INFORME Nro. DFOE-SAF-IF-00009-2019

18 de noviembre, 2019

INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LOS CENTROS DE DATOS DEL MINISTERIO DE HACIENDA

2019

Contraloría General de la República, Costa Rica
División de Fiscalización Operativa y Evaluativa
Área de Fiscalización del Sistema de Administración Financiera de la República

CONTENIDO

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Resumen Ejecutivo

¿Qué examinamos?

La auditoría de carácter especial tuvo como objetivo evaluar la seguridad de la información de los centros de datos del Ministerio de Hacienda, para lo cual se evaluaron los controles definidos para asegurar que se cumple con los principios de confidencialidad y disponibilidad de la información en el periodo 2018.

¿Por qué es importante?

El Ministerio de Hacienda brinda servicios a los ciudadanos e instituciones públicas del país, apoyados en las tecnologías de información y comunicación, por lo que estas revisten un carácter estratégico para la institución. Estos servicios deben garantizar la seguridad de la información para la toma de decisiones y la salvaguarda de los activos.

Una tarea fundamental que se encomienda al Ministerio como rector del Sistema de Administración Financiera de la República es la coordinación de las actividades de procesamiento de datos, relacionados con los temas de Presupuesto, Tesorería, Crédito Público, Contabilidad, Administración de Bienes y Contratación Administrativa, declaración y recaudación tributaria, y gestión aduanera, entre otros.

¿Qué encontramos?

En la auditoría se determinó que el Ministerio de Hacienda no cuenta con un plan de continuidad del negocio, con planes de contingencia tecnológica, ni acuerdos de nivel de servicio. La ausencia de dichos controles impide que la administración tome las medidas necesarias para minimizar las pérdidas económicas, afectaciones legales, regulatorias o de imagen, que tendría que enfrentar en caso de que se presente una falla para la cual no esté preparado.

Además, se identificaron debilidades significativas en la seguridad física y ambiental en los centros de procesamiento de datos administrados por el Ministerio de Hacienda, relacionadas con: el acceso físico que garantice que sólo los usuarios autorizados puedan acceder; el cumplimiento de normas que mitiguen los riesgos de incendio o daños por inundación; el deterioro de la infraestructura física y debilidades en el mantenimiento de equipos, tales como el sistema eléctrico, el sistema de alimentación ininterrumpida y los aires acondicionados.

En cuanto a seguridad lógica, se encontraron más de 5.000 cuentas de usuarios activas que no corresponden a funcionarios del Ministerio, lo que pone en riesgo la confidencialidad e integridad de la información, que es procesada y almacenada, en sistemas críticos. Además, se encontraron falencias, en el nivel de complejidad de las contraseñas y la regla de cambio de las mismas, así

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

como, reglas de bloqueo de usuarios y en el proceso para modificar y revocar el acceso de los usuarios a los sistemas.

Se evidenció en la auditoría, que el Ministerio de Hacienda, a pesar de realizar evaluaciones de vulnerabilidades en servidores, no realizó el seguimiento de 20 informes emitidos por la Unidad de Seguridad TIC, por lo que, más de 4.200 vulnerabilidades permanecen activas, exponiendo la información.

Adicionalmente, se determinó que no se aplican actualizaciones de seguridad en los servidores de los sistemas del Ministerio, desde el año 2013. En una muestra seleccionada de los mismos, se identificaron 2.160 vulnerabilidades de seguridad críticas, que pueden ser aprovechadas por personas mal intencionadas, para obtener acceso a información sensible y crítica, y a los sistemas y procesos subyacentes.

Además, se encontró que el Ministerio tiene en uso licencias del software base, que no cuentan con versiones actualizadas y parches de seguridad. También, tiene en uso software de prueba para "emulador de terminales".

Finalmente, no tiene diseñados e implementados procedimientos por medio de los cuales se regule lo atinente a; la documentación de información en estudios de vulnerabilidades y su seguimiento; inventario de software; repositorio de acuerdos de licencias; realización de respaldos y restauraciones; manejo y almacenamiento de la información; eliminación segura de medios de respaldo, y la actualización de la Base de Datos de Configuración CMDB y software de los servidores.

¿QUÉ SIGUE?

Con fundamento en los resultados obtenidos y con el propósito de fortalecer la gestión de tecnología y de seguridad del Ministerio de Hacienda, se gira una disposición al Ministro de Hacienda, para que se implemente un plan de continuidad de negocio.

Por su parte, a la Dirección de Tecnología de Información y Comunicaciones, se le dispone implementar una serie de controles, en la forma de procedimientos, y actividades que permitirán subsanar las debilidades encontradas a nivel operacional.

.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

INFORME Nro. DFOE-SAF-IF-00009-2019

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN DEL SISTEMA DE ADMINISTRACIÓN FINANCIERA DE LA REPÚBLICA

BORRADOR DE INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN DE LOS CENTROS DE DATOS DEL MINISTERIO DE HACIENDA

1. Introducción

ORIGEN DE LA AUDITORÍA

1.1. El estudio se efectuó con fundamento en las competencias que le confieren a la Contraloría General de la República (CGR) los artículos 183 y 184 de la Constitución Política, 12 y 21 de su Ley Orgánica, N.º 7428.

1.2. Al Ministerio de Hacienda como rector del Sistema de Administración Financiera (SAF) le corresponde la coordinación de las actividades de procesamiento de datos, relacionados con los temas de Presupuesto, Tesorería, Crédito Público, Contabilidad, Administración de Bienes y Contratación Administrativa, declaración y recaudación tributaria, y gestión aduanera, entre otros. Como resultado de lo anterior, es el responsable de implementar los controles de seguridad, preventivos, de detección y correctivos que le permitan proteger de forma confiable y consistente la información que procesa, almacena o transmite, los sistemas y tecnología asociada, con el fin de minimizar el impacto de una interrupción en la prestación de los servicios que brinda, la cual de no ser atendida de forma adecuada tendría un impacto negativo alto a nivel país.

1.3. La seguridad de la información es parte integral de la gobernanza de tecnología de información y es la disciplina que orienta los esfuerzos institucionales hacia la salvaguarda de estos activos y el respaldo técnico para la consecución de los objetivos institucionales. Además, permite diseñar e implementar controles para procesar, almacenar y disponer de información por los diferentes sistemas que soportan los procesos encomendados.

1.4. Aunado a lo anterior, las medidas de seguridad de naturaleza técnica y los factores humanos como la concienciación de los usuarios forman y complementan el triángulo de la seguridad, en el cual convergen: la confidencialidad, la disponibilidad y la integridad, lo que permite, que la

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

información no sea revelada a individuos no autorizados, sea accesible, utilizable y que cuente con la protección contra la destrucción o modificación no autorizada.

1.5. Por lo anterior, es relevante que la seguridad de la información sea administrada; que se alcance el cumplimiento normativo y legal aplicable, que permitan garantizar razonablemente al Ministerio la confidencialidad, disponibilidad e integridad de la información para brindar servicios a la ciudadanía.

1.6. El Ministerio de Hacienda es una entidad estratégica para el país, la cual administra información sensible, por lo que debe garantizar su confidencialidad, así como la disponibilidad de la información y los sistemas. Como parte de esa gestión, la seguridad sobre la infraestructura (equipos e instalaciones) y del personal resulta significativa y merece una atención inmediata.

OBJETIVOS

1.7. El estudio tiene como propósito evaluar la seguridad de la información de los Centros de Datos del Ministerio de Hacienda. Esto mediante la valoración de las políticas y procedimientos implementados para almacenar y transferir información de manera segura y la revisión de controles implementados para impedir la divulgación de información a usuarios no autorizados y soportar la continuidad de las operaciones en caso de disrupción.

ALCANCE

1.8. Se evaluaron los controles definidos por el Ministerio de Hacienda para garantizar la confidencialidad y disponibilidad de la información de los Centros de Datos administrados por éste; en el periodo 2018; el cual se amplió en los casos que se estimó necesario.

CRITERIOS DE AUDITORÍA

1.9. Los criterios de auditoría fueron expuestos formalmente al Señor Nogui Acosta, en su calidad de Viceministro de Ingresos y a la Señora Alicia Avendaño, Directora de Tecnologías de Información y Comunicación, el 14 de junio de 2019 y se comunicaron mediante oficio DFOE-SAF-0322 (8657) del 19 de junio de 2019.

METODOLOGÍA APLICADA

1.10. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.11. Para la elaboración de esta auditoría se utilizaron las técnicas y procedimientos estipulados en el Manual General de Fiscalización Integral (MAGEFI) de la Contraloría General de la República. Además, se observó, en lo atinente, las disposiciones contenidas en las Normas Generales de Auditoría para el Sector Público (NGASP), y demás normativa aplicable.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Generalidades Acerca del Objeto Auditado

1.12. El Ministerio de Hacienda asignó la responsabilidad de responder a las demandas tecnológicas a la DTIC, de manera que se obtenga el máximo valor de las inversiones y se garantice la adecuada operación de sus servicios, en un contexto bajo el cual las tecnologías de información se han convertido en un componente estratégico para la prestación de los servicios al ciudadano.

1.13. La DTIC en su estructura organizacional instauró una Unidad de Seguridad de TIC, que reporta al Departamento de Control y Aseguramiento de TIC. Esta unidad tiene como objetivo garantizar la disponibilidad, integridad y confidencialidad de la información relacionada con los servicios TIC, así como asegurar la seguridad física de dichos servicios.

1.14. En línea con lo comentado, el Ministerio de Hacienda contrató el alquiler de centros de procesamiento de datos, equipamiento, servicios de custodia y resguardo de la información, de sus sistemas y tecnología asociada, con un conjunto de proveedores, a saber; el Instituto Costarricense de Electricidad (ICE), Radiográfica Costarricense (RACSA), y la Empresa de Servicios Públicos de Heredia (ESPH).

1.15. Adicionalmente, el Ministerio de Hacienda administraba cuatro instalaciones, en las que se procesaba, almacenaba o transmitía, información; ubicados en el Edificio Central, Edificio Efitec, Edificio Noga y Edificio SIGMA.

1.16. Dada la importancia de la información que se procesa en los mencionados centros, la auditoría consideró pertinente enfocar sus esfuerzos a determinar si ese Ministerio cuenta con los controles adecuados para garantizar razonablemente la seguridad de la información que se transfiere a los centros y la que se mantiene custodiada en los mismos, así como la disponibilidad de dicha información en caso de presentarse una interrupción.

Mejoras Implementadas por la Administración Durante la Auditoría

1.17. En cuanto a la seguridad física de los centros de procesamiento propios del Ministerio, la administración, trasladó los sistemas que se tenían en operación, con el fin de mitigar las debilidades apuntadas por el Órgano Contralor[1], en dos de las instalaciones. Es preciso aclarar, que producto de las acciones realizadas por la Administración, uno de los centros fue totalmente deshabilitado.

1.18. Durante la auditoría, la Administración realizó la depuración de 3.798 cuentas de usuario sin utilidad, que se encontraban en la aplicación que almacena y organiza la información sobre los usuarios de la red, vinculadas al proceso de presentación de declaraciones tributarias.

1.19. La Administración, realizó un análisis de los elementos contenidos en la base de datos de configuraciones (CMDB), y elaboró una propuesta de estructura, que utilizará como punto de partida para actualizar la información, en dicha base.

[1] Oficio N° DFOE-SAF-0232 (4339) del 25 de marzo de 2019.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.20. A finales del mes de julio del 2019, la DTIC autorizó el Procedimiento para Ejecutar Estudios de Vulnerabilidades y/o Auditorías de Cumplimiento MH-DTIC-PRO01-PCD-001, con el fin de detectar comportamientos irregulares en los sistemas informáticos; en los componentes de hardware y software, de los servidores y equipos de red.

1.21. El Ministerio de Hacienda oficializó la Política para la continuidad del negocio (MH-DIPI-PRO02-POL-006) y los procedimientos, elaboración, implementación y mantenimiento del plan de continuidad (MH-DIPI-PRO02-PCD-010) y activación del plan de continuidad de negocio (MH-DIPI-PRO02-PCD-011).

Comunicación Preliminar de Resultados

1.22. Los resultados de la auditoría se presentaron verbalmente el día 28 de octubre de 2019 en las Oficinas de la Dirección de Tecnologías de Información y Comunicaciones, Edificio Sigma, en presencia de los señores: Alicia Avendaño, Directora DTIC; Norma Hidalgo, Sub Directora DTIC; Ana Patricia Hidalgo, Jefe Unidad de Normalización y Control Interno; Rosibel Jiménez, Jefe de Infraestructura; Ademar Guzmán, Jefe del Departamento Servicios TIC; Roy Padilla, Profesional en Informática; Laura Alfaro, Jefe de Gestión de Servicios TIC; Francini Segura, Jefe de Administración de Software; Maria Gabriela Espinoza, Jefe de Redes; Óscar Gómez, Líder Funcional del Proyecto Definición e implementación del Proceso de Continuidad del Negocio; Oldemar Murillo, Sub Auditor Interno a.i.; y Gerardo Mora, Auditor Interno en TI.

1.23. El borrador del presente informe se envió el 4 de noviembre de 2019 a Alicia Avendaño, Directora DTIC con el oficio DFOE-SAF-0616 (17033), con el propósito de que formulará y remitiera a este Órgano Contralor las observaciones que estimara pertinentes sobre el contenido del documento.

1.24. La Administración no remitió observaciones de acuerdo con el oficio DTIC-831-2019.

Siglas

1.25. La descripción de las siglas utilizadas en este documento se detallan a continuación:

Sigla	Significado
CGR	Contraloría General de la República
CPD	Centro de Procesamiento de Datos
DTIC	Dirección de Tecnologías de Información y Comunicación
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
ESPH	Empresa de Servicios Públicos de Heredia
ICE	Instituto Costarricense de Electricidad

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

LGCI	Ley General de Control Interno
MAGEFI	Manual General de Fiscalización Integral
NGASP	Normas Generales de Auditoría para el Sector Público
NTGCTI	Norma Técnica para la gestión y el control de las Tecnologías de Información
RACSA	Radiográfica Costarricense Sociedad Anónima
SLA	Acuerdo de Nivel de Servicio (SLA por sus siglas en inglés)
TICA	Tecnología de Información para el Control Aduanero
UAS	Unidad de Administración de Software
UGSTIC	Unidad de Gestión de Servicios de Tecnología de Información y Comunicaciones
UNSI	Unidad de Normalización y Control Interno de TIC
USTIC	Unidad de Seguridad de TIC

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2. Resultados

Debilidades Relacionadas con la Continuidad de Servicios del Ministerio

2.1. La Norma 1.4.7 “Continuidad de los servicios de TI” de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información[2], establece que la organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios; además, 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.

2.2. Por su parte, la Norma 4.1 “Definición y administración de acuerdos de servicio” prescribe que se debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades, así como que el jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño.

2.3. La Política General de Seguridad de la Información MH-DOM-PRO01-POL-001, lineamiento 6.3.7 “Continuidad de las actividades del Ministerio”, establece requisitos que deben ser abordados en los planes de continuidad, con el fin de minimizar los efectos de interrupciones de las actividades normales y proteger la información sensible o crítica.

2.4. La Política para la Gestión de los Servicios TIC DTIC-POL-033, en el numeral 6, indica que el Gestor de Servicios TIC, debe liderar la creación, modificación o eliminación de los servicios TIC, así como los acuerdos de niveles de servicios, realizando las coordinaciones respectivas con los involucrados y el aval de la Dirección DTIC.

2.5. La Política para la Gestión de la Contingencia Tecnológica (DTIC-POL-036) establece lineamientos para la recuperación de los servicios TIC, ante un evento o desastre, así como, que se debe desarrollar, implementar y mantener vigente un Plan de Contingencia Tecnológica de forma que, en caso de manifestarse una interrupción no deseada o desastre, sea posible reanudar las operaciones tecnológicas según los requisitos y prioridades definidas por la dirección.

2.6. La ISO 22301:2015 “Sistema de Gestión de Continuidad de Negocio”, en su numeral 8.4.4 “Planes de continuidad de negocio” indica que, la organización debe establecer procedimientos documentados para responder a un incidente disruptivo y cómo continuará o recuperará sus actividades dentro de un plazo predeterminado.

[2] N-2-2007-CO-DFOE, aprobadas mediante Resolución del Despacho de la Contraloría General de la República, Nº R-CO-26-2007 del 7 de junio, 2007.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.7. En la auditoría se encontró, que el Ministerio no cuenta con un plan de continuidad de negocio, planes de contingencia tecnológica y acuerdos de nivel de servicio, que le permita, de manera razonable, la recuperación de las operaciones normales ante interrupciones o desastres que le afecten significativamente.

2.8. En cuanto a los planes de continuidad, el Ministerio incluyó una iniciativa de proyecto "Definición e implementación del Proceso de Continuidad del Negocio"[3] como parte de la "Estrategia de implementación de seguridad de la información". El acta constitutiva del proyecto, firmada a finales de noviembre 2017, indicaba que el objetivo del proyecto es "definir e implementar un proceso de continuidad de negocio en el Ministerio de Hacienda, a través del desarrollo de una estrategia enfocada en los procesos críticos de la institución, que permita la recuperación de las operaciones ante interrupciones o desastres tanto operativos como tecnológicos".

2.9. El Líder Funcional indicó al Órgano Contralor[4], que el proyecto tiene un avance del 42%, al 2 de octubre del 2019, no obstante, la fecha de finalización era el 15 de enero de 2019. Además, menciona que realizó las gestiones para el cambio en el cronograma[5] que, de ser aprobado, tentativamente el Ministerio contaría con los planes de continuidad en el primer semestre del 2020.

2.10. Por otro lado, de acuerdo con la información facilitada, se contaba con borradores de planes de contingencias para seis de los dieciocho servicios, a saber; infraestructura de comunicaciones, administración de base de datos, gestión de respaldos, servidores, Tributación Digital, Tecnologías de Información para el Control Aduanero; en abril de 2018. Los borradores fueron enviados a revisión, de acuerdo con los lineamientos de la Política DTIC-POL-036, sin embargo, no se encontró evidencia de su revisión.

2.11. En cuanto a los acuerdos de nivel de servicio (SLA), en la auditoría se encontró, que se han realizado acciones para elaborar los "Acuerdos de Nivel de Operativo" (OLA), que son acuerdos internos que cubren la entrega de servicios que soporta la DTIC, con el fin de respaldar los SLA con el negocio, y así disminuir la brecha entre las expectativas del negocio y los servicios ofrecidos.

2.12. Al respecto, la Jefatura de la Unidad de Gestión de Servicios TIC, facilitó a este Órgano Contralor, los documentos que demuestran el avance en los OLA de Software e Infraestructura, este último incluye las Unidades; Gestión de Redes y Comunicaciones, Administración de Servidores, Gestión de Operaciones TIC, Administración de Base de Datos y Administración de Micros.

2.13. La razón por la cual el Ministerio de Hacienda no cuenta con un plan de continuidad, se debe a que su definición e implementación se ligó al avance de un proyecto, el cual ha tenido un retraso significativo en su ejecución. El proyecto ha tenido tres líderes funcionales, lo cual, conlleva un período de aprendizaje que ocasionó atrasos en el desarrollo de las tareas definidas en el

[3] El Consejo Institucional de Tecnologías de Información (CITI) aprueba la iniciativa en la Sesión Ordinaria Nº 61, efectuada el 16 de febrero de 2017. Aunado, aprueba el caso de negocio del proyecto, en Sesión Ordinaria Nº 65 efectuada el 23 de octubre de 2017.

[4] Oficio DIPI-182-2019, de fecha 3 de octubre de 2019.

[5] Solicitud de Cambio de un Proyecto 002-2019, firmada el 5 de agosto de 2019.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

cronograma; aunado a que, el proyecto se detuvo totalmente por ocho meses en espera del último nombramiento.

2.14. Por otra parte, la dirección de la DTIC señala que la razón por la cual no se cuenta con planes de contingencia tecnológica y acuerdos de nivel de servicio, fue la atención prioritaria de las tareas del proyecto de Migración a Guatuso, implementación y post-implementación; y a la implementación de las leyes de reforma tributaria.

2.15. La ausencia de un plan de continuidad, planes de contingencia tecnológica y acuerdos de nivel de servicio, que le permitan al Ministerio, garantizar de manera razonable, responder, recuperar, reanudar y restaurar a un nivel predefinido la operación; impide que la administración minimize pérdidas económicas, afectaciones legales, regulatorias o de imagen, sí se presenta un evento o falla inesperada que interrumpa las actividades normales.

2.16. Además, el no contar con acuerdos de nivel de servicio, podría generar que el negocio no tenga claridad respecto a la capacidad de la DTIC, para la atención de requerimientos e incidencias, a fin de restablecer el servicio; lo que dificulta que la administración tome decisiones informadas y oportunas en caso de que se presente un incidente que afecte servicios críticos.

DEBILIDADES RELACIONADAS CON LA SEGURIDAD FÍSICA Y AMBIENTAL

2.17. En la auditoría se evidenció, durante las inspecciones físicas realizadas a las instalaciones de procesamiento de datos ubicadas en el Edificio Efitec, Edificio Noga (actualmente subsanado dada la migración al CPD Guatuso) y Oficinas Centrales, factores de riesgo relacionados con el personal y la plataforma (hardware y software). A continuación, se detallan algunas situaciones identificadas:

a) Acceso Físico: No se cuenta con dispositivos adecuados para el control de acceso, que garanticen que solo usuarios autorizados pueden acceder.
b) Peligro de incendio: Se identificaron extintores manuales en el piso, sin carga o vencidos. Asimismo, los sensores de humo se encuentran deshabilitados.
c) Daños por inundación: El centro de procesamiento de datos del Edificio Efitec se encuentra en el primer piso, lo que no es recomendable. Por su lado, en el edificio de oficinas centrales, ubicado en un tercer piso; hay cableado expuesto. Además, no existe un detector de humedad.
d) Aire acondicionado: En Oficinas Centrales y Edificio Efitec, no se evidencia que el sistema de aire acondicionado del centro de procesamiento garantice condiciones ambientales óptimas para el funcionamiento de los equipos que allí se alojan. Además, no se localizó una unidad de aire acondicionado de respaldo y no existe un dispositivo que permitiera monitorear que se mantiene el ambiente a una temperatura idónea para los equipos.
e) Sistema eléctrico: En Oficinas Centrales y Edificio Efitec, se identificaron cajas de breaker sin etiquetar o bloqueadas. En el Edificio Efitec, el sistema de alimentación ininterrumpida se encontraba fuera de servicio y no se cuenta con planta eléctrica para respaldar el aprovisionamiento eléctrico.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.18. En relación con las medidas de protección de activos, las Normas Técnicas para la Gestión y el Control de la Seguridad de la Información[6], en la Norma 1.4.3 "Seguridad física y ambiental" señala 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.

2.19. Por su parte, la Política Seguridad Física y Ambiental MH-DOM-PRO01-POL-003, en el numeral 6 "Declaratoria de la Política", regula lo siguiente: 6.1. Perímetro de seguridad física, 6.2. Controles de acceso físico, 6.3. Protección de edificios, oficinas e instalaciones, 6.5. Aislamiento de las áreas de recepción y distribución, 6.7. Suministros de energía, 6.8. Seguridad del cableado, 6.9. Mantenimiento de equipos, y 6.13. Retiro de los bienes, entre otros.

2.20. La ISO/IEC 27001:2014, en el apartado 9 "Seguridad física y ambiental", punto 9.1, sobre áreas Seguras, indica que, "Las instalaciones de procesamiento de información crítica o sensible de la organización deberían estar ubicadas en áreas seguras y resguardadas por un perímetro de seguridad definido, con barreras de seguridad y controles de acceso apropiados".

2.21. La DTIC[7] indicó, que la razón por la cual, los centros de procesamiento de datos ubicados en el Edificio Central y el Edificio Efitec, presentan las condiciones mencionadas, es que los edificios son antiguos, por lo que no cumplen con los estándares actuales de seguridad para instalaciones de esa naturaleza, así como, que se encontraban en el proceso de migración.

2.22. La situación comentada, expone al Ministerio de Hacienda a un riesgo de accesos no autorizados a las instalaciones físicas, además de exponer la integridad física de los funcionarios que realicen mantenimientos en las instalaciones, en caso de presentarse un siniestro. Principalmente el riesgo de disrupción en la entrega de los servicios críticos de la institución respaldados por los sistemas del Ministerio, podría implicar un detrimento del cumplimiento de los objetivos institucionales.

2.23. La administración indicó[8] que solventará las debilidades mencionadas, trasladando los sistemas y equipos de comunicación al CPD ubicado en Guatuso. Al respecto, facilitaron un calendario que señala como fecha de finalización, el 7 de febrero de 2020.

Debilidades Relacionadas con la Seguridad Lógica

2.24. El Ministerio de Hacienda tiene debilidades en la gestión de la seguridad lógica relacionadas con el nivel de complejidad de las contraseñas y la regla de cambio de las mismas, así como, reglas de bloqueo de usuarios y en el proceso para modificar y revocar el acceso de los usuarios a los sistemas. La revisión se enfocó, en la aplicación que almacena y organiza la información sobre los usuarios de la red y en los sistemas, SIIAT, Integra, SIGAF, TICA, Tesoro Digital y Tributación Digital.

---

[6] N-2-2007-CO-DFOE, aprobadas mediante Resolución del Despacho de la Contraloría General de la República, Nº R-CO-26-2007 del 7 de junio, 2007.

[7] Oficio DTIC-233-2019, del 1 de abril de 2019.

[8] Oficio DTIC 700-2019, de fecha 10 de setiembre de 2018.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.25. Los sistemas evaluados tienen una parametrización débil en lo que respecta a la complejidad de las contraseñas, debido a que la mayoría permiten ingresar contraseñas de menos de ocho caracteres, palabras comunes, secuencias numéricas, entre otros. También, se encontró que en el sistema SIIAT, se permite reutilización de contraseñas y las mismas no caducan.

2.26. Además, la sesión del usuario en los sistemas, no es bloqueada por inactividad o por intentos de ingreso fallidos y no se generan alertas al respecto.

2.27. Por otro lado, se encuentran funcionarios que cambian de ubicación laboral y no hay evidencia de que se haya realizado una valoración para asignar en los perfiles, tales cambios. Además, existen usuarios activos en los sistemas, que corresponden a funcionarios que dejaron de laborar para la institución. Tampoco se suspenden usuarios por ausencias prolongadas como vacaciones, incapacidades, permisos y licencias.

2.28. Adicionalmente, la matriz de autorizaciones no presenta detalles relacionados con las personas que cuentan con facultades, para colocar requerimientos relacionados con cambios en los roles y perfiles de los usuarios finales. Tampoco se cuenta con un registro que permita al área técnica conocer a nivel de sistema, roles y perfiles, los accesos que han sido concedidos a cada funcionario.

2.29. Las Normas técnicas para la gestión y el control de las Tecnologías de Información[9], en su Norma 1.4 indican que la organización debe garantizar, de manera razonable, la confidencialidad, e integridad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados.

2.30. También puntualiza ese marco normativo, en su numeral 1.4.5, que la organización debe establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI; asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización; e implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI.

2.31. La Política de Seguridad para el Control del Acceso Lógico (MH-DOM-PRO01-POL-006) establece en el numeral 6.1, que cada usuario debe tener sólo una sesión abierta por sistema, así como que la Unidad de Seguridad TIC definirá un estándar sobre registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, y que se deben establecer los respectivos controles en relación con el lapso de inactividad de los equipos.

2.32. Por último, la ISO/IEC 27002:2009 “Tecnologías de Información. Código de prácticas para la gestión de la seguridad de la información”, también indica, en su aparte 8.3.3 que “los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información deberían ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia”.

[9] N-2-2007-CO-DFOE, aprobadas mediante Resolución del Despacho de la Contraloría General de la República, Nº R-CO-26-2007 del 7 de junio, 2007.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.33. Las fallas en la parametrización de las contraseñas y bloqueo de usuarios, obedecen a la ausencia de procedimientos relacionados a esta temática.

2.34. Asimismo, las situaciones supracitadas sobre modificación y revocación de permisos de acceso a los sistemas, se presenta por la descentralización del proceso, el cual no garantiza que los responsables, informen de manera oportuna los cambios en la relación laboral de los funcionarios. Además, las responsabilidades y funciones de los administradores de sistemas de aplicación carecen de formalidad.

2.35. La situación que exhibe la aplicación que almacena la información sobre los usuarios de la red, es un ejemplo de las debilidades mencionadas, ya que tiene 1.286 cuentas que no corresponden a usuarios identificables, lo que dificulta que la administración pueda sentar responsabilidades sobre la modificación de los datos en los sistemas, además, se expone la información a acceso no autorizado.

2.36. Al respecto, la DTIC manifiesta que está realizando esfuerzos para atender las debilidades señaladas y para cada una se está desarrollando un proyecto o una actividad tendente a cerrar las brechas entre los controles actuales y las medidas que deben tomarse para favorecer la gestión de seguridad lógica y la configuración de parámetros de seguridad.

DEBILIDADES RELACIONADAS CON LA SEGURIDAD EN LAS OPERACIONES

2.37. La Norma 1.4.4 “Seguridad en las operaciones y comunicaciones” de las Normas Técnicas para la gestión y control de las tecnologías de información[10] establece 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,

> “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.”

2.38. Asimismo, la Norma 4.2 “Administración y operación de la plataforma tecnológica”, establece en el inciso c, que la organización debe controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software). Además, en el inciso h, establece que la organización debe definir formalmente y efectuar rutinas de respaldo, custodiar

[10] N-2-2007-CO-DFOE, aprobadas mediante Resolución del Despacho de la Contraloría General de la República, Nº R-CO-26-2007 del 7 de junio, 2007.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.

2.39. La Norma de control interno para el Sector Público 4.4.1, “Documentación y registro de la gestión institucional”, dicta que el jerarca y los titulares subordinados, deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten.

2.40. El Decreto Nº 37859-H “Estructura Organizacional de la Dirección de Tecnologías de Información y Comunicación”, Artículo 13, dicta a la Unidad de Administración de Servidores, (j) Realizar la actualización física o lógica de los servidores y componentes a su cargo, de forma oportuna y segura y (l) actualizar y velar por la calidad de la Base de Datos de la Configuración (CMBD) en cuanto a los servidores, componentes y otros dispositivos utilizados para la gestión de los servicios TIC.

2.41. En el Artículo 17, del decreto citado, se establece que la Unidad de Gestión de Operaciones de TIC es responsable de auditar y controlar los componentes de un servicio de la Base de Datos de Configuración (CMDB), de velar porque los componentes de los servicios se mantengan actualizados en la (CMDB); de brindar informes de los cambios realizados en la CMDB y las plataformas; y velar por la actualización de los registros cuando existan nuevos componentes de servicio.

2.42. Además, en su artículo 37, inciso d, se establece que la Unidad de Gestión Servicios TIC (UGS), debe diseñar el mapa de cada servicio, a fin de identificar los componentes que soportan la disponibilidad y calidad; dicho mapa sirve de apoyo en la definición de los distintos acuerdos para el servicio.

2.43. En el artículo 44 inciso b, establece que la Unidad de Normalización y Control Interno de TIC (UNCI) debe informar los resultados obtenidos, emitir las recomendaciones correspondientes y dar seguimiento a la atención de las mismas a nivel de la Dirección de Tecnologías de Información y Comunicación.

2.44. Finalmente, en su artículo 48, inciso h, establece que la Unidad de Administración del Software (UAS) debe “establecer y mantener actualizado el inventario de software, así como un repositorio central que contenga todo el detalle del licenciamiento corporativo”.

2.45. En concomitancia con lo indicado supra, la Política de seguridad para respaldos y recuperación de la información DTIC-POL-027, en el numeral 6, indica que se debe establecer e implementar procedimientos de respaldo y restauración de la información para asegurar la continuidad del servicio en un nivel aceptable o de las operaciones esenciales.

2.46. Por su parte, la Política de seguridad para el manejo y destrucción de medios de almacenamiento de datos DTIC-POL-016 vigente de enero 2016 a marzo 2019, y la política MH-DOM-PRO01-POL-008 Política de Seguridad para la gestión de comunicaciones y operaciones vigente a partir de marzo 2019, punto 6.6; establecen pautas para la administración y seguridad de los medios de almacenamiento.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.47. La Política de Control de Software Autorizado, DTIC-POL-041, establece en el punto 6.15 que la Unidad de Administración de Software debe contar con un inventario del software del Ministerio, que considere tanto el software instalado como el no instalado.

2.48. El procedimiento para Ejecutar Estudios de Vulnerabilidades y/o Auditorías de Cumplimiento MH-DTIC-PRO01-PCD-001, en el numeral 5.15, establece que se debe realizar una sesión de trabajo con el personal para explicar los resultados obtenidos y el contenido del informe, para que los responsables de los sistemas y/o infraestructura realicen las remediaciones correspondientes. También, en esta sesión participa el encargado de la Unidad de Normalización y Control Interno de TIC, para gestionar la definición, seguimiento y control del plan de remediación.

2.49. En la auditoría se encontraron deficiencias relacionadas con la seguridad en las operaciones, tales como:

- Inexistencia de procedimientos para la gestión de respaldos;
- debilidades en el proceso de documentación de los estudios de vulnerabilidades y en el seguimiento de los mismo; así como, en la gestión de licencias; y
- desactualización de la base de datos de configuraciones (CMDB) y del software de los servidores.

2.50. En cuanto a la gestión de respaldos, no se han definido procedimientos para, realizar respaldos y restauraciones; el manejo y almacenamiento de la información; y la eliminación segura de los medios de información; de acuerdo con lo que establecen las políticas citadas.

2.51. La Unidad de Gestión de Operaciones de TIC ejecuta los respaldos de los sistemas sin una estrategia documentada. Al respecto, la estrategia que se sigue fue heredada de años anteriores y no se cuenta con documentación que indique si en ese momento obedeció a una estrategia pactada con los propietarios de la información.

2.52. Además, en la inspección física de dos de las localidades en las que el Ministerio mantiene medios de respaldo, se encontraron medios en cajas sin rotulación adecuada, así como, medios con respaldos que datan del 2002, para los cuales, no se posee tecnología para accederlos. El almacenamiento no cuenta con condiciones ambientales, que protejan contra: humedad, calor, luz, campos magnéticos o eléctricos, organismos vivos y caídas, golpes o inestabilidades. Asimismo, no se encontró un inventario que consignara el registro de los medios, su vida útil e información contenida.

2.53. La ausencia de procedimientos formalmente documentados e implementados para realizar el respaldo, la recuperación y el almacenamiento; impiden poder minimizar los efectos de fallas (provocadas o accidentales), en medios físicos o lógicos en operación, que contienen información crítica del Ministerio. Además, la inexistencia de procedimientos para el manejo y eliminación segura de los medios de información, expone al Ministerio a mal uso o divulgación no autorizada de información sensible.

2.54. Con respecto a las debilidades en el proceso de los estudios de vulnerabilidades, de la revisión de cumplimiento del procedimiento MH-DTIC-PRO01-PCD-001, con los estudios realizados en el 2019, se determinó que el mismo se ejecutó parcialmente, y que varias de las sesiones de trabajo

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

no se han realizado. Además, para las tareas del procedimiento que se obtuvo evidencia de cumplimiento, la documentación se encontraba dispersa, lo que dificulta la trazabilidad de la información.

2.55. Asimismo, la UNCI no dio seguimiento a la definición de los planes de remediación, de 20 informes relacionados con estudios de vulnerabilidades, emitidos por la Unidad de Seguridad de TIC (USTIC) entre el 2018 y 2019, por lo que, más de 4.200 vulnerabilidades permanecen activas, exponiendo la información. En el informe DTIC-UNCI-INF-034-2019 firmado el 30 de agosto de 2019, se indica que se dará por cerrados, los informes del año 2018, ya que "no se cuenta con más información de estos casos", refiriéndose a que no tienen planes de remediación.

2.56. La UNCI mantiene un detalle con información de los estudios de vulnerabilidades, en un archivo electrónico, que contiene hojas separadas con información del 2018 y 2019, cada hoja con diferentes formatos y nivel de detalle. Además, emitía un "Informe de Seguimiento a Informes de Vulnerabilidades" mensual, que indica que se realizaba de acuerdo con el requerimiento planteado en el oficio DTIC-083-2018[11]; sin embargo, para agosto 2019 se cambia al responsable del seguimiento y se deja de emitir el informe en cita.

2.57. Es importante aclarar que el seguimiento por parte de la UNCI inicia al finalizar el estudio de vulnerabilidades, con la gestión de la definición del plan de remediación, la no recepción del plan de remediación, no suprime la obligación de la UNCI, de iniciar el seguimiento a las acciones que debe llevar a cabo el responsable en relación con la implementación de las mejoras solicitadas.

2.58. El seguimiento de la implementación de las oportunidades de mejora identificadas en los estudios de vulnerabilidades, es un factor crítico para que la administración implemente las medidas correctivas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, de lo anterior, se desprende la importancia del cumplimiento de las funciones establecidas a la Unidad de Normalización y Control Interno de TIC.

2.59. En lo que se refiere a la gestión de licencias, se encontró que no se mantiene un inventario de software, ni un repositorio con todo el detalle de licenciamiento, ni tampoco un control que integre los acuerdos de licencias asociados, como lo establece la normativa aplicable. Además, se tiene en uso, software de prueba y licencias que no cuentan con versiones actualizadas.

2.60. La UAS tiene las siguientes aplicaciones en las que se almacena información sobre software instalado en los equipos de cómputo. Estas herramientas recopilan la información del software, por conexión de red, de aquellos equipos que estén encendidos al momento de la inspección.

a. Inventario de Software (IS): tiene información de software instalado en computadoras de escritorio y portátiles, permite descargar un resumen en una hoja de cálculo. El resumen cuenta con información sobre el software licenciado y libre, cantidad de licencias según contrato, licencias en uso y su saldo, así como, la indicación de si está disponible.

[11] Oficio DTIC-083-2018, de fecha 6 de febrero de 2018. Se solicita incluir en el PAO la presentación de un informe mensual a la Dirección sobre la macro-actividad "Seguimiento a los planes de acción relacionados con informes de vulnerabilidades de USTIC".

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

b. Open Computer and Software Inventory Next Generation (OCS Inventory): existen dos servidores activos de esta herramienta, uno para computadoras de escritorio y portátiles, y otro para servidores.

2.61. Es importante mencionar que, software que no requiere instalación en equipos, como lo son, las aplicaciones que se administran por accesos vía web o servidores de licencias, no se reflejan en las herramientas citadas.

2.62. La información en los repositorios indicados, es información útil para conocer lo que está instalado en cada equipo, inclusive a nivel de librerías de las aplicaciones, sin embargo, requiere de la integración, análisis y clasificación, para constituir un inventario de software.

2.63. La UAS, en el 2019, elaboró un "Inventario de Contratos", en un archivo electrónico, que contiene información de contrataciones vigentes. El archivo tiene información de algunos de los productos contratados y de la cantidad de licencias por módulo del producto. Dicho registro, no representa un repositorio de licencias, ni un control de acuerdos de licencias, dado que, no tiene el registro de todas las licencias que posee el Ministerio en uso, las características de las licencias (renovación anual, perpetua, otro), o si tienen costos de mantenimiento, entre otros.

2.64. La gestión de licencias tiene como fin último, determinar si es necesario retener, adquirir nuevas, o cancelar las licencias. De forma que, la administración considere la posibilidad de cancelar las licencias que no esté usando y así ahorrar en mantenimiento innecesario, capacitación y otros costos; o, por otro lado, justificar la necesidad de comprar nuevas licencias adicionales para cumplir con los acuerdos de licencia.

2.65. Al respecto, en la auditoría se encontró que el Ministerio tiene en uso licencias del software base, que no cuentan con versiones actualizadas y parches de seguridad. También, tiene en uso software de prueba para "emulador de terminales".

2.66. Cabe mencionar, de acuerdo con el informe DTIC-INF-010-2018[12], que la activación y actualización de las licencias de Tributación Digital, era requisito indispensable para poder migrar el sistema al centro de procesamiento de datos, sin embargo, no se tiene constancia de que se haya realizado la regularización de la situación con el proveedor y el sistema se migró al centro indicado.

2.67. Al no contar con un inventario actualizado y la información de los acuerdos de licencia asociados, el Ministerio se expone a violar los términos con los que adquirió un software, usando copias de software sin licencias o un número excesivo de ellas, incumpliento de la Ley Nº 6683, Ley de Derechos de Autor y Derechos Conexos. Además, debe estar consciente, de que el uso de software sin licencia, se considera una práctica ilegal, que podría generar salidas de efectivo, en caso de reclamos por parte de los proveedores.

2.68. La DTIC indicó, como la razón por la cual no se cuenta con un inventario de licencias, de acuerdo a lo que establece la política, que se consideraba como inventario de licencias la información de la herramienta OCS Inventory.

[12] Informe sobre actualización de licencias de Tributación Digital, DTIC-DCA-INF-010-2018 de fecha julio 2018.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.69. Por otro lado, la desactualización de la Base de Datos de Configuraciones (CMDB)[13] y del Software de los Servidores es una debilidad significativa, que podría incidir negativamente en la confidencialidad, integridad y disponