

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330 - 13615 -01	Sistemas de Información	Falta de un informe de Avalúo de Riesgos sobre los sistemas de información computadorizados	<p>El Departamento de la Vivienda está evaluando la planificación de diseñar un Plan de Avalúo de Riesgo costo efectivo que contenga procedimientos de controles internos necesarios para verificar su efectividad. El Plan propuesto se enfocará inicialmente en los siguientes objetivos:</p> <ul style="list-style-type: none"> · Identificar los activos materiales y el valor monetario asignado a los mismos. Se realizará un inventario de los activos materiales revisando los siguientes factores: <ul style="list-style-type: none"> o Condición del activo y vida útil. o Identificación del activo (# de propiedad único). o Localización del activo. o Costo y valor presente del activo luego de depreciación. o Viabilidad de permanecer con el activo o disponer del mismo. o Clasificación de importancia para la continuidad de operaciones. · Identificar las vulnerabilidades y amenazas de los recursos de sistema de información. Al identificar las vulnerabilidades y amenazas se tomarán en consideración los siguientes factores entre otros: <ul style="list-style-type: none"> o Amenazas de acceso físico no autorizado, acceso no autorizado por intranet y acceso no autorizado por redes externas a los sistemas. o Vulnerabilidad de sistemas por la no actualización de programas, “hardware” y “drivers”. o Vulnerabilidad por la efectividad de los sistemas de resguardo. o Amenazas por eventos de fuerza mayor. 	Se está trabajando con el inventario de propiedad del Área de Sistemas de Información

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330 - 13615 -01 Continuación	Sistemas de Información		<ul style="list-style-type: none"> · Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad de gobierno. Al identificar las amenazas se les asignará un por ciento de probabilidad basado en datos históricos, experiencias pasadas y proyecciones razonables. También se cuantificará el costo de que una de las amenazas suceda y su impacto en las operaciones de la entidad de gobierno. · Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implementarse. Las medidas de seguridad a tomarse para prevenir y superar cualquier amenaza proyectada estarán basadas en un análisis de costo/eficiencia. El costo de las medidas a tomar no puede ser mayor al posible daño de la amenaza. · Se realizará un inventario de los datos contenidos en los sistemas de información y se catalogarán a base del nivel de confidencialidad necesario. · En cumplimiento con la Política Núm. TIG-003, se revisará que los siguientes controles internos estén implementados: <ul style="list-style-type: none"> o Instalación de controles automáticos para la prevención y detección de programas no deseados (i.e. virus, spyware, hardware y updates automáticos). o La seguridad de la información son 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. o La información y los programas de aplicación utilizadas en las operaciones de la agencia tienen controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos que necesita ver, o usar las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles incluyen mecanismos de autenticación y autorización. 	

AGENCIA: DEPARTAMENTO DE LA VIVIENDA

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330 - 13615 -01 Continuación	Sistemas de Información		<ul style="list-style-type: none"> o Todos los mecanismos de autenticación incluyen una contraseña combinada de números y letras, no menor de ocho (8) caracteres. o Los privilegios de acceso de los usuarios son re-evaluados regularmente. o Existen procesos que permiten monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten. o La disposición de equipo que contiene información sensitiva se realiza de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las facilidades de la Agencia. o Implementación de controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde nuestras redes internas hacia otros sistemas de información externos. <p>El análisis de riesgo planificado servirá de base para desarrollar un Plan de Continuidad de Negocios que incluya un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones. Como parte del Plan de Continuidad de Negocios se implementarán procedimientos para tener y mantener una copia de resguardo (backup) recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones. También se revisará que las facilidades de sistemas de información estén colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otras formas de desastres.</p>	

