extractor Renovaciones Onli**	**44 días**	**vie 9/16/22**	**mié 11/16/2**
2		**Fase de Kickoff**	**2 días**	**vie 9/16/22**	**lun 9/19/22**
3		Preparacion de PPT	1 día	vie 9/16/22	vie 9/16/22
4		Ejecucion Kickofff	1 día	lun 9/19/22	lun 9/19/22
5		Hito de Reunion de Kickoff Realizada	0 días	lun 9/19/22	lun 9/19/22
6		**Fase de Analisis y Revision de Requisitos**	**42 días**	**mar 9/20/22**	**mié 11/16/22**
7		**Revision de Requisitos**	**4 días**	**mar 9/20/22**	**vie 9/23/22**
8		VPN	1 día	mar 9/20/22	mar 9/20/22
9		Usr BD	1 día	mié 9/21/22	mié 9/21/22
10		Acceso Srv	1 día	jue 9/22/22	jue 9/22/22
11		Acceso Srv Destino	1 día	vie 9/23/22	vie 9/23/22
12		**Analisis**	**4 días**	**lun 9/26/22**	**jue 9/29/22**
13		Revision de Querys	2 días	lun 9/26/22	mar 9/27/22
14		Generar Documento de Procesos	1 día	mié 9/28/22	mié 9/28/22
15		Validacion de Documento de Proceso	1 día	jue 9/29/22	jue 9/29/22
16		Hito de Fase Analisis y Revision Terminada	0 días	jue 9/29/22	jue 9/29/22
17		**Fase de Implementacion**	**29 días**	**vie 9/30/22**	**mié 11/9/22**
18		**Construccion**	**24 días**	**vie 9/30/22**	**mié 11/2/22**
19		Desarrollo de Tabla de Agentes y Conexcion	1 día	vie 9/30/22	vie 9/30/22

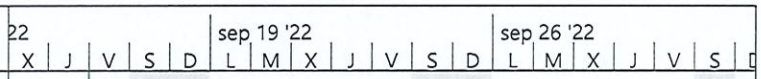


TECSECURE INC.

Proyecto: Plan_Extractores_Ren
Fecha: vie 9/16/22

Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Progreso	
Resumen del proyecto		Resumen manual		Progreso manual	
Tarea inactiva		solo el comienzo			
Hito inactivo		solo fin			

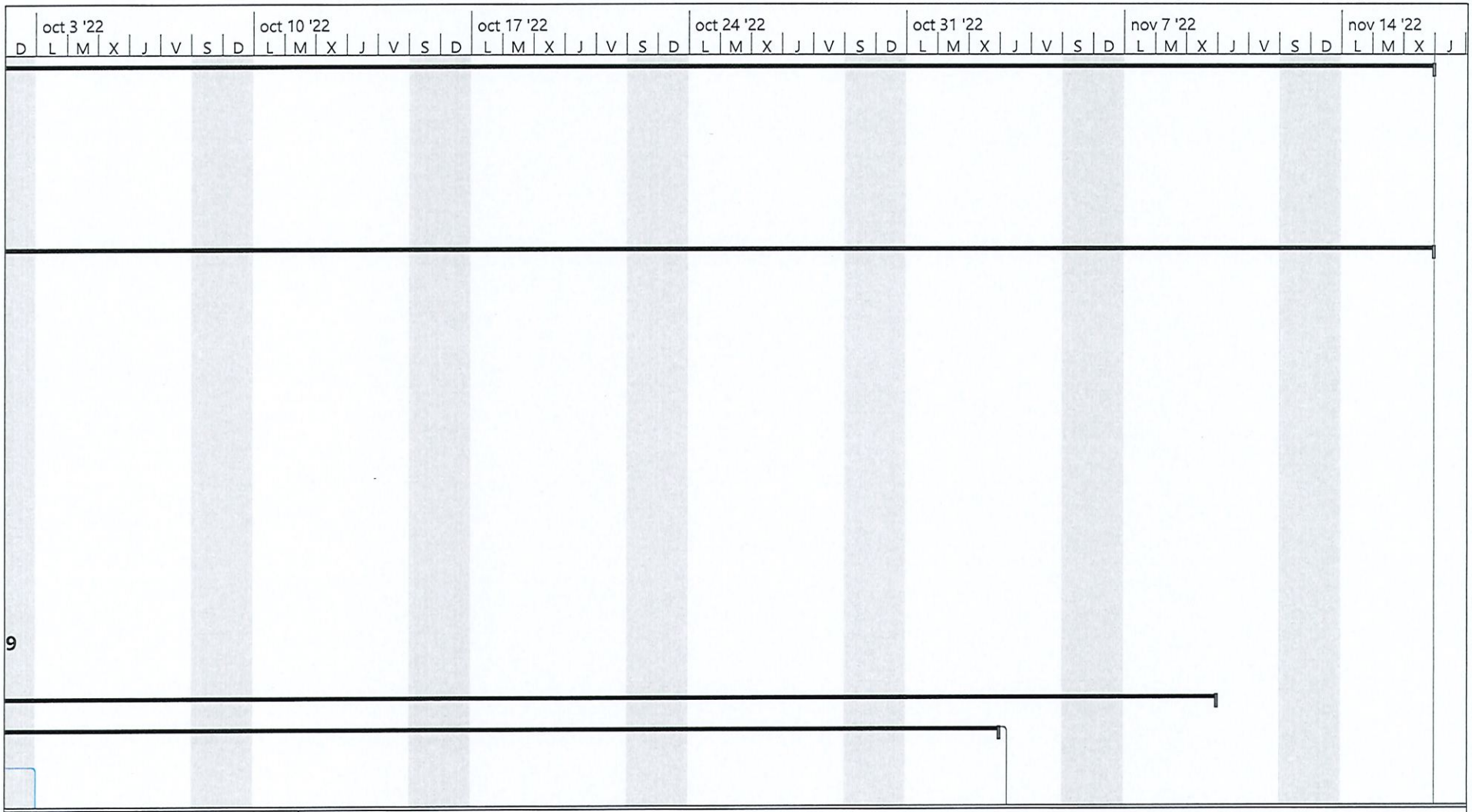
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
20		Shell de Envio	4 días	lun 10/3/22	jue 10/6/22
21		Envio Archivos procesa	2 días	vie 10/7/22	lun 10/10/22
22		Envio de archivo histori	2 días	mar 10/11/2	mié 10/12/22
23		Shell para la extracción	10 días	jue 10/13/22	mié 10/26/22
24		Implementar Job en SO	3 días	jue 10/27/22	lun 10/31/22
25		Implementar Job de Anexos	2 días	mar 11/1/22	mié 11/2/22
26		**Pruebas**	**5 días**	**jue 11/3/22**	**mié 11/9/22**
27		Ejecucion y Elaboracion de	5 días	jue 11/3/22	mié 11/9/22
28		Preparacion de entrega	1 día	jue 11/10/22	jue 11/10/22
29		Hito de Etrega	0 días	jue 11/10/22	jue 11/10/22
30		Apoyo Puesta en Produccion	4 días	vie 11/11/22	mié 11/16/22



TECSECURE INC.

