ESTUDIO SOBRE LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD FÍSICA, LÓGICA, CONTINGENCIAS, RESPALDOS Y RECUPERACIÓN DE INFORMACIÓN EN EL DEPARTAMENTO DE INFORMÁTICA (ADMINISTRACIÓN PORTUARIA) Y EN EL ÁREA DE INFORMÁTICA (ADMINISTRACIÓN DE DESARROLLO)

ÍNDICE

Limón, 17 de julio del 2017
AG-AR-008-17

RESUMEN EJECUTIVO DEL INFORME DE AUDITORÍA

ESTUDIO SOBRE LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD FÍSICA, LÓGICA, CONTINGENCIAS, RESPALDOS Y RECUPERACIÓN DE INFORMACIÓN EN EL DEPARTAMENTO DE INFORMÁTICA (ADMINISTRACIÓN PORTUARIA) Y EN EL ÁREA DE INFORMÁTICA (ADMINISTRACIÓN DE DESARROLLO)

¿Qué examinamos?

La auditoría abarcó las acciones realizadas desde el 14 de agosto del 2015 al 17 de julio del 2017, ampliándose en aquellos casos en que se consideró necesario.

¿Por qué es importante?

La Institución debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello se requiere documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, así como asignar los recursos necesarios para lograr los niveles de seguridad requeridos y asegurar la continuidad de los servicios de Tecnología de Información (en adelante TI), mediante un plan que defina la generación de respaldos de información y su recuperación en un sitio alterno, en caso de contingencias informáticas.

¿Qué encontramos?

- Que en el Departamento de Informática no existen suficientes medidas de seguridad física para proteger los recursos de TI; y a pesar de que se poseen alarmas en la puerta de acceso, el funcionamiento de las mismas no se prueba en forma periódica.

- Que no existe certeza de que todos los equipos de cómputo y dispositivos periféricos, instalados en el Departamento de Informática, están incluidos en la Póliza de Incendios No. INC-6314.

- Que el Departamento de Informática no ha establecido procedimientos formales para proteger la información almacenada en cualquier tipo de medio fijo o removible.

- Que el Reglamento para la Utilización de Recursos Informáticos no posee un capítulo sobre planes de contingencias en casos de desastres.

- Que el Área de Informática de la Administración de Desarrollo no cuenta con políticas ni procedimientos de seguridad y contingencias.

¿Qué sigue?

- Se recomienda al Departamento de Informática determinar las medidas adicionales de seguridad física que deben ser implementadas en esa dependencia para fortalecer la protección de los recursos de TI, especialmente cuando los funcionarios no se encuentran laborando, de acuerdo con lo indicado en el punto 2.1 del presente informe.

- Se recomienda al Departamento de Informática probar en forma periódica el funcionamiento de las alarmas, instaladas en la puerta de acceso al mismo, documentando el resultado de dichas pruebas.

- Se insta al Departamento de Informática a coordinar con el Encargado de la Unidad de Seguros la inclusión en la Póliza de Incendios No. INC-6314 de todos los equipos de cómputo y dispositivos periféricos, instalados en el Departamento de Informática.

- Se recomienda al Departamento de Informática elaborar y someter a la aprobación de la División Financiera Contable un procedimiento para proteger la información almacenada en cualquier tipo de medio fijo o removible, que incluya el manejo y desecho de esos medios.

- Se recomienda al Departamento de Informática incluir en el Reglamento para la Utilización de Recursos Informáticos de JAPDEVA un capítulo o artículo sobre planes de continuidad en casos de desastres para el computador central (NX-5600) y los servidores y someterlo a la aprobación del Consejo de Administración.

- Se insta al Área de Informática de la Administración de Desarrollo a participar en forma activa, junto a funcionarios del Departamento de Informática de la Administración Portuaria, en la elaboración de políticas y procedimientos de seguridad de la información, análisis de riesgos y planeamiento contra contingencias informáticas en casos de desastres.

INFORME DE AUDITORÍA

ESTUDIO SOBRE LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD FÍSICA, LÓGICA, CONTINGENCIAS, RESPALDOS Y RECUPERACIÓN DE INFORMACIÓN EN EL DEPARTAMENTO DE INFORMÁTICA (ADMINISTRACIÓN PORTUARIA) Y EN EL ÁREA DE INFORMÁTICA (ADMINISTRACIÓN DE DESARROLLO)

1. INTRODUCCIÓN.

1.1 ORIGEN DEL ESTUDIO.

El presente estudio sobre la implementación de medidas de seguridad física, lógica, contingencias, respaldos y recuperación de información en el Departamento de Informática de JAPDEVA (Administración Portuaria y Desarrollo), forma parte del Plan Anual de Trabajo de la Auditoría General para el año 2017.

1.2 OBJETIVOS DEL ESTUDIO.

1.2.1 OBJETIVO GENERAL.

Determinar la existencia e implementación de medidas de seguridad física y lógica en el Departamento de Informática, tendientes a minimizar el impacto negativo en procesos esenciales de la Institución, cuya interrupción afecta de manera importante la prestación de servicios que se brindan.

1.2.2 OBJETIVOS ESPECÍFICOS.

- Determinar si las medidas de seguridad incorporan de forma oportuna y práctica, con acciones tendientes a minimizar el impacto de los riesgos en los recursos de Tecnología de Información (en adelante TI), según su criticidad.

- Analizar si efectivamente las medidas de seguridad están orientadas a levantar en el menor tiempo posible los servicios críticos que debe brindar JAPDEVA a sus clientes.

- Plantear las medidas correctivas y mejoras de control interno que procedan.

1.3 ALCANCE DEL ESTUDIO Y PERÍODO REVISADO.

El estudio se efectuó de conformidad con la normativa técnica aplicable y el período examinado es el comprendido entre el 14 de agosto del 2015 y el 17 de

julio del 2017, ampliándose en aquellos casos en que se consideró necesario, revisándose legislación, normas y documentos relacionados, según se detalla a continuación:

a. Ley General de Control Interno No. 8292.

b. Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la Contraloría General de la República (en adelante CGR).

c. Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).

d. Objetivos de control para la información y tecnologías relacionadas (Cobit 5).

e. Reglamento para la Utilización de Recursos Informáticos de JAPDEVA.

f. ISO/IEC 27001:2013 (Estándar Internacional de Sistemas de Gestión para Seguridad de la Información); en adelante SGSI.

g. ISO/IEC 27002:2013 (Estándar Internacional de Código para la práctica de SGSI).

h. ISO/IEC 22301:2012 (Estándar Internacional de Sistemas de Gestión para la Continuidad del Negocio).

Adicionalmente se efectuaron entrevistas a los siguientes funcionarios, relacionados todos con la materia.

- MBA Karla Ávila Abrahams, Jefa División Financiera Contable.
- Ing. Rafael Rivas Delgado, Jefe Departamento de Informática.
- MSc. René Palacios Castañeda, Jefe Sección de Análisis y Programación.
- Licda. María Luz Acosta Gómez, Jefa Sección de Soporte Técnico.
- Lic. Danny Morris Brumley, Jefe Área de Informática Desarrollo.
- Licda. Gladys Esquivel Rodríguez, Área de Informática Desarrollo.

2. RESULTADOS.

De la revisión efectuada se obtuvieron los siguientes resultados:

2.1 En el Departamento de Informática no existen suficientes medidas de seguridad física para proteger los recursos de TI.

En el Departamento de Informática se han implementado algunas medidas de seguridad física y ambiental para proteger los recursos de TI, como por ejemplo las siguientes:

- Extintores de incendios.
- Deshumidificador.
- Sistema de control de acceso en la puerta principal.
- Los servidores administrados por la Sección de Soporte Técnico se encuentran en el cuarto de telecomunicaciones, que es un lugar seguro, pues únicamente tienen acceso las jefaturas y el operador del computador central (NX-5600); dicho recinto cuenta con sistema de enfriamiento (aire acondicionado), UPS y planta eléctrica de emergencia.
- Medidas específicas para regular el acceso del personal externo a las instalaciones del Departamento de Cómputo, cuya autorización debe ser conferida por la Dirección de Seguridad Portuaria (ver Anexo No. 1, Reglamento para la Utilización de Recursos Informáticos).

Sin embargo, la infraestructura física del Centro de Cómputo no está diseñada para soportar incendios, terremotos, huracanes y otros siniestros de gran magnitud y carece de hermeticidad, lo que permite la penetración de elementos contaminantes como la salinidad de la brisa marina, polvo y humo, provenientes del tráfico constante de equipo pesado, que a largo plazo aceleran la corrosión de las partes metálicas y daños paulatinos en los componentes electro-mecánicos de los equipos.

