PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR
OFICINA DE TECNOLOGÍA

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
5350-AUDITORIA 15526	SISTEMA DE RETIRO PARA MAESTROS	**Deficiencias relacionadas con el informe de análisis de riesgos de los sistemas de información computadorizados** Un análisis de riesgos es un proceso mediante el cual se identifican los activos de sistemas de información, sus vulnerabilidades y las amenazas a las que se encuentran expuestos. Además, se establecen medidas y controles para evitar o disminuir los riesgos y proteger los activos. Toda entidad gubernamental debe realizar un análisis de riesgos, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional. El Sistema cuenta con el Entregable 2: Documento de Estimación y Análisis de Riesgo (Análisis de Riesgo). Este fue preparado y entregado por una compañía externa y aceptado por el Sistema el 19 de mayo de 2009. El examen realizado el 16 de noviembre de 2021 reveló que este análisis carecía de lo siguiente: 1) Un inventario de activos de los sistemas de información que detallara los equipos, programas y datos del Sistema. Esto, con su valoración y clasificación de acuerdo con el nivel de importancia para la continuidad de las operaciones y, en el caso de los datos, su nivel de confidencialidad. 2) La identificación de las posibles amenazas contra los sistemas de información y la probabilidad de que ocurran las mismas.	1- El presidente envió Intrucciones al Director Ejecutivo para que cumpliera con las recomendaciones impartidas por la Oficina del Contralor. El Director Ejecutivo impartió intrucciones para que se revisara y actualizara el Análisis de Riesgo del Sistema para que se incluyera un inventario actualizado de los activos de sistemas de información, la identificación de las posibles amenazas contra estos y la probabilidad de que ocurran las mismas. Este fue preparado	Cumplimentada. Anejo 1 Cumplimentada. Anejo 2

		Falta de actualización de información en la Estrategia de Tecnología y en otros documentos entregables del Sistema Las entidades gubernamentales deben desarrollar un plan de continuidad de negocios que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones basado en un análisis de riesgos. Estos planes deben establecer, entre otras cosas, las estrategias de respuesta, recuperación, reanudación y restauración para todos los procesos principales de la entidad. Estos planes deben ser actualizados cada vez que se incorpore un sistema o aplicación crítica en la entidad o cuando se realice un cambio significativo dentro de su infraestructura operacional. Además, toda entidad gubernamental debe contar con un plan de contingencias para restablecer sus operaciones más importantes en caso de que surja una emergencia. Dicho plan debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de los sistemas de información computadorizados. El Sistema contaba con el Entregable 4: Documento Estrategia de Tecnología (Estrategia de Tecnología) del 28 de junio de 2009, que incluía las actividades concernientes para prevenir y asegurar que la plataforma tecnológica que apoyaba los procesos críticos del negocio fuera reanudada después de un desastre. Esto, para que pudiera continuar su operación y satisfacer las necesidades de sus clientes externos e internos. También se enfocaba en los procesos de negocios y establecía los procedimientos y sistemas necesarios para asegurar la continuación de los servicios indispensables. Además, el Sistema contaba con otros 11 documentos entregables que estaban relacionados con el plan de recuperación de desastres. El propósito de estos era proveer una guía documentada que permitiera recuperar, restaurar y mantener en operación las funciones tecnológicas y de negocio más críticas cuando ocurriera un incidente que potencialmente pudiera afectar al Sistema y generar una interrupción en el Centro de Datos. El examen realizado el 9 de noviembre de 2021 a la Estrategia de Tecnología y a los otros documentos entregables reveló que la información contenida en estos no estaba actualizada, según se indica: 1) Las aplicaciones implementadas luego del 28 de junio de 2009 no estaban incluidas. 2) Como parte de la infraestructura para la continuidad de las operaciones incluían sucursales8 que fueron cerradas. 3) Como parte de los procesos de recuperación incluían la definición de un centro alterno que no existe. 4) Incluían nombres de servidores, sistemas operativos, bases de datos y versiones de aplicaciones que no existían a la fecha del examen. 5) Los nombres incluidos del personal perteneciente al equipo funcional ya no laboraban en el Sistema.	2-Se preparó un Informe sobre Análisis de Riesgos, en el cual se incluyó un inventario de los activos de sistemas de información, la identificación de las posibles amenazas contra estos y la probabilidad de que ocurra las mismas.	Cumplimentada. Anejo 3