Proyecto: Plan_Extractores_Ren
Fecha: vie 9/16/22

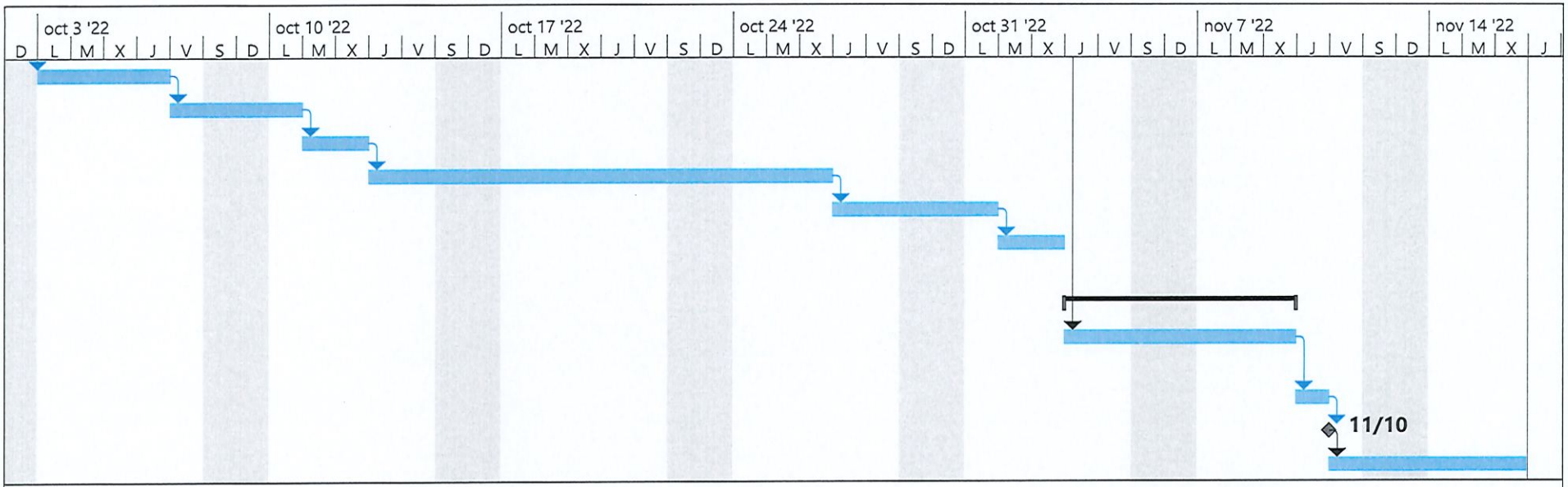
Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Progreso	
Resumen del proyecto		Resumen manual		Progreso manual	
Tarea inactiva		solo el comienzo			
Hito inactivo		solo fin			



TECSECURE INC.

Proyecto: Plan_Extractores_Ren
Fecha: vie 9/16/22

Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Progreso	
Resumen del proyecto		Resumen manual		Progreso manual	
Tarea inactiva		solo el comienzo			
Hito inactivo		solo fin			



TECSECURE INC.

Proyecto: Plan_Extractores_Ren
Fecha: vie 9/16/22

Tarea		Resumen inactivo		Tareas externas	
División		Tarea manual		Hito externo	
Hito		solo duración		Fecha límite	
Resumen		Informe de resumen manual		Progreso	
Resumen del proyecto		Resumen manual		Progreso manual	
Tarea inactiva		solo el comienzo			
Hito inactivo		solo fin			

Elizabeth Cruz Gonzalez

From: Mayra Toro Tirado
Sent: martes, 27 de septiembre de 2022 9:08 a. m.
To: Elizabeth Cruz Gonzalez; Carlos J. Mercado Ruiz; Elizabeth Maldonado Rodríguez
Cc: Miguel Verdiales Morales
Subject: RE: Plan de Accción Correctiva, Informe de Auditoría TI-22-11-Tecsecure, Inc.

Saludos:

Debido a la situación de emergencia por el Huracán Fiona, el personal se encuentra atendiendo la respuesta en refugios, negocios de alimentos y llenaderos de agua potable. En adición a esto las oficinas regionales al día de hoy se encuentran sin energía eléctrica por lo que el personal no tiene acceso a sus computadoras y servicios de internet. Debido a todo lo antes expuesto no fue posible dar el adiestramiento y el mismo se encuentra en proceso de ser recalendarizado.

Atte.

Mayra Toro Tirado, MSA
Assistant Secretary
for Environmental Health and
Public Health Laboratory
Puerto Rico Department of Health
PO Box 70184
San Juan, PR 00936-8184
Tel. 787-765-2929 ext. 3211
Mobile: 787-692-6303
Fax. 787-274-7809
mtoro@salud.gov.pr

DEPARTAMENTO DE SALUD

From: Elizabeth Cruz Gonzalez <elizabeth.cruz@salud.pr.gov>
Sent: Tuesday, September 27, 2022 8:45 AM
To: Carlos J. Mercado Ruiz <cjmercado@salud.pr.gov>; Mayra Toro Tirado <mtoro@salud.pr.gov>; Elizabeth Maldonado Rodríguez <emaldonado@salud.pr.gov>
Cc: Miguel Verdiales Morales <miguel.verdiales@salud.pr.gov>
Subject: RE: Plan de Accción Correctiva, Informe de Auditoría TI-22-11-Tecsecure, Inc.

Estimado Sr. Mercado Ruiz:

Reciba un cordial saludo. En atención a los adiestramientos programados para e 21 de septiembre de 2022, solicitamos confirme si los mismos fueron impartidos o si fueron reprogramados. De haber sido impartidos solicitamos se nos remita evidencia de la asistencia y del adiestramiento. En caso de haber sido reprogramados solicitamos se notifique la nueva fecha.

Anejo 4

26 de octubre de 2022

drcarlos.mellado@salud.pr.gov
elizabeth.cruz@salud.pr.gov
miguel.verdiales@salud.pr.gov

Hon. Carlos Mellado López
Secretario
Departamento de Salud
San Juan, Puerto Rico

Estimado señor secretario:

Evaluamos el *Plan de Acción Correctiva (PAC)* que nos remitió el 29 de septiembre de 2022, relacionado con el *Informe de Auditoría TI-22-11* de la Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública del Departamento de Salud (Secretaría Auxiliar para Salud Ambiental). Determinamos que las **recomendaciones 1.a. y b.** se consideran cumplimentadas y, las **recomendaciones 2a. y b.** se consideran parcialmente cumplimentadas.

En el *Informe Complementario al Plan de Acción Correctiva (ICP-1)* deberá suministrarnos la evidencia de las directrices y gestiones en anejos para:

1. Asegurarse de que la secretaria auxiliar de Salud Ambiental le requiera al contratista lo siguiente:

    a. Provea, en el término establecido, los respaldos de los datos procesados mediante la plataforma. **[Recomendación 2.a.] [Apartado b.]**

    b. Adiestre al personal designado sobre los procesos para acceder y grabar estos respaldos. Una vez adiestrados, se asegure de que los respaldos se graben periódicamente y se mantengan en un lugar seguro. **[Recomendación 2.b.] [Apartado b.]**

Agradeceremos que nos remita el *ICP-1* con la información y los documentos solicitados, no más tarde del 1 de febrero de 2023, mediante la aplicación *Sistema Plan de Acción Correctiva* (*Sistema PAC*) localizada en nuestra página en Internet: www.ocpr.gov.pr. El *ICP-1* será evaluado y la información remitida estará sujeta a verificación por esta Oficina.

En interés de que se cumplimenten las recomendaciones pendientes, le exhortamos a planificar, implantar y mantener un proceso de seguimiento que permita corroborar el cumplimiento de las acciones correctivas en el tiempo establecido, medir su efectividad y realizar los ajustes que sean necesarios. Esto, entre otras acciones, según orientamos y sugerimos en nuestra *Carta Circular OC-16-05*. Además, le recordamos que cualquier cambio de funcionario de enlace principal o Sustituto a cargo de remitir la información y los documentos solicitados debe ser registrado en el *Sistema PAC*. En la *Carta Circular OC-17-18* se establecen las instrucciones para utilizar dicho *Sistema* y para mantener actualizada la información sobre los referidos funcionarios, entre otras.

Para información adicional, el funcionario designado por usted puede comunicarse con la Sra. Linette Y. Collazo Rivera, analista de acción correctiva, al (787) 754-3030, extensión 5613.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,

Myrelis Hernández
Ayudante Ejecutiva
Oficina de Asuntos de Auditoría

c Lcda. Lizamarie Serrano Rodríguez
Asesora Legal del Presidente
Hon. Rafael Hernández Montañez
Cámara de Representantes de Puerto Rico

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: **TI-22-11** Número de unidad: **5290** Nombre de la entidad auditada: **DEPARTAMENTO DE SALUD-Secretaría Auxiliar para la Salud Ambiental y Laboratorio de Salud Pública**

Fecha del informe de auditoría o especial: **31 de mayo de 2022** Período auditado: **5 de mayo de 2014 al 30 de noviembre de 2020**

Indique el informe que remite: ☐ **PAC** ☑ **ICP -** 1 Indique si incluye anejo/s: ☑ **Sí** ☐ No

Funcionario de enlace: **Sra. Mayra Toro Tirado** Puesto: Secretaria Auxiliar Teléfono: (787) 765-2929 ext. 3211

Funcionario principal o su representante autorizado: **Dr. Carlos R. Mellado López** Puesto: Secretario de Salud Teléfono: (787) 765-2929 .

