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

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

Indique: ☐ PAC ☒ ICP - 2

Funcionario enlace: Ricardo Dalmau, CPA Puesto: Director Oficina de Auditoría Interna Teléfono: 787-721-9168

Funcionario principal o su representante autorizado: Henry Neumann Zayas Puesto: Secretario Teléfono: 787-721-8259

CERTIFICO QUE ESTA INFORMACIÓN ES CORRECTA Y COMPLETA _____ Fecha: 29 de octubre de 2010
Firma del funcionario principal o su representante autorizado

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
Al SECRETARIO DE RECREACIÓN Y DEPORTES 1. Ejercer una supervisión efectiva sobre el OPI para asegurarse de que: a. Colabore con la persona encargada de ofrecer los adiestramientos durante las orientaciones a los funcionarios y a los empleados del Departamento sobre las normas establecidas en el **Reglamento Interno sobre el Uso de Computadoras del Departamento de Recreación y Deportes**, aprobado el 20 de enero de 2009 por el Secretario, y en otras leyes y políticas aplicables sobre el uso oficial de las computadoras, de	El **Reglamento Interno sobre el Uso de Computadoras del Departamento de Recreación y Deportes** se sometió el 2 de septiembre de 2010 a la Oficina de Asesoramiento Legal para el proceso de revisión y aprobación. El 20 de octubre de 2010 se dió seguimiento a dicho proceso y el mismo no se ha completado.	Parcialmente Cumplimentada

Iniciales _____

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
las cuentas para acceder a Internet y al sistema de correo electrónico. Además, velar por que se conserve evidencia de dichas orientaciones. **[Hallazgo del 1-a.1) al 3) y b.]**	Cuando el reglamento esté aprobado la Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales, en coordinación con el Oficial Principal de Informática ofrecerán a los funcionarios y empleados orientaciones sobre las normas establecidas en el referido reglamento. Veáse Anejo 1	
c. El Administrador de Redes: 1) Identifique las computadoras que tienen problemas con las actualizaciones del programa de antivirus y se establezca un plan para asegurarse de que el archivo de definiciones de virus de las mismas se actualice mediante un proceso alterno automatizado o manual. **[Hallazgo 1-a.4)]**	Veáse Anejo II (Certificación)	Cumplimentada
3) Efectúe las modificaciones en los parámetros de seguridad del sistema operativo para: c) Restringir que los usuarios no puedan repetir las últimas cinco contraseñas utilizadas previamente. **[Hallazgo 5-a.1)c)]**	Véase Anejo III (Certificación)	Cumplimentada

Iniciales_____

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
d) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la Red. **[Hallazgo 5-a.1)d) y e)]**.	Véase Anejo III (Certificación)	Cumplimentada
7) Establezca un máximo de 90 días para cambiar la contraseña en la cuenta de acceso con privilegios de administrador. **[Hallazgo 5-b.1)]**	Véase Anejo III (Certificación)	Cumplimentada
d. Prepare y someta para aprobación: 1) El **Plan de Seguridad** en el que se establezcan los proyectos, las tareas y las actividades requeridas para proteger al personal y a los activos del sistema de información. **[Hallazgo 3-a.]**	Se preparará el Plan de Seguridad requerido en esta recomendación.	No cumplimentada
2) Las normas y los procedimientos para establecer acuerdos de confidencialidad con los funcionarios, los empleados y los consultores del Departamento. **[Hallazgo 3-b.]**	Se continúan preparándose las normas y los procedimientos para establecer acuerdos de confidencialidad con los funcionarios, los empleados y los consultores del Departamento.	No cumplimentada
3) El procedimiento para el manejo de incidentes no esperados. Como parte del procedimiento, se debe requerir que se documenten todos los incidentes y cómo se resolvieron, de manera que cuando se repitan los mismos, se puedan resolver en el menor tiempo posible sin afectar los sistemas de	Se preparará el procedimiento requerido en esta recomendación.	No cumplimentada