Aparte de lo anterior, se carece de medidas básicas de seguridad, necesarias para proteger los equipos de cómputo cuando los funcionarios no se encuentran laborando, tales como cámaras de video, para alertar al personal de seguridad portuaria en caso de accesos no autorizados, detectores de fuego y humo “de aviso temprano” (similares a los sensores de muestreo de aire o de tipo laser) y rociadores automáticos de gases “limpios” (ecológicamente aceptados, como por ejemplo 3M NOVEC 1230 o FM-200) para la extinción de incendios.

Finalmente, a la fecha de emisión del presente informe, el Ing. Rafael Rivas Delgado, jefe del Departamento de Informática, no ha comunicado a esta Auditoría si el computador central (NX-5600), equipo de respaldo y sus dispositivos periféricos, computadoras portátiles y de escritorio, instalados en dicha dependencia, se encuentren incluidos en la Póliza de Incendios No. INC-6314.

El Glosario de las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la CGR en el año 2007, define **seguridad física** como "*la protección física del hardware, software, instalaciones y personal relacionado con los sistemas de información*", mientras que le llama **recursos de TI** a *"las aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TI de una organización*".

Esas mismas Normas, en su capítulo I (Normas de aplicación general), artículo 1.4.3 (Seguridad física y ambiental), según lo detallado en el Anexo No. 2, establecen que:

> **"*La organización debe proteger los recursos de TI, estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos*".**

Es necesario destacar que a la fecha la jefatura del Departamento de Informática no ha definido ni implementado suficientes medidas de seguridad física y ambiental, políticas y procedimientos de seguridad y metodología formal de análisis de riesgos, tendientes a proteger en forma completa y efectiva los recursos de TI, sobre todo cuando el personal no está laborando; y a pesar de que se poseen alarmas en la puerta de acceso a la dependencia arriba indicada, el funcionamiento de las mismas no se prueba en forma periódica.

Las situaciones anteriores podrían causar que la protección física y ambiental de las aplicaciones, información, infraestructura (tecnología e instalaciones) y personas que interactúan en un ambiente de TI, sea insuficiente y podría poner en situación de riesgo dichos recursos, ante la ocurrencia de eventos naturales y/o antrópicos, lo que contraviene aspectos regulados en las Normas supra citadas.

2.2 El Departamento de Informática no ha establecido procedimientos para proteger la información almacenada en medios fijos o removibles.

El Departamento de Informática ha implementado medidas de seguridad, relacionadas con la operación de los recursos de TI y las comunicaciones, a fin de minimizar su riesgo de fallas y proteger la integridad del software y de la información, específicamente medidas preventivas, detectivas y correctivas con

respecto a software “malicioso” o virus, a través del software ESET ENDPOINT ANTIVIRUS.

Sin embargo, a pesar de que los respaldos generados se almacenan bajo llave, no se han establecido procedimientos formales para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, discos duros fijos y portátiles, cartuchos, llaves maya, discos compactos, tarjetas de memoria USB u otros medios), incluso los relativos al manejo y desecho de esos medios.

Aparte de lo anterior, el Departamento de Informática carece de mecanismos formales de control que permitan asegurar la “***no negación***” (según el Glosario de las normas arriba indicadas es la “*condición o atributo que tiene una transacción informática que permite que las partes relacionadas con ella no puedan aducir que la misma transacción no se realizó o que no se realizó en forma completa, correcta u oportuna*”), la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la CGR en el año 2007, en su capítulo I (Normas de aplicación general), artículo 1.4.4 (Seguridad en las operaciones y comunicaciones), inciso b, según lo detallado en el Anexo No. 2, establecen que:

> **“*La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios*”.**

Es necesario indicar que la jefatura del Departamento de Informática a la fecha no ha definido ni implementado formalmente este tipo de procedimientos, tendientes a regular el uso de dispositivos de almacenamiento externo y considerando la eliminación “segura” de cualquier medio fijo o removible, pues en ambientes de microcomputadoras o servidores generalmente se utilizan los comandos del sistema operativo para eliminar los archivos, pero con las herramientas adecuadas es posible recuperar los datos de un dispositivo formateado o de archivo eliminado, incluso después de vaciar la papelera de reciclaje, razón por la cual es necesario contemplar en el procedimiento de marras un método de borrado seguro, como por ejemplo destrucción física del dispositivo, “desmagnetización” y “sobre-escritura”.