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 21 de febrero de 2023
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Asegurarse que la Secretaría Auxiliar de Salud Ambiental le requiera al contratista que provea en el término establecido los respaldos de los datos procesados mediante la plataforma	Se colocará un resguardo FULL a través de un SFTP en un servidor del Departamento de Salud.	Oficina de Informática del Departamento de Salud	Se incluye notificación del estado de los trabajos	Parcialmente cumplimentada
" "	Establecer requerimientos de solución (View/Read Only) para acceder a los datos de resguardo.	Oficina de Informática del Departamento de Salud	Se incluye notificación del estado de los trabajos	Parcialmente cumplimentada
Adiestrar al personal designado sobre los procesos para acceder y realizar respaldos de información	Coordinar Taller de capacitación con proveedor y usuarios del Departamento de Salud	Secretaría Auxiliar de Salud Ambiental y Laboratorio de Salud Pública	8 de febrero de 2023	Cumplimentada

(Véanse instrucciones al final).

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: **TI-22-11** Número de unidad: **5290** Nombre de la entidad auditada: **DEPARTAMENTO DE SALUD-Secretaría Auxiliar para la Salud Ambiental y Laboratorio de Salud Pública**

Fecha del informe de auditoría o especial: **31 de mayo de 2022** Período auditado: **5 de mayo de 2014 al 30 de noviembre de 2020**

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN

(Véanse instrucciones al final).

INSTRUCCIONES PARA COMPLETAR Y REMITIR
EL PLAN DE ACCIÓN CORRECTIVA

Instrucciones:

1. Este documento debe estar completado en todas sus partes.

   a. La primera página debe contener, entre otra información: el número y la fecha del informe de auditoría o especial relacionado; indicación sobre el documento que se remite (*PAC* o *ICP*); el nombre del funcionario de enlace y del funcionario principal; y la firma del funcionario principal o su representante autorizado.

   b. En las columnas se requiere la siguiente información:

      1) **Recomendación**: En esta columna se detallan las recomendaciones. Las recomendaciones se presentan en el mismo orden y con el número de identificación que aparece en el informe de auditoría o especial.

      2) **Acción Correctiva**: En esta columna se indican las medidas adoptadas o las que adoptarán para corregir las situaciones señaladas y eliminar las causas de estas. Las acciones correctivas deben ser alcanzables y diseñadas para prevenir que las situaciones se repitan.

      3) **Persona o área responsable**: En esta columna se identifica/n el/los funcionario/s o el/las área/s responsable/s de implantar las acciones correctivas.

      4) **Fecha de implantación**: En esta columna se indica la fecha probable para cumplir con las acciones correctivas.

      5) **Estatus de la recomendación:** En esta columna se indica el nivel de cumplimiento de la recomendación. Esto es:

         - **Cumplimentada**: Recomendaciones para las cuales se tomaron acciones correctivas y se obtuvieron los resultados deseados.
         - **Parcialmente cumplimentada**: Recomendaciones para las cuales se han establecido medidas correctivas, pero quedan algunos asuntos pendientes.
         - **No cumplimentada**: Recomendaciones para las cuales no se han establecido acciones correctivas.

      En cada una de los columnas descritas en el apartado del **b.2) al 5)** de esta instrucción se deben ofrecer datos que permitan una evaluación adecuada. Si se objeta alguna recomendación, se deben incluir las razones y una descripción específica de la/s acción/nes correctiva/s alterna/s.

2. Cuando el funcionario principal delegue la función de certificar este documento, antes de remitir el mismo, debe notificar por escrito a la dirección de correo electrónico AdminPAC@ocpr.gov.pr el nombre y el puesto del funcionario en quien delegó la misma.

3. El documento digitalizado debe remitirse a la Oficina mediante la aplicación *Sistema Plan de Acción Correctiva* que esta creó para estos propósitos[1]. Esto, dentro del término de 90 días consecutivos, contados a partir del primer día del mes siguiente a la fecha de publicación del informe de auditoría o el especial. Cuando queden recomendaciones pendientes de cumplimentar, a la fecha del primer informe, se prepararán informes complementarios *(ICP)* cada 90 días, contados a partir del primer día del mes siguiente a la fecha de la notificación del resultado de la evaluación. El envío debe ser en la forma indicada anteriormente.

4. Los documentos que se utilicen para justificar las acciones correctivas informadas deben estar disponibles para examen por esta Oficina.

[1] La aplicación *Sistema Plan de Acción Correctiva* v1.0 está localizada en nuestra página en Internet: www.ocpr.gov.pr bajo la sección Contraloría Digital. Si no tiene una cuenta registrada en dicha aplicación envíe un correo electrónico a AdminPAC@ocpr.gov.pr para solicitar información de cómo registrar una cuenta en la misma.

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DE SALUD
Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública

21 de febrero de 2023

Lcdo. Miguel A. Verdiales Morales
Principal Asesor Legal del Secretario
Director Oficina de Asesores Legales
Departamento de Salud

Mayra Toro Tirado, MS
Secretaria Auxiliar
Secretaría Auxiliar para Salud Ambiental

PLAN DE ACCION CORRECTIVA INFORME DE AUDITORÍA TI-22-11

El pasado 8 de febrero de 2023 nuestro personal gerencial, de todas las regiones de Salud Ambiental, participó de un adiestramiento virtual ofrecido por el administrador de TecSecure, Inc., compañía a cargo de la plataforma www.renovacionesonline.com sobre los procesos para acceder y grabar respaldos. Durante el taller se explicó las maneras como extraer la información y ser descargada a formato Excel para guardar respaldos. Como parte del taller se discutieron dudas y se mostraron ejemplos de como realizar ciertas operaciones en el sistema.

Certificamos y anejamos a esta comunicación la citación al adiestramiento que incluye los nombres de todas las personas que participaron del taller.

Mayra Toro Tirado

Subject:	ADIESTRAMIENTO - RENOVACIONES ONLINE
Start:	Wed 2/8/2023 9:00 AM
End:	Wed 2/8/2023 10:00 AM
Recurrence:	(none)
Meeting Status:	Accepted
Organizer:	Elizabeth Maldonado Rodríguez
Required Attendees:	Mayra Toro Tirado; Carlos J. Mercado Ruiz; Ramon E. Abreu Aviles; Marla Carrion Ruiz; Maria S. Rodriguez Irizarry; Mónica Vélez Camacho; Juan Capeles Cordero; Santiago Rivera Lopez; Carlos Mojica Camis; Orlando Llanos Bonilla; Eduardo Padilla Zapata; Janice Albino Figueroa; Neribel Del Toro Lugo; Kelvin Torres Rodriguez; Keyshla M. Acevedo Feliciano; Irvia I. Morales De Jesus; Manuel Rivera Nieves; Glorimar Santiago Perez
Optional Attendees:	Eduardo Padilla; Manuel Guerra-Mondragon (mgm@renovacionesonline.com)
SkypeTeamsProperties:	{"cid":"19:meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm@thread.v2","rid":0,"mid":0,"uid":null,"private":true,"type":0}
SkypeTeamsMeetingUrl:	https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm%40thread.v2/0?context=%7b%22Tid%22%3a%22e906065a-f03e-47ad-a4c4-6b139a08445c%22%2c%22Oid%22%3a%22115cebfb-0cca-44d9-b2cb-2e27b88d15e3%22%7d
SchedulingServiceUpdateUrl:	https://api.scheduler.teams.microsoft.com/teams/e906065a-f03e-47ad-a4c4-6b139a08445c/115cebfb-0cca-44d9-b2cb-2e27b88d15e3/19_meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm@thread.v2/0
OnlineMeetingConfLink:	conf:sip:ElizabethM@salud.gov.pr;gruu;opaque=app:conf:focus:id:teams:2:0!19:meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm-thread.v2!115cebfb0cca44d9b2cb2e27b88d15e3!e906065af03e47ada4c46b139a08445c
TeamsVtcTenantId:	e906065a-f03e-47ad-a4c4-6b139a08445c