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330 - 13615 -01	Sistemas de Información	Falta de un Plan de Seguridad	<p>El Departamento se encuentra desarrollando un Plan de Seguridad para ser aprobado por el Secretario. El mismo estará en cumplimiento con los requisitos de la Política Núm. TIG-003. Se implementará un programa de adiestramientos a toda la gerencia y los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes. También, el personal de sistemas de información y telecomunicaciones estará adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas. Se crearán mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.</p> <p>El Departamento quiere enfatizar que aunque se encuentre en el proceso de desarrollar un Plan de Seguridad comprensivo, si tiene implementado varias medidas de seguridad tanto a nivel físico como virtual.</p>	
CG 5330 - 13615 - 01	Sistemas de Información	Deficiencias en el Plan de Manejo de Emergencia del Área de Sistemas de Información, flata de acuerdos para mantener centro de recuperación de operaciones y falta de simulacros para comprobar la efectividad de los procedimientos de emergencias	<p>Nos encontramos en el proceso de revisar y actualizar el Plan de Emergencia. Entre las actualizaciones a realizarse se hará referencia a:</p> <ul style="list-style-type: none"> · Los programas utilizados a la fecha como Symantec Backup Exec 2010. · Los servidores virtuales. · El diagrama organizacional del Departamento. · El personal autorizado para acceder la bóveda externa. Ver Anejo I, Manual de Procedimientos Administrativos y Operacionales del Área de Sistemas de Información. · Las pruebas y simulacros realizados para confirmar el buen funcionamiento del Plan de Emergencias. 	

AGENCIA: DEPARTAMENTO DE LA VIVIENDA

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330-13615-01 Continuación	Sistemas de Información		<p>El Departamento está considerando la creación de un centro alternativo de operaciones computarizadas, físico o virtual, en casos de emergencias. La creación del mismo tomará en consideración el costo de la implementación y su beneficio. Como parte del análisis de costo efectividad que nos encontramos realizando se han solicitado varias cotizaciones a distintos suplidores para la creación de un centro alternativo virtual para restaurar las operaciones computarizadas en casos de emergencias. También nos encontramos cuantificando el costo de implementación de un centro alternativo en una de las oficinas regionales. Una vez culminado el análisis de costo, el Departamento elegirá la solución más costo efectiva e identificará los fondos necesarios en su presupuesto para poder implementarlo.</p> <p>Las cotizaciones se solicitaron a los siguientes suplidores:</p> <ul style="list-style-type: none"> · Quantum Systems Integrators, Inc. · Netwave Equipment, Corp. <p>Ver Anejo II, Plan de Emergencia.</p>	
CG 5330 - 13615 - 01	Sistemas de Información	Deficiencias relacionadas con los controles ambientales de los cuartos servidores del ASI en los cuartos de distribución de cableado ("wiring closets") del Departamento	<p>Nos encontramos en el proceso de instalar equipo especializado para verificar de forma preventiva los niveles de humedad en los cuartos de los servidores. Como parte de los procedimientos se ha realizado una requisición a la División de Compras.</p> <p>Según mencionado en comunicaciones anteriores (Ver Anejo III), el Departamento en colaboración con el Arquitecto Fernando L. Pagán de Fase 3 Arquitectura C.S.P., se encuentran en el proceso de avalúo y diseño de mejoras en los cuartos de servidores y cableado.</p>	

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG 5330-13615-01 Continuación	Sistemas de Información		<p>El Departamento ha limpiado de polvo los equipos y sacado partes residuales de equipo de oficina, cajas de cartón, equipo de limpieza de los cuartos de cableado. Además, se encuentra en proceso de adquisición e instalación de una losa electroestática para los cuartos, de modo que se logre reducir el polvo y proteger los equipos. El Departamento verificó la iluminación de los cuartos y refirió las mejoras de la iluminación al personal correspondiente. Ver Anejo IV.</p> <p>El Departamento se encuentra en el proceso de elevar del nivel del piso los equipos de respaldo que se encontraban en los cuartos de cableado. Las soluciones a implementarse incluyen el alza de equipo contenido en el “racking system” y la fijación permanente de equipo a la pared a una altura mayor a las doce pulgadas.</p> <p>Además, el Departamento ha colocado los diagramas esquemáticos de la infraestructura de la red en los cuartos de cableados y mantiene copias disponibles en el Área de Sistemas de Información. Ver Anejo V.</p>	<p>Se instalaron las losas electroestáticas en los cuartos de comunicación</p> <p style="text-align: center;">Completado</p>
CG 5330 - 13615 - 01	Sistemas de Información	Cuentas de acceso activas de exempleados del Departamento	<p>El Departamento implementó un control interno en el que el Área de Recursos Humanos le envía al Área de Sistemas de Información una notificación escrita llamada HOJA DE NOTIFICACIÓN DE EMPLEADOS QUE NO LABORAN EN LA AGENCIA al momento de liquidación de un empleado o cuando este cesa sus funciones con el Departamento. El Área de Sistemas de Información procede a eliminar los accesos al sistema de los empleados contenidos en dicha hoja. Ver Anejo VI.</p> <p>El Departamento se encuentra en el proceso de actualizar el Manual de Procedimientos Administrativos y Operacionales del Área de Sistemas de Información para que contengan la siguiente sección:</p>	