La carencia de procedimientos para proteger la información almacenada en medios físicos o removibles expone a la Institución a riesgos innecesarios, como por ejemplo pérdidas económicas por el extravío de dichos medios, el acceso a la información contenida en ellos por personas no autorizadas e inclusive a la infección por virus, en caso de que la intención de la persona sea sabotear o infectar los servidores, lo que contraviene aspectos regulados en las Normas supra indicadas.

2.3 El Reglamento para la Utilización de Recursos Informáticos no posee un capítulo sobre planes de contingencias en casos de desastres.

El Reglamento para la Utilización de Recursos Informáticos, publicado en el año 2006, no posee un capítulo o apartado específico sobre planes de contingencias en casos de desastres para el computador central (NX-5600) y los servidores.

En cuanto al computador central (NX-5600), éste no cuenta con un Plan de contingencias en casos de desastres debido a que es una máquina tecnológicamente desactualizada y no existen en el país equipos con características similares, por lo que esta Auditoría solicitó a la MBA Karla Ávila Abrahams, jefa de la División Financiera Contable, elaborar y ejecutar un cronograma para la migración de los sistemas que allí operan, específicamente el Sistema de Operaciones Portuarias (conocido como POPER) y el Módulo de Planillas y Recursos Humanos, para luego descontinuar el uso de dicho equipo.

Al respecto, el 29 de mayo del 2017 la jefatura supra indicada remitió mediante correo electrónico a esta Auditoría el cronograma de migración de datos y programas del computador central (NX-5600) a bases de datos Oracle, así como el diseño y desarrollo de las soluciones para los Módulos de Facturación, Procesos de Registro de Cobros, Comprobantes de Ingresos, Planillas-Personal, Proceso de Reclamos y N/C (Notas de Crédito) Manuales y Bonificación, actividades que se espera concluir a mediados de agosto del 2017.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la CGR en el año 2007, en su capítulo I (Normas de aplicación general), artículo 1.4.7 (Continuidad de los servicios de TI), según lo detallado en el Anexo No. 2, establecen que:

> **"*La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad*".**

Esta Auditoría se permite indicar que a la fecha la jefatura del Departamento de Informática no ha incluido en el Reglamento arriba indicado un capítulo o apartado específico sobre planes de contingencias en casos de desastres para el computador central (NX-5600) y los servidores.

La situación anterior evidencia la falta de lineamientos que garanticen la continuidad razonable de los procesos señalados, para que su interrupción no afecte significativamente a los usuarios; y además que no se han puesto en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias para el planeamiento contra contingencias informáticas en casos de desastres, lo que contraviene aspectos regulados en las supra citadas Normas.

2.4 En el Área de Informática de la Administración de Desarrollo no existen políticas ni procedimientos de seguridad y contingencias.

De acuerdo con lo informado el 13 de marzo del 2017 por la Licda. Gladys Esquivel Rodríguez, funcionaria del Área de Informática de la Administración de Desarrollo, en sus respuestas al cuestionario de control interno que esta Auditoría le aplicó, la gestión de los sistemas informáticos es ejecutada por el Departamento de Informática de la Administración Portuaria, mientras que su dependencia se encarga del soporte técnico, mantenimiento y reparación de los equipos e instalación de software, lo cual se logró constatar en el "Manual de Procedimientos Informáticos de la Administración de Desarrollo", confeccionado en mayo del 2015.

Según lo comunicado el 27 de abril del 2017 por el Lic. Danny Morris Brumley, Jefe del Área de Informática, en sus respuestas al cuestionario de control interno que esta Auditoría le aplicó, a pesar de que la Gerencia de la Administración de Desarrollo no ha solicitado la implementación de políticas y procedimientos de seguridad, las medidas para garantizar la integridad de la información están contenidas en el supra indicado Reglamento, el cual requiere ser actualizado, pues data de enero del 2006.

El Área de Informática, a pesar de ser independiente funcional y administrativamente del Departamento de Informática de la Administración Portuaria, no tiene implementado un ambiente propio de seguridad de información, carece de políticas, reglas y procedimientos de seguridad, no realiza análisis de riesgos ni posee un plan de contingencias en casos de desastres, pues según criterio de la jefatura arriba indicada, es dicho departamento el encargado de aplicar lo dispuesto en el supra citado reglamento.