Microsoft Teams meeting

Join on your computer, mobile app or room device
Click here to join the meeting

Meeting ID: 263 377 292 464
Passcode: EFerdt
Download Teams | Join on the web

Elizabeth Cruz Gonzalez

From: Hiram Rivera Santiago
Sent: martes, 21 de febrero de 2023 4:24 p. m.
To: Miguel Verdiales Morales
Cc: Elizabeth Cruz Gonzalez
Subject: RE: Plan de Acción Correctiva, Informe de Auditoría TI-22-11-Tecsecure, Inc. - Seguimiento *2da notificación)

Saludos, en efecto los 2 puntos no se han completado.

1. Estado del Plan de Trabajo sobre:
   a. la colocación del resguardo FULL a través de un SFTP en un servidor del Departamento. **La configuración esta realizada, estamos teniendo problemas en la conexión externa con el suplidor ya que indica que la contraseña brindada no es funcional martes 22 se debe completar este punto.**
   b. Establecer requerimiento de solución (View/Read Only) para acceder a los datos de resguardo. **Luego de que el paso A se complete se establece solución para acceder la data.**

Atentamente,

Hiram Rivera Santiago | Director
Oficina de Informática y Avances Tecnológicos (O1AT)
Departamento de Salud de Puerto Rico
O 787.765.2929 ext. 9000 M 787.640.6556

DEPARTAMENTO DE SALUD

6 de marzo de 2023

drcarlos.mellado@salud.pr.gov
elizabeth.cruz@salud.pr.gov
miguel.verdiales@salud.pr.gov

Hon. Carlos Mellado López
Secretario
Departamento de Salud
San Juan, Puerto Rico

Estimado señor secretario:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-1)* que nos remitió el 28 de febrero de 2023, relacionado con el *Informe de Auditoría TI-22-13* de la auditoría a los sistemas de información de la Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública del Departamento de Salud. Determinamos que las **recomendaciones 2 a. y b.** consideran parcialmente cumplimentada.

En el *Informe Complementario al Plan de Acción Correctiva (ICP-2)* deberá suministrarnos la siguiente evidencia:

1. Del acceso provisto a los respaldos de los datos procesados mediante la plataforma. **[Recomendación 2.a.] [Apartado b.]**

2. Del adiestramiento ofrecido al personal designado sobre los procesos para acceder y grabar estos respaldos. Además, incluirnos copia de las instrucciones impartidas para asegurarse de que los respaldos se graben periódicamente y se mantengan en un lugar seguro. **[Recomendación 2.b.] [Apartado b.]**

Agradeceremos que nos remita el *ICP-1* con la información y los documentos solicitados, no más tarde del 5 de julio de 2023, mediante la aplicación *Sistema Plan de Acción Correctiva* (*Sistema PAC*) localizada en nuestra página en Internet: www.ocpr.gov.pr. El *ICP-1* será evaluado y la información remitida estará sujeta a verificación por esta Oficina.

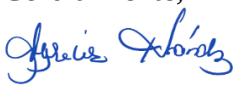
En interés de que se cumplimenten las recomendaciones pendientes, le exhortamos a planificar, implantar y mantener un proceso de seguimiento que permita corroborar el cumplimiento de las acciones correctivas en el tiempo establecido, medir su efectividad y realizar los ajustes que sean necesarios. Esto, entre otras acciones, según orientamos y sugerimos en nuestra *Carta Circular OC-16-05*. Además, le recordamos que cualquier cambio de funcionario de enlace principal o

Sustituto a cargo de remitir la información y los documentos solicitados debe ser registrado en el *Sistema PAC*. En la *Carta Circular OC-17-18* se establecen las instrucciones para utilizar dicho *Sistema* y para mantener actualizada la información sobre los referidos funcionarios, entre otras.

Para información adicional, el funcionario designado por usted puede comunicarse con la Sra. Linette Y. Collazo Rivera, analista de acción correctiva, al (787) 754-3030, extensión 5613.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,



Myrelis Hernández
Ayudante Ejecutiva
Oficina de Asuntos de Auditoría

c Lcda. Laura S. Rodríguez Cordero
Directora
Comisión Conjunta Sobre Informes Especiales del Contralor

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: TI-22-11 Número de unidad: 5290 Nombre de la entidad auditada: Departamento de Salud – Oficina de informática y Avances Tecnológicos

Fecha del informe de auditoría o especial: 30 de mayo de 2022 Período auditado: 5 de mayo de 2014 al 30 de noviembre de 2020

Indique el informe que remite: ☐ **PAC** ☒ **ICP -** 02 Indique si incluye anejo/s: ☒ Sí ☐ No

Funcionario de enlace: Sr. Hiram Rivera Santiago Puesto: Director de la Oficina de informática y Avances Tecnológicos (OIAT) Teléfono: (787) 765-2929 Ext. 9000

Funcionario principal o su representante autorizado: Dr. Carlos Mellado Puesto: Secretario de Salud de Puerto Rico Teléfono: (787) 765-2929 Ext. 3393

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 7/6/2023
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Asegurarse de que la Secretaria Auxiliar de la Secretaría Auxiliar para Salud Ambiental le requiera al contratista provea, en el término establecido, los respaldos de los datos procesados mediante la plataforma. **[Recomendación 2.a.] [Apartado b.]**	1. Se colocó un resguardo FULL a través de un SFTP en un servidor del Departamento de Salud. Se adjunta descripción del método y ubicación para el respaldo de los datos procesados mediante la plataforma. Se realizó la diseño, programación e implementación del área en los servidores para realizar el resguardo correspondiente. Ver Anejo.	Oficina de Informática y Avances Tecnológicos (OIAT)	30 de junio de 2023	Cumplimentada
	2. Establecer un requerimiento de solución (View/Read Only) para acceder a los datos de resguardo. Diseño y programación completados. Se incluyó en plan de	Oficina de Informática y Avances	30 de junio de 2023	Parcialmente cumplimentada

INICIALES HRS

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: TI-22-11 Número de unidad: 5290 Nombre de la entidad auditada: Departamento de Salud – Oficina de informática y Avances Tecnológicos

Fecha del informe de auditoría o especial: 30 de mayo de 2022 Período auditado: 5 de mayo de 2014 al 30 de noviembre de 2020

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
	trabajo el comienzo de las pruebas con proveedor durante el mes de julio 2023. *Ver anejo.*	Tecnológicos (OIAT)		
Adiestrar al personal designado sobre los procesos para acceder y realizar respaldos de información. **[Recomendación 2.b.] [Apartado b.]**	1. Se coordinó taller de capacitación con proveedor y usuarios del Departamento de Salud. La solución a corto plazo incluyó las formas para extraer información y respaldo en formato Excel. Ver anejo.	Secretaría Auxiliar de Salud Ambiental y Laboratorio de Salud Pública (SASA)	8 de febrero de 2023	Cumplimentada
	2. En este nuevo Año Fiscal 2023-24 se ha establecido como prioridad en nuestro Plan de Trabajo ofrecer los adiestramientos a finales del 1er semestre del año fiscal, al personal designado sobre los procesos para acceder y grabar estos respaldos, utilizando la solución identificada e implantada.	Oficina de Informática y Avances Tecnológicos (OIAT)	1er Semestre del Plan de Trabajo de Adiestramientos de OIAT	Parcialmente cumplimentada

INICIALES HRS

INSTRUCCIONES PARA COMPLETAR Y REMITIR
EL PLAN DE ACCIÓN CORRECTIVA

Instrucciones:

1. Este documento debe estar completado en todas sus partes.

   a. La primera página debe contener, entre otra información: el número y la fecha del informe de auditoría o especial relacionado; indicación sobre el documento que se remite (*PAC* o *ICP*); el nombre del funcionario de enlace y del funcionario principal; y la firma del funcionario principal o su representante autorizado.

   b. En las columnas se requiere la siguiente información:

      1) **Recomendación**: En esta columna se detallan las recomendaciones. Las recomendaciones se presentan en el mismo orden y con el número de identificación que aparece en el informe de auditoría o especial.