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG5330-13615-01 Continuación	Sistemas de Información		<p>“El Director del Área de Recursos Humanos le enviará al Área de Sistemas de Información la forma titulada HOJA DE NOTIFICACIÓN DE EMPLEADOS QUE NO LABORAN EN LA AGENCIA al momento de liquidación de un empleado o cuando este cesa sus funciones con el Departamento. El Director del Área de Recursos Humanos certificará y firmará la forma. El Área de Sistemas de Información procederá a eliminar los accesos al sistema de los empleados contenidos en la forma.”</p> <p>El Departamento implementó otro control interno en el que el Área de Recursos Humanos le envía al Área de Sistemas de Información un reporte mensual en Excel de los empleados que a la fecha laboran en la Agencia y el Área de Sistemas de Información reconcilia el listado con los usuarios en su sistema. De haber una diferencia, se eliminan los accesos a los empleados que no estén en la lista y se solicita una HOJA DE NOTIFICACIÓN DE EMPLEADOS QUE NO LABORAN EN LA AGENCIA para documentar los procedimientos.</p> <p>El Departamento se encuentra en el proceso de actualizar el Manual de Procedimientos Administrativos y Operacionales del Área de Sistemas de Información para que contengan la siguiente sección:</p>	

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG5330-13615-01 Continuación	Sistemas de Información		<p>“El Área de Recursos Humanos le enviará al Área de Sistemas de Información un reporte mensual en Excel de los empleados que a la fecha laboran en la Agencia. El reporte será enviado dentro de los primeros cinco días de cada mes y contendrá las siguientes columnas: Agencia, Nombre del Empleado, Ubicación, Fecha del Cese y el Número de Tarjeta. El Área de Sistemas de Información reconciliará el listado con los usuarios en su sistema. De haber empleados en el sistema que no aparezcan en el reporte, se eliminarán los accesos al sistema a dichos empleados y se solicitará al Área de Recursos Humanos una HOJA DE NOTIFICACIÓN DE EMPLEADOS QUE NO LABORAN EN LA AGENCIA.”</p> <p>El Departamento se encuentra en el proceso de realizar pruebas para documentar la efectividad de los nuevos controles internos.</p>	
CG 5330 - 13615 - 01	Sistemas de Información	Falta de adiestramiento sobre el uso y la seguridad de los sistemas de información	Según discutido en el Hallazgo 2, el Plan de Seguridad que será sometido al Secretario para su aprobación, contendrá disposiciones relacionadas con la capacitación y adiestramiento del personal que utiliza los sistemas de información. Las disposiciones del Plan de Seguridad serán diseñadas a tenor con la Política Núm. TIG-003.	
CG 5330 13615 - 01	Sistemas de Información	Falta de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados del Departamento, para el trámite de renuncias, separación o destitución de los empleados, y deficiencias en las Normas Sobre el Uso de los Sistemas Electrónicos	<p>El Departamento se encuentra en las etapas finales de aprobación del Manual de Procedimientos Administrativos y Operacionales del Área de Sistemas de Información (Ver Anejo I). El Manual de Procedimientos contiene procedimientos y regulaciones para la administración y seguridad de los sistemas de información computarizados del Departamento, entre los que se encuentran los siguientes:</p> <ul style="list-style-type: none"> · Procedimiento en Control Seguridad Física · Control de Llaves Seguridad Física · Procedimiento para Registro de Contratos · Procedimiento para Reportar de Equipo Garantía (Hardware) · Advertencia para el uso del Sistemas de Información · Procedimiento para Accesar la Red del Departamento 	Está en revisión final para ser entregado a la Secretaría de Asuntos Legales para su aprobación. Una vez aprobado se tramitará para la firma del Secretario