Las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas por la CGR en el año 2007, en su capítulo I (Normas de aplicación general), artículo 1.4 (Gestión de la seguridad de la información), según lo detallado en el Anexo No. 2, establecen que:

"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- ***La implementación de un marco de seguridad de la información.***
- ***El compromiso del personal con la seguridad de la información.***
- ***La seguridad física y ambiental.***
- ***La seguridad en las operaciones y comunicaciones.***
- ***El control de acceso.***
- ***La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.***
- ***La continuidad de los servicios de TI*"**.

Es necesario informar que la jefatura del Área de Informática de la Administración de Desarrollo a la fecha no ha creado sus propias políticas y procedimientos de seguridad, lo que impide garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información.

La anterior situación impide proteger dicha información contra el uso, divulgación o modificación no autorizada, daño o pérdida u otros factores disfuncionales. Adicionalmente, causa que el personal de la Administración de Desarrollo desconozca o no esté comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI, lo que contraviene aspectos regulados en las supra citadas Normas.

2.5 Análisis de riesgos y mapa térmico.

En el Anexo No. 3 se presentan los riesgos más relevantes, analizados en el presente estudio, considerando su probabilidad de ocurrencia, calificación (según su impacto para la Administración activa), nivel del riesgo y controles asociados, establecidos por dicha administración.

3. CONCLUSIONES.

De conformidad con los resultados del presente estudio, esta Auditoría arribó a las siguientes conclusiones:

3.1 En el Departamento de Informática no existen suficientes medidas de seguridad física para proteger los recursos de TI; y a pesar de que se poseen alarmas en la puerta de acceso, el funcionamiento de las mismas no se prueba en forma periódica.

3.2 No existe certeza de que todos los equipos de cómputo y dispositivos periféricos, instalados en el Departamento de Informática, están incluidos en la Póliza de Incendios No. INC-6314.

3.3 El Departamento de Informática no ha establecido procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible.

3.4 El Reglamento para la Utilización de Recursos Informáticos no posee un capítulo sobre planes de contingencias en casos de desastres.

3.5 El Área de Informática de la Administración de Desarrollo no cuenta con políticas ni procedimientos de seguridad y contingencias.

4. RECOMENDACIONES.

De conformidad con los hechos señalados y las conclusiones a las que arribó, esta Auditoría se permite efectuar las siguientes recomendaciones:

Para el Departamento de Informática:

4.1 Determinar las medidas adicionales de seguridad física que deben ser implementadas en el Departamento de Informática para fortalecer la protección de los recursos de TI, especialmente cuando los funcionarios no se encuentran laborando, de acuerdo con lo indicado en el punto 2.1 del presente informe.

4.2 Probar en forma periódica el funcionamiento de las alarmas, instaladas en la puerta de acceso al Departamento de Cómputo, documentando el resultado de dichas pruebas.

4.3 Coordinar con el Encargado de la Unidad de Seguros la inclusión en la Póliza de Incendios No. INC-6314 de todos los equipos de cómputo y dispositivos periféricos, instalados en el Departamento de Informática.

4.4 Elaborar y someter a la aprobación de la División Financiera Contable un procedimiento para proteger la información almacenada en cualquier tipo de medio fijo o removible, que incluya el manejo y desecho de esos medios.

4.5 Incluir en el Reglamento para la Utilización de Recursos Informáticos de JAPDEVA un capítulo o artículo sobre planes de continuidad en casos de desastres para el computador central (NX-5600) y los servidores y someterlo a la aprobación del Consejo de Administración.

Para el Área de Informática de la Administración de Desarrollo:

4.6 Participar en forma activa, junto a funcionarios del Departamento de Informática de la Administración Portuaria, en la elaboración de políticas y procedimientos de seguridad de la información, análisis de riesgos y planeamiento contra contingencias informáticas en casos de desastres.

Cordialmente,

MSc. Mainor Loría Núñez
Auditor Designado

Lic. Marvin Jiménez León
Auditor General

ANEXO No. 1

Reglamento para la Utilización de Recursos Informáticos

La Gaceta #6 09-01-2006

Capítulo II (Normas para la seguridad del Departamento de Informática)

Artículo 6º—El acceso al Departamento de Informática es restringido, pudiendo ingresar a él solo el personal autorizado.