      2) **Acción Correctiva**: En esta columna se indican las medidas adoptadas o las que adoptarán para corregir las situaciones señaladas y eliminar las causas de estas. Las acciones correctivas deben ser alcanzables y diseñadas para prevenir que las situaciones se repitan.

      3) **Persona o área responsable**: En esta columna se identifica/n el/los funcionario/s o el/las área/s responsable/s de implantar las acciones correctivas.

      4) **Fecha de implantación**: En esta columna se indica la fecha probable para cumplir con las acciones correctivas.

      5) **Estatus de la recomendación**: En esta columna se indica el nivel de cumplimiento de la recomendación. Esto es:

         - **Cumplimentada**: Recomendaciones para las cuales se tomaron acciones correctivas y se obtuvieron los resultados deseados.
         - **Parcialmente cumplimentada**: Recomendaciones para las cuales se han establecido medidas correctivas, pero quedan algunos asuntos pendientes.
         - **No cumplimentada**: Recomendaciones para las cuales no se han establecido acciones correctivas.

      En cada una de los columnas descritas en el apartado del **b.2) al 5)** de esta instrucción se deben ofrecer datos que permitan una evaluación adecuada. Si se objeta alguna recomendación, se deben incluir las razones y una descripción específica de la/s acción/nes correctiva/s alterna/s.

2. Cuando el funcionario principal delegue la función de certificar este documento, antes de remitir el mismo, debe notificar por escrito a la dirección de correo electrónico AdminPAC@ocpr.gov.pr el nombre y el puesto del funcionario en quien delegó la misma.

3. El documento digitalizado debe remitirse a la Oficina mediante la aplicación *Sistema Plan de Acción Correctiva* que esta creó para estos propósitos[1]. Esto, dentro del término de 90 días consecutivos, contados a partir del primer día del mes siguiente a la fecha de publicación del informe de auditoría o el especial. Cuando queden recomendaciones pendientes de cumplimentar, a la fecha del primer informe, se prepararán informes complementarios *(ICP)* cada 90 días, contados a partir del primer día del mes siguiente a la fecha de la notificación del resultado de la evaluación. El envío debe ser en la forma indicada anteriormente.

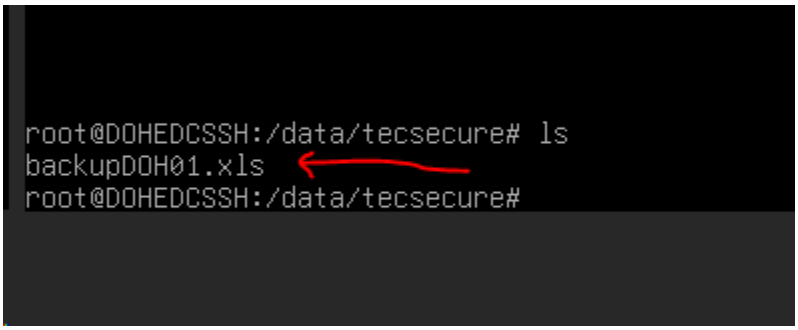
4. Los documentos que se utilicen para justificar las acciones correctivas informadas deben estar disponibles para examen por esta Oficina.

[1] La aplicación *Sistema Plan de Acción Correctiva* v1.0 está localizada en nuestra página en Internet: www.ocpr.gov.pr bajo la sección Contraloría Digital. Si no tiene una cuenta registrada en dicha aplicación envíe un correo electrónico a AdminPAC@ocpr.gov.pr para solicitar información de cómo registrar una cuenta en la misma.

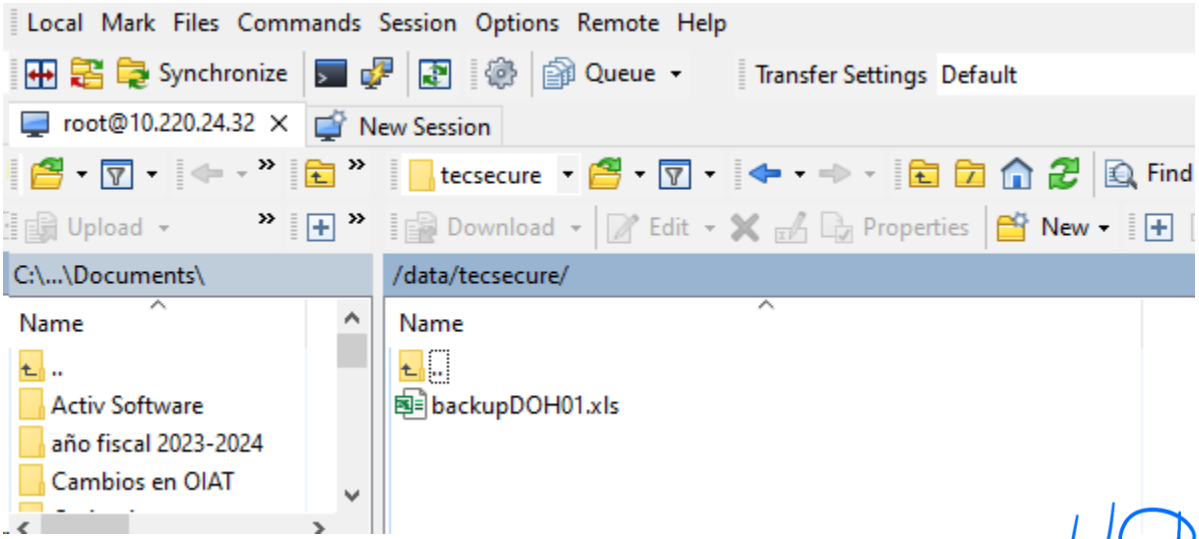
Anejo A:

La Oficina de Informática y Avances Tecnológicos (OIAT) prepara la programación y método de resguardo la cual utilizará renovaciones en línea para los resguardos (backups)s. La compañía realizará una conexión segura al servidor (DOHEDCSSH) del Departamento de Salud de Puerto Rico, ubicado en las facilidades de OIAT, por método seguro ssh a un folder /data/tecsecure.

En esta carpeta depositarán semanalmente los resguardos (*backup*) de los datos en un archivo .xls. Adjunto imagen con la información antes mencionada.



El usuario utilizara la herramienta winscp para descargar el archivo y ser utilizado para reportes. El archivo es solo de lectura y no se puede ser modificado desde el servidor.
https://winscp.net/eng/index.php



6/30/2023

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DE SALUD
Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública

21 de febrero de 2023

Lcdo. Miguel A. Verdiales Morales
Principal Asesor Legal del Secretario
Director Oficina de Asesores Legales
Departamento de Salud

Mayra Toro Tirado, MS
Secretaria Auxiliar
Secretaría Auxiliar para Salud Ambiental

PLAN DE ACCION CORRECTIVA INFORME DE AUDITORÍA TI-22-11

El pasado 8 de febrero de 2023 nuestro personal gerencial, de todas las regiones de Salud Ambiental, participó de un adiestramiento virtual ofrecido por el administrador de TecSecure, Inc., compañía a cargo de la plataforma www.renovacionesonline.com sobre los procesos para acceder y grabar respaldos. Durante el taller se explicó las maneras como extraer la información y ser descargada a formato Excel para guardar respaldos. Como parte del taller se discutieron dudas y se mostraron ejemplos de como realizar ciertas operaciones en el sistema.