AGENCIA: DEPARTAMENTO DE LA VIVIENDA

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG5330-13615-01 Continuación	Sistemas de Información		<ul style="list-style-type: none"> · Procedimientos para cancelar cuentas de acceso · Procedimiento para crear cuenta nueva en la RED · Procedimiento para Solicitud Servicios Técnicos · Control y/o Inventario de Licencia · Control y/o Inventario de Equipo Electrónico · Requerimiento para solicitar en cualquier Desarrollo de Aplicaciones · Procedimiento para Solicitar Acceso a las Diferentes Áreas y/o Oficinas Utilizando Tarjeta de Aproximación · Procedimiento de Seguridad Lógica de Sistemas de Información · Procedimiento para realizar Resguardo de Información (BACKUP) · Inventario de Servidores · Procedimiento para Prender Servidores en el Área Operacional · Procedimiento para Apagar Servidores en el Área Operacional · Personal Autorizado a acceder la Bóveda de International Safe Deposit · Procedimiento de Manejo de Correspondencia Electrónica (E-Mail) · Auditoría Automática de los Sistemas · Procedimiento para instalar Programas (SOFTWARE) y/o actualizaciones (UP-GRADE) en la RED del Departamento · Plan de Continuidad de Negocio <p>Según discutido en el Hallazgo 5, el Área de Sistemas de Información en conjunto con el Área de Recursos Humanos han implementado controles internos que atienden los casos de separación o destitución de empleados.</p> <p>También, el Departamento revisará y actualizará las normas y procedimientos escritos del Departamento, a tenor con la Política Núm. TIG-008, para incluir, revisar o expandir los procedimientos sobre:</p> <ul style="list-style-type: none"> · Los controles de acceso físico a los sistemas de información. 	

PLANES DE ACCION CORRECTIVA
REQUERIDOS POR LA OFICINA DEL CONTRALOR

Cita o Número de Informe	Oficina Auditada	Descripción de los Hallazgos	Plan de Acción Correctiva	Estatus del Plan de Acción Correctiva
CG5330-13615-01 Continuación	Sistemas de Información		<ul style="list-style-type: none"> · El establecimiento de un itinerario de mantenimiento preventivo del equipo de acuerdo a las especificaciones del proveedor. · La solicitud, la aprobación, la creación, la otorgación de niveles de acceso, la modificación y la cancelación de las cuentas de los usuarios de los sistemas de información. · El desarrollo de nuevas aplicaciones y el control de cambios a las existentes. · La identificación y documentación de incidentes no esperados en las aplicaciones críticas del Departamento. · El monitoreo del funcionamiento de la aplicación crítica del Departamento. · El monitoreo de la utilización del correo electrónico. · El monitoreo de los accesos y el uso de Internet. · La detección de accesos no autorizados a los sistemas de información del Departamento. · La prohibición de utilizar o publicar material que viole los derechos de autor. · El establecer que el Departamento se reserva el derecho de radicar acusaciones por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras. 	
CG 5330 - 13615 - 01	Sistemas de Información	Falta de participación de la Oficina de Auditoría Interna en la evaluación de la seguridad, los controles y las operaciones de los sistemas computadorizados de información del Departamento	<p>Debido a la aprobación e implementación de la Ley Núm. 42 del 16 abril de 2010, Ley del Inspector General del Gobierno de Puerto Rico, la Oficina de Gerencia y Presupuesto absorbió la Oficina de Auditoría Interna del Departamento.</p> <p>Aunque la Oficina de Auditoría Interna se encuentre asignada a otra dependencia, el Área de Sistemas de Información realizará sus propios procedimientos para evaluar los controles internos de los sistemas de información. Un ejemplo sería la verificación de la implementación de los nuevos controles internos descritos en el Hallazgo 5.</p>	