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
información y la continuidad de las operaciones. **[Hallazgo 3-c.]**		
4) El Plan de Continuidad de Negocios, que incluya un Plan para la Recuperación de Desastres y un Plan para la Continuidad de las Operaciones. Una vez éste sea aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios del Departamento. Además, asegurarse de que sea distribuido a los funcionarios y los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. [Hallazgo 4-a.]	Se revisará el borrador de Plan de Continuidad para su aprobación final. Véase Anejo IV	Parcialmente Cumplimentada
5) Las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 8.**	Se continúan preparando las normas y los procedimientos para reglamentar las operaciones relacionadas con el sistema de información.	Parcialmente Cumplimentada
e. Se eliminen prontamente las cuentas de acceso de los empleados que cesaron en sus funciones y vea que, en lo sucesivo, las cuentas se eliminen en el momento en que el empleado cesa. Esto, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 5-b.2)**.	La prueba realizada por la Oficina de Auditoría Interna reveló que: a. La Secretaría Auxiliar de Recursos Humanos notifica prontamente a la Oficina de Sistema Información los nombres de los empleados que	Cumplimentada

Iniciales_____

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

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
	cesaron en sus funciones. Veáse Anejo V. b. La Oficina de Sistema de Información inactivo la cuenta de acceso que tenían los empleados que cesaron en sus funciones. Véase Anejo VI.	
f. Establezca una configuración que incluya una Zona Desmilitarizada (DMZ, por sus siglas en inglés) [3] que limite el acceso desde Internet a los servidores de la Red del Departamento y viceversa. Esto es necesario para proteger la Red de ataques cibernéticos y para evitar que personas externas y no autorizadas puedan acceder a ésta y comprometer la seguridad de sus sistemas. [Hallazgo 7-a.]	En esta agencia no es necesario que se establezca una configuración que incluya una Zona Desmilitarizada. Esto debido a los siguientes factores: a. No se ofrece servicio a la ciudadanía mediante el internet. b. Nuestra página de Web se origina de los servidores de la Oficina de Gerencia y Presupuesto (OGP). c. El servicio de navegación en el internet es através de la OGP. d. El servicio de correo electrónico es certificado. e. El servicio de DNS aplica solamente a un dominio local que no depende de proveedores externos. Ej. Dominio.com vs. Dominio.local	Cumplimentada

Iniciales_____

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
g. Actualice el diagrama de las instalaciones y las configuraciones de la Red del Departamento, dentro de un término razonable, para que incluya la información descrita en el Hallazgo 7-b.	Los diagramas de las instalaciones y las configuraciones de la Red del Departamento están actualizados desde el 25 de marzo de 2010. Éstos se sometieron a la Oficina del Contralor el 2 de junio de 2010 como parte del Primer Informe Complementario de este Plan de Acción Correctiva. Véase Anejo VII.	Cumplimentada
3. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece en la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipo y Programas de Información Tecnológica para los Organismos Gubernamentales**, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, y según se sugiere en las mejores prácticas del campo de la tecnología. El informe, producto de este análisis de riesgos, debe ser sometido para su revisión y aprobación. **[Hallazgo 2]**.	El Oficial Principal de Informática realizó y documentó todo lo relacionado con el Plan de Análisis de Riesgos. Este plan fue sometido el 25 de octubre de 2010 a la Oficina de Asesoramiento Legal para su revisión y aprobación. Véase Anejo VIII	Parcialmente Cumplimentada
4. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus equipos en caso de desastres o emergencias en el Departamento, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. [Hallazgo 4-b.]	La agencia continuará realizando gestiones encaminadas a implantar esta recomendación.	Parcialmente Cumplimentada

Iniciales_____

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

PLAN DE ACCIÓN CORRECTIVA

Informe de auditoría: TL-10-06 Número de unidad: 5030 Entidad auditada: Departamento de Recreación y Deportes

Fecha del informe: 1 de octubre de 2009 Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

RECOMENDACIÓN	ACCIÓN CORRECTIVA	RESULTADO
7. Ver que la Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales, en coordinación con el OPI, establezca un procedimiento para que se notifique a tiempo a la OSI el cese de un usuario en sus funciones para la cancelación de su cuenta de acceso. [Hallazgo 5-b.2)]	Este procedimiento fue incluido como parte de las normas establecidas en el **Reglamento Interno sobre el Uso de las Computadoras del Departamento de Recreación y Deportes.** Véase Anejo 1.	Parcialmente Cumplimentada.

Iniciales_____