Certificamos y anejamos a esta comunicación la citación al adiestramiento que incluye los nombres de todas las personas que participaron del taller.

Mayra Toro Tirado

Subject:	ADIESTRAMIENTO - RENOVACIONES ONLINE
Start:	Wed 2/8/2023 9:00 AM
End:	Wed 2/8/2023 10:00 AM
Recurrence:	(none)
Meeting Status:	Accepted
Organizer:	Elizabeth Maldonado Rodríguez
Required Attendees:	Mayra Toro Tirado; Carlos J. Mercado Ruiz; Ramon E. Abreu Aviles; Marla Carrion Ruiz; Maria S. Rodriguez Irizarry; Mónica Vélez Camacho; Juan Capeles Cordero; Santiago Rivera Lopez; Carlos Mojica Camis; Orlando Llanos Bonilla; Eduardo Padilla Zapata; Janice Albino Figueroa; Neribel Del Toro Lugo; Kelvin Torres Rodriguez; Keyshla M. Acevedo Feliciano; Irvia I. Morales De Jesus; Manuel Rivera Nieves; Glorimar Santiago Perez
Optional Attendees:	Eduardo Padilla; Manuel Guerra-Mondragon (mgm@renovacionesonline.com)
SkypeTeamsProperties:	{"cid":"19:meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm@thread.v2","rid":0,"mid":0,"uid":null,"private":true,"type":0}
SkypeTeamsMeetingUrl:	https://teams.microsoft.com/l/meetup-join/19%3ameeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm%40thread.v2/0?context=%7b%22Tid%22%3a%22e906065a-f03e-47ad-a4c4-6b139a08445c%22%2c%22Oid%22%3a%22115cebfb-0cca-44d9-b2cb-2e27b88d15e3%22%7d
SchedulingServiceUpdateUrl:	https://api.scheduler.teams.microsoft.com/teams/e906065a-f03e-47ad-a4c4-6b139a08445c/115cebfb-0cca-44d9-b2cb-2e27b88d15e3/19_meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm@thread.v2/0
OnlineMeetingConfLink:	conf:sip:ElizabethM@salud.gov.pr;gruu;opaque=app:conf:focus:id:teams:2:0!19:meeting_YTY5OGIwZGItYWFkMy00NjU4LWFhZTQtZjM4MjVkODY5NDVm-thread.v2!115cebfb0cca44d9b2cb2e27b88d15e3!e906065af03e47ada4c46b139a08445c
TeamsVtcTenantId:	e906065a-f03e-47ad-a4c4-6b139a08445c

Microsoft Teams meeting

Join on your computer, mobile app or room device
Click here to join the meeting

Meeting ID: 263 377 292 464
Passcode: EFerdt
Download Teams | Join on the web

17 de julio de 2023

drcarlos.mellado@salud.pr.gov
elizabeth.cruz@salud.pr.gov
miguel.verdiales@salud.pr.gov

Hon. Carlos Mellado López
Secretario
Departamento de Salud
San Juan, Puerto Rico

Estimado secretario:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-2)* que nos remitió el 6 de julio, relacionado con el *Informe de Auditoría TI-22-11* de la Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública del Departamento de Salud. Determinamos que la **Recomendación 2.a.** se considera cumplimentada. La **Recomendación 2.b.** considera parcialmente cumplimentada.

En el *Informe Complementario al Plan de Acción Correctiva (ICP-3)* deberá suministrarnos la siguiente información relacionada con la **Recomendación 2.b. [Apartado b.]**:

1. Certificación de la compañía que ofreció el adiestramiento que indique los temas incluidos y los participantes de este.

2. Evidencia de que los respaldos se graban periódicamente y se mantienen en un lugar seguro.

Agradeceremos que nos remita el *ICP-3* con la información y los documentos solicitados, no más tarde del 1 de noviembre de 2023, mediante la aplicación *Sistema Plan de Acción Correctiva* (*Sistema PAC*) localizada en nuestra página en Internet: www.ocpr.gov.pr. El *ICP-3* será evaluado y la información remitida estará sujeta a verificación por esta Oficina.

En interés de que se cumplimenten las recomendaciones pendientes, le exhortamos a planificar, implantar y mantener un proceso de seguimiento que permita corroborar el cumplimiento de las acciones correctivas en el tiempo establecido, medir su efectividad y realizar los ajustes que sean necesarios. Esto, entre otras acciones, según orientamos y sugerimos en nuestra *Carta Circular OC-16-05*. Además, le recordamos que cualquier cambio de funcionario de enlace principal o sustituto a cargo de remitir la información y los documentos solicitados debe ser

registrado en el *Sistema PAC.* En la *Carta Circular OC-17-18* se establecen las instrucciones para utilizar dicho *Sistema* y para mantener actualizada la información sobre los referidos funcionarios, entre otras.

Para información adicional, el funcionario designado por usted puede comunicarse con el Sr. Jaime Nogueras Arbelo, analista de acción correctiva, al (787) 754-3030, extensión 5617.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,

Myrelis Hernández
Ayudante ejecutiva
Oficina de Asuntos de Auditoría

c Lcda. Laura S. Rodríguez Cordero
Directora
Comisión Conjunta Sobre Informes Especiales del Contralor

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

PLAN DE ACCIÓN CORRECTIVA

Número del informe de auditoría o especial: TI-22-11 Número de unidad: 5290 Nombre de la entidad auditada: Departamento de Salud – Oficina de informática y Avances Tecnológicos

Fecha del informe de auditoría o especial: 30 de mayo de 2022 Período auditado: 5 de mayo de 2014 al 30 de noviembre de 2020

Indique el informe que remite: ☐ **PAC** ☒ **ICP -** 03 Indique si incluye anejo/s: ☒ Sí ☐ No

Funcionario de enlace: Sr. Hiram Rivera Santiago Puesto: Director de la Oficina de informática y Avances Tecnológicos (OIAT) Teléfono: (787) 765-2929 Ext. 9000

Funcionario principal o su representante autorizado: Dr. Carlos Mellado Puesto: Secretario de Salud de Puerto Rico Teléfono: (787) 765-2929 Ext. 3393

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 3 de noviembre de 2023
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	PERSONA O ÁREA RESPONSABLE	FECHA DE IMPLANTACIÓN	ESTATUS DE LA RECOMENDACIÓN
Adiestrar al personal designado sobre los procesos para acceder y realizar respaldos de información. **[Recomendación 2.b.] [Apartado b.]**	1. Se coordinó taller de capacitación con proveedor y usuarios del Departamento de Salud. La solución a corto plazo incluyó las formas para extraer información y respaldo en formato Excel. Ver anejo.	Secretaría Auxiliar de Salud Ambiental y Laboratorio de Salud Pública (SASA)	8 de febrero de 2023	Cumplimentada Anejo A y B
	2. En este nuevo Año Fiscal 2023-24 se ha establecido como prioridad en nuestro Plan de Trabajo ofrecer los adiestramientos a finales del 1er semestre del año fiscal, al personal designado sobre los procesos para acceder y grabar estos respaldos, utilizando la solución identificada e implantada.	Oficina de Informática y Avances Tecnológicos (OIAT)	1er Semestre del Plan de Trabajo de Adiestramientos de OIAT	Parcialmente cumplimentada

INICIALES_____

TECSECURE INC.