		Falta de almacenamiento de los respaldos fuera de los predios del Sistema y de un centro alterno para la recuperación de las operaciones computadorizadas a. Las entidades deben establecer procedimientos para respaldar periódicamente la información y los programas computadorizados, y almacenarlos en un lugar seguro y distante de sus predios. Esto, para que, de ocurrir una emergencia o desastre que afecte las instalaciones principales de la entidad, los respaldos estén disponibles para poder recuperar la mayor cantidad de información. Al 4 de mayo de 2021, en el Sistema se realizaban respaldos de forma automática en la librería de discos virtuales9 localizada en el Centro de Datos10. Los respaldos diarios eran realizados de forma automática durante las noches. Estos se realizaban a las bases de datos11, los repositorios de documentos de los empleados (Fólder Z), la información que los usuarios mantienen en Desktop y en My Documents, las aplicaciones desarrolladas internamente y a las configuraciones e información del Active Directory. En la mañana siguiente, los respaldos de la base de datos eran comprimidos y el especialista en microcomputadoras y redes de comunicación o el administrador de la base de datos los movían manualmente de la base de datos de la librería de discos virtuales a la nube que utiliza el Sistema. Nuestro examen reveló que, al 4 de mayo de 2021, las copias de los respaldos que incluían los repositorios de documentos de los empleados, de la información que los usuarios mantenían en el Desktop y en My Documents, de las aplicaciones desarrolladas internamente y de las configuraciones e información del Active Directory, no se mantenían en un lugar seguro fuera de los predios del Sistema. b. Como parte integral del plan de continuidad de negocios de una entidad, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Al 11 de mayo de 2021, el Sistema no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.	3- El Director Ejecutivo impartió Instrucciones Al Director interino de OTI para que cumpliera con las recomendaciones emitidas por la Oficina del Contralor. A) Se preparo y aprobó un Plan De Recuperación de Desastres en el que se actualizo la Estrategia de Tecnología. B) Se creo una Copia de respaldo de las aplicaciones desarrolladas internamente y de las Configuraciones e Información del Active Directory y se subió a la nube (Azure).	Cumplimentada. Anejo 2 Cumplimentada. Anejo 4 Cumplimentada. Anejo 5
		Deficiencias relacionadas con la administración y **documentación de cuentas de acceso activas en el SABI y PeopleSoft** La información y los programas de aplicación utilizados en las operaciones de las entidades gubernamentales deben tener controles de acceso para su utilización, de manera que solamente el personal autorizado pueda ver los datos necesarios o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deben incluir mecanismos de autenticación y autorización. En la Norma de Uso y Seguridad se establece que la asignación, la modificación y la cancelación de acceso a los recursos de la red y las aplicaciones del Sistema deben ser enviadas a la OSI mediante el Portal de Asistencia a Usuarios12. Cada supervisor de área es responsable de solicitar al dueño de la aplicación (administrador o encargado de la aplicación en su área) o al director, la asignación, modificación y cancelación de accesos y privilegios para los recursos que estén bajo su supervisión. Además, se establece que cada dueño de aplicación y director de área, encargados de sistemas aplicativos, son responsables de la revisión de accesos, al menos, cada seis meses o períodos más cortos si así lo estiman necesario. Si el dueño de una aplicación o director de área no tiene la capacidad de ver los accesos directamente en la aplicación, debe pedir a la OSI los informes de accesos de usuarios para poder revisar los mismos. La función de crear, modificar y desactivar las cuentas de acceso de las aplicaciones del Sistema era realizada por el oficial de seguridad de sistemas de informática. Los supervisores de las oficinas del Sistema eran responsables de solicitar, mediante el Sistema de Ticket o correo electrónico, los accesos del personal que supervisaban. En el 2010, se adquirió el SABI para administrar las transacciones de los participantes que cotizan en el Sistema. Al 31 de mayo de 2021, el SABI contaba con 170 cuentas de acceso asignadas a 158 usuarios activos, quienes realizaban transacciones de acuerdo con los permisos de acceso asignados. Los permisos existentes en el SABI eran Administrador, Administrador de Sistema, Director, Supervisor, Técnico, Operador, y Consulta. **1)** El examen realizado el 15 de septiembre de 2021 sobre la documentación relacionada con la solicitud y autorización de una muestra de 11 usuarios activos en el SABI, al 31 de mayo de 2021, que tenían más de una cuenta de acceso asignada, reveló lo siguiente: a) No se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para solicitar y autorizar la creación de nueve cuentas de acceso asignadas a seis usuarios. b) La documentación entregada para solicitar y autorizar la creación de las cuentas de acceso no incluía lo siguiente: (1) La solicitud y autorización para la creación de cinco cuentas de acceso asignadas a tres usuarios (2) El nombre de las cuatro cuentas a las que se autorizaba el acceso asignadas a dos usuarios (3) La unidad de trabajo a la que tenían acceso para seis cuentas de acceso asignadas a cuatro usuarios (4) El tipo de permiso13 autorizado para cinco cuentas de acceso asignadas a tres usuarios (5) La justificación para la creación de ocho cuentas de acceso asignadas a cinco usuarios. **2)** El examen realizado el 15 de octubre de 2021 sobre la documentación relacionada con la solicitud y autorización de accesos otorgados a una muestra de 11 usuarios activos en el SABI, al 31 de mayo de 2021, con cuentas de acceso que tenían más de un permiso asignado, reveló que de 113 permisos otorgados:	C) Se contrato con Integration Technologies, Corp. para crear un centro alterno en la nube (Azure) para restaurar las operaciones computadorizadas críticas de la Junta De Retiro. D) Se le impartio intrucciones al oficial de seguridad de sistemas de informática conforme a las recomendaciones emitidas en el informe. E) Actualice los sistema operativos de los servidores donde residen el Sistema De Aportaciones Y Beneficios Integrados (SABI) Y de la aplicación PeopleSoft de Finanzas. Se contrató con Integration Technologies, Corp. para mantener en la nube (AZURE) los respaldos de los repositorios de documentos de los empleados, la onformación que los usuarios mantienen en el Desktop y en My Documents, las aplicaciones desarrolladas y las configuraciones del Active Directory. La Junat de Retiro reorganizó las operaciones de los Sistemas de retiro por virtud de la Ley Núm. 1062017. Esto ha permitido unir el personal de OTI del Sistema de Retiro para Maestro y el Sistema de Retiro de los Empleados Públicos , bajo una sola oficina.	Cumplimentada. Anejo 6 Cumplimentada. Anejo 7 y 8 Cumplimentada. Anejo 5 Cumplimentada Anejo 6 Cumplimentada Anejo 9

		a) No se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para la solicitud y autorización de 96 permisos otorgados a las cuentas de acceso asignadas a 10 usuarios. b) De la documentación entregada para solicitar y autorizar los restantes 17 permisos otorgados a las cuentas de acceso asignadas a 5 usuarios, determinamos lo siguiente: (1) No se incluyó la justificación para la asignación de 16 permisos otorgados a 5 cuentas de acceso. (2) Ocho permisos, otorgados a dos cuentas de acceso, no correspondían a los que fueron autorizados. (3) Dos permisos (técnico y director), otorgados a una cuenta de acceso, no incluían autorización. **3)** El examen realizado el 30 de noviembre de 2021 sobre los permisos otorgados a una muestra de 12 usuarios activos en el SABI, al 31 de mayo de 2021, para determinar si el acceso otorgado fue basado en las funciones asignadas y a su puesto, reveló lo siguiente: a) Existían cuatro cuentas de acceso asignadas a tres usuarios con permisos que no correspondían a las funciones de sus puestos, según se indica: (1) La oficial de servicios de retiro auxiliar tenía asignada una cuenta con permiso de administrador de sistemas, que solo debe otorgarse a las cuentas de los empleados de la OSI. (2) El oficial de seguridad de sistemas de informática tenía asignada una cuenta de acceso que, además del permiso de administrador de sistema correspondiente a su puesto, tenía el permiso de supervisor. Este permiso es otorgado a empleados que tienen asignadas funciones de supervisión en el Área de Servicios de Retiro, o de mayor jerarquía. (3) Una voluntaria del Programa de Voluntariado14 tenía asignada dos cuentas de acceso con el permiso de técnico. Este permite realizar transacciones relacionadas con los casos de participantes, tales como añadir, modificar o eliminar data demográfica o numérica. Este permiso es otorgado a empleados que tienen asignadas funciones técnicas o de mayor jerarquía. b) Cuatro cuentas de acceso con permisos de técnico asignadas a una exempleada y a una exvoluntaria, que cesaron sus funciones entre el 28 de febrero de 2020 y el 20 de noviembre de 2020, no se habían desactivado. Esto, luego de haber transcurrido entre 388 y 654 días desde la fecha de separación de estas y el 13 de diciembre de 202115. b. En el 2006 se adquirió PeopleSoft para administrar todas las transacciones de desembolsos que se generan en el Sistema. Al 31 de mayo de 2021, esta aplicación contaba con 102 cuentas de acceso activas. Del examen realizado el 21 de octubre de 2021 sobre la documentación relacionada con la solicitud y autorización de una muestra de 16 cuentas de acceso asignadas a 14 usuarios activos en PeopleSoft, determinamos que no se encontró, ni le fue suministrada a nuestros auditores, evidencia de los documentos utilizados para la solicitud yautorización de 10 cuentas de acceso asignadas a 9 usuarios.		

		Falta de actualización de los sistemas operativos de los servidores donde residen las principales aplicaciones del Sistema El sistema operativo controla la ejecución de los programas de computadoras y provee servicios, tales como asignación de recursos, planificación, controles de entrada y salida, y administración de datos. Las entidades deben verificar y actualizar periódicamente los sistemas operativos de los servidores para protegerlos de vulnerabilidades conocidas, y asegurarse de que los mismos funcionen adecuadamente. Nuestro examen reveló que, al 21 de abril de 2021, los sistemas operativos de los servidores donde residen el SABI, PeopleSoft y sus bases de datos no estaban actualizados. En dicha fecha, el especialista en microcomputadoras y red de comunicaciones nos informó que los servidores, donde reside el SABI y su base de datos, tienen instalado el sistema operativo Windows Server 2008. Además, nos indicó que los servidores, donde reside PeopleSoft y su base de datos, tienen instalados los sistemas operativos Windows Server 2003 y Windows Server 2008, respectivamente. Estos sistemas operativos no cuentan con el apoyo técnico del proveedor desde el 14 de julio de 2015 y 14 de enero de 2020.	5- Se le impartio intrucciones al director del Área de Servicio de Retiro comforme a las recomendaciones emitidas en el informe.	Cumplimentada. Anejo 10