Artículo 7º—Toda persona que ingrese al Departamento de Informática y no pertenezca a esta área deberá estar acompañada por un empleado del Departamento.

Artículo 8º—Los visitantes externos a JAPDEVA que estén dentro de las instalaciones del Departamento de Informática deben portar una identificación en un lugar visible que los distinga como visitante.

Artículo 9º—Los visitantes o funcionarios ajenos al Departamento de Informática no podrán ingresar al mismo con bolsos, ni maletines, entre otras cosas. Estos elementos deberán dejarse en la secretaría del Departamento de Informática.

Artículo 10º.—A la biblioteca, la cintoteca, la sala del computador central o a cualquier área así rotulada dentro del Departamento de Informática, sólo podrá tener acceso el personal autorizado.

Artículo 11º.—Queda terminantemente prohibido que los visitantes entren al Departamento de Informática con cualquier medio portátil de almacenamiento de información.

Artículo 12º.—El Departamento de Informática llevará un registro de: hora de entrada, razón de la visita y hora de salida, de todas las personas ajenas al Departamento.

ANEXO No. 2

Contraloría General de la República

Normas técnicas para la gestión y el control de las Tecnologías de Información

(N-2-2007-CO-DFOE)

Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio 2007. Publicada en La Gaceta 119 del 21 de junio 2007

Capítulo I (Normas de aplicación general)

Artículo 1.4 (Gestión de la seguridad de la información).

"*La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos:

- *La implementación de un marco de seguridad de la información.*
- *El compromiso del personal con la seguridad de la información.*
- *La seguridad física y ambiental.*
- *La seguridad en las operaciones y comunicaciones.*
- *El control de acceso.*
- *La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.*
- *La continuidad de los servicios de TI.*

Además debe establecer las medidas de seguridad relacionadas con:

- *El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.*
- *El manejo de la documentación.*
- *La terminación normal de contratos, su rescisión o resolución.*
- *La salud y seguridad del personal.*

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados".

Artículo 1.4.2 (Compromiso del personal con la seguridad de la información).

"*El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.*

Para ello, el jerarca, debe:

a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.

b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.

c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos".

Artículo 1.4.3 (Seguridad física y ambiental).

"*La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar:*

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.

b. La ubicación física segura de los recursos de TI.

c. El ingreso y salida de equipos de la organización.

d. El debido control de los servicios de mantenimiento.

e. Los controles para el desecho y reutilización de recursos de TI.

f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.

g. El acceso de terceros.

h. Los riesgos asociados con el ambiente".

Artículo 1.4.4 (Seguridad en las operaciones y comunicaciones).

"*La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:*

a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

c. Establecer medidas preventivas, detectivas y correctivas con respecto a software malicioso o virus".

Artículo 1.4.7 (Continuidad de los servicios de TI).

"La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad".

ANEXO No. 3: Análisis de riesgos y mapa térmico

A. Posibles Riesgos o eventos	Probabilidad de ocurrencia	Calificación (según su impacto para la Administración activa)	Nivel de riesgo (B*C)	Controles asociados establecidos por la Administración
En el Departamento de Informática no existen suficientes medidas de seguridad física para proteger el equipo de cómputo	4	4	**Muy alto**	No existieron controles para establecer suficientes medidas de seguridad física, tendientes a proteger el equipo de cómputo, sobre todo cuando los funcionarios no se encuentran laborando
El Departamento de Informática no ha establecido procedimientos para proteger la información almacenada en medios fijos o removibles	4	5	**Muy alto**	No existieron controles para establecer procedimientos que protegieran la información almacenada en medios fijos o removibles
El Reglamento de Utilización de Recursos Informáticos no posee un capítulo sobre planes de contingencias en casos de desastres	4	4	**Muy alto**	No existieron controles para establecer un capítulo o artículo en el Reglamento de Utilización de Recursos Informáticos, relacionado con planes de contingencias en caso de desastres
En el Área de Informática de la Administración de Desarrollo no existen políticas ni procedimientos de seguridad y contingencias	5	4	**Muy alto**	No existieron controles para definir e implementar políticas y procedimientos de seguridad y contingencias en el Área de Informática de la Administración de Desarrollo

Área de mapa Térmico

Muy alto	**4**
Alto	**0**
Medio	**0**
Bajo	**0**
Muy bajo	**0**