Certificación de Adiestramiento

To: Elizabeth Cruz González JD, Lcdo. Miguel Verdiales Morales

From: Manuel Guerra-Mondragón

Date: 7/27/23

Re: Adestramiento a Personal de Salud Ambiental “Directores Regionales”

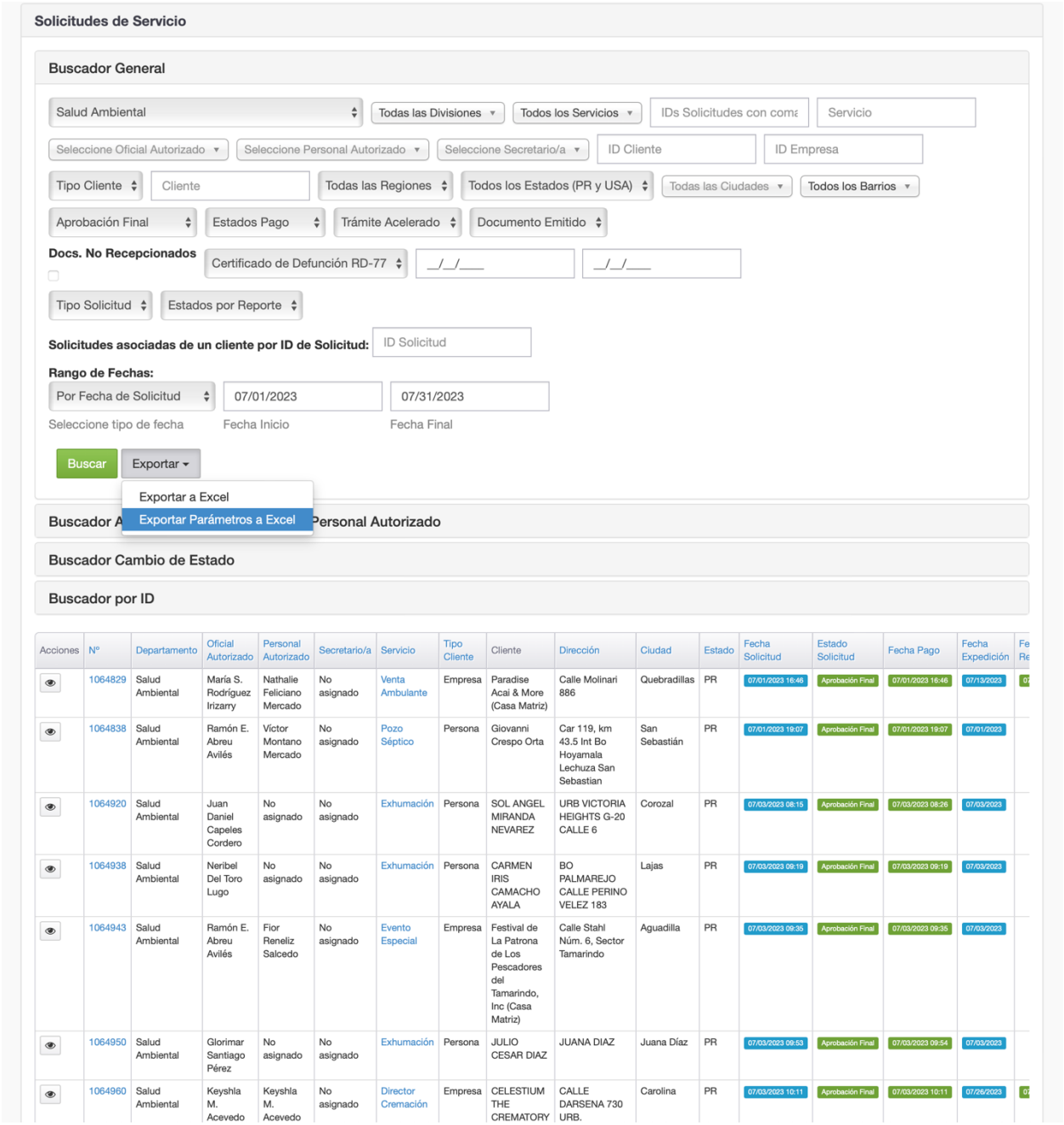
En él días febrero 8 del 2023 citados a las 9am se realizó un adestramiento con los Directores Regionales de Salud Ambiental con la finalidad de muestrales y adiestra en como pueden extraer data del sistema para ellos resguarda su información

A continuación, las pantallas de ejemplo que se mostraron en el adestramiento. Duración fue de unos 15 minutos y luego se abrió a preguntas y respuestas sobre el tema y tema abierto.

Adjunto:

Copyright © 2009, TECSECURE INC. All Rights Reserved

El Adiestramiento fue “Live” donde se presentaron todos módulos donde el sistema tiene estas funcionalidad de extraer información



Copyright © 2009, TECSECURE INC. All Rights Reserved

From: **Mayra Toro Tirado** mtoro@salud.pr.gov
Subject: FW: ADIESTRAMIENTO - RENOVACIONES ONLINE
Date: February 8, 2023 at 9:16 AM
To: Manuel Guerra-Mondragon (mgm@renovacionesonline.com) mgm@renovacionesonline.com

MT

-----Original Appointment-----
From: Elizabeth Maldonado Rodríguez <emaldonado@salud.pr.gov>
Sent: Wednesday, February 1, 2023 11:28 AM
To: Elizabeth Maldonado Rodríguez; Elizabeth Maldonado Rodríguez; Mayra Toro Tirado; Carlos J. Mercado Ruiz; Ramon E. Abreu Aviles; Marla Carrion Ruiz; Maria S. Rodriguez Irizarry; Mónica Vélez Camacho; Juan Capeles Cordero; Santiago Rivera Lopez; Carlos Mojica Camis; Orlando Llanos Bonilla; Eduardo Padilla Zapata; Janice Albino Figueroa; Neribel Del Toro Lugo; Kelvin Torres Rodriguez; Keyshla M. Acevedo Feliciano; Irvia I. Morales De Jesus; Manuel Rivera Nieves; Glorimar Santiago Perez
Cc: Eduardo Padilla
Subject: ADIESTRAMIENTO - RENOVACIONES ONLINE
When: Wednesday, February 8, 2023 9:00 AM-10:00 AM (UTC-04:00) Georgetown, La Paz, Manaus, San Juan.
Where:

Microsoft Teams meeting

Join on your computer, mobile app or room device
Click here to join the meeting

Meeting ID: 263 377 292 464
Passcode: EFerdt
Download Teams | Join on the web

Learn More | Meeting options

NOTA DE CONFIDENCIALIDAD: La información contenida en esta transmisión está destinada únicamente a las personas o entidades a la que se dirige. Puede contener información privilegiada y confidencial, incluida Información de Salud Protegida (PHI). Si usted no es el destinatario, se le notifica que cualquier revisión, difusión, distribución o duplicación de esta comunicación está estrictamente prohibida. Si recibe esta comunicación por error, notifique al remitente inmediatamente y destruya este mensaje.
CONFIDENTIALITY NOTE: The information contained in this transmission is intended only for the persons or entities to which it is addressed. It may contain privileged and confidential information, including Protected Health Information (PHI). If you are not the recipient, you are hereby notified that any revision, dissemination, distribution or duplication of this communication is strictly prohibited.

If you receive this communication by error, notify the sender immediately and destroy this message.

Mail Attachment.ics

Elizabeth Cruz Gonzalez

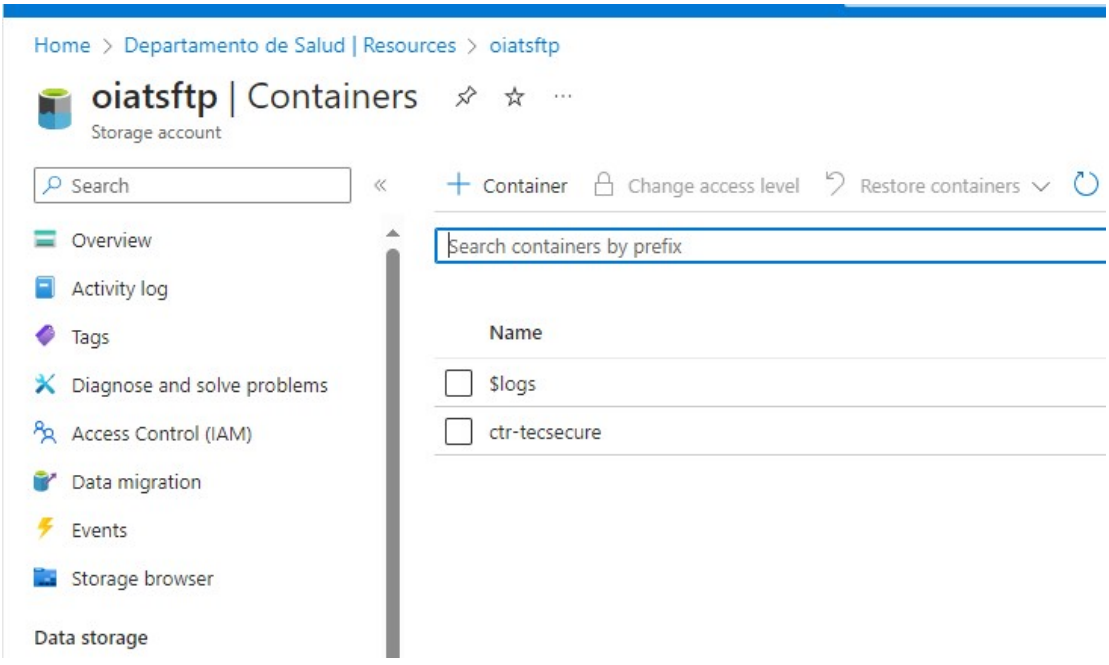
From: Hiram Rivera Santiago
Sent: jueves, 2 de noviembre de 2023 12:03 p. m.
To: Elizabeth Cruz Gonzalez
Subject: FW:

Elizabeth saludos, disculpa la tardanza. Adjunto la información para el ICP, Erick no pudo terminar por que el contrato se terminó.

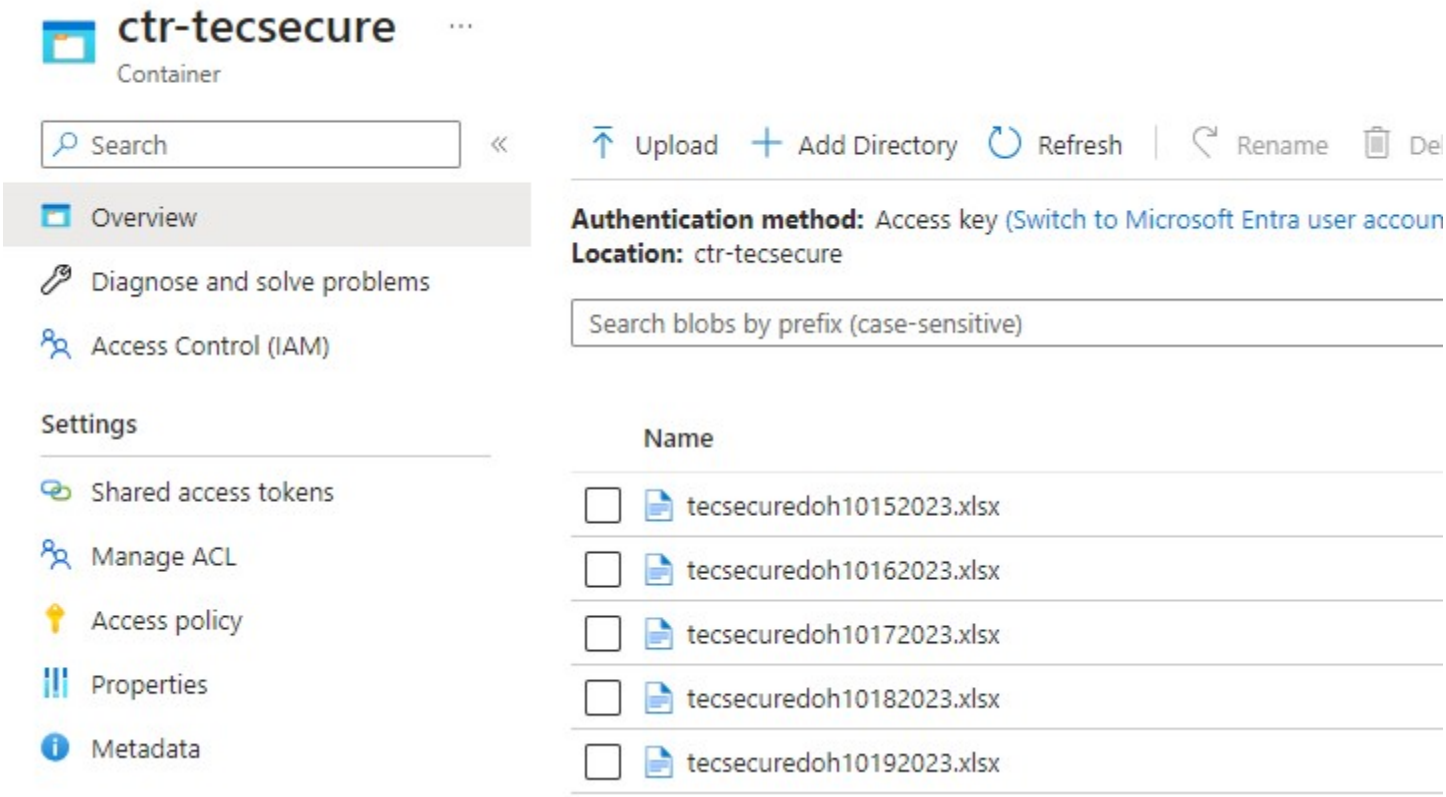
Atentamente,

Hiram Rivera Santiago | Director
Oficina de Informática y Avances Tecnológicos (O1AT)
Departamento de Salud de Puerto Rico
O 787.765.2929 ext. 9000 M 787.640.6556

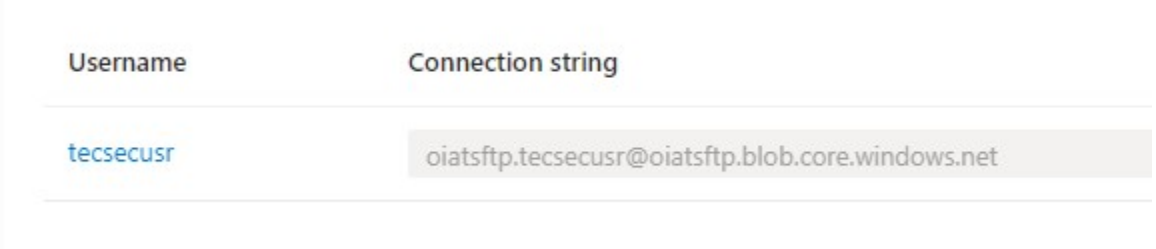
El backup es almacenado automaticamenteque, el suplidor establece una conexión Segura desde su entorno a un contenedor en la nube del Departamento de Salud, el cual se trasmite cada dia a las 11pm



La data es guardada en archivos xlsx



La conexión es a travez sftp



Solo tienen acceso los suplidor externo para que séa Seguro.

No network selected.

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

☐ Add your client IP address ('173.211.162.165') ⓘ

Address range	
70.45.69.70	🗑
98.129.210.19	🗑
98.129.210.20	🗑
98.129.210.17	🗑
98.129.210.16	🗑
12.205.81.94	🗑
IP address or CIDR	

8 de diciembre de 2023

CORREO ELECTRÓNICO

Hon. Carlos Mellado López
Secretario
Departamento de Salud
San Juan, Puerto Rico

Estimado secretario:

Evaluamos el *Informe Complementario al Plan de Acción Correctiva (ICP-3)* que nos remitió el 3 de noviembre de 2023, relacionado con el *Informe de Auditoría TI-22-11* de la Secretaría Auxiliar para Salud Ambiental y Laboratorio de Salud Pública del Departamento de Salud. Determinamos que la **Recomendación 2. b.** se considera cumplimentada.

Para información adicional, el funcionario designado por usted puede comunicarse con el Sr. Jaime Nogueras Arbelo, analista de acción correctiva, al (787) 754-3030, extensión 5617.

Comprometidos en mejorar la fiscalización y administración de la propiedad y de los fondos del Gobierno, para generar valor público con buenas prácticas fiscalizadoras.

Cordialmente,

Myrelis Hernández
Ayudante ejecutiva
Oficina de Asuntos de Auditoría

c Sr. Jorge I. Fernández Porto
Director ejecutivo
Comisión Conjunta Sobre Informes
Especiales del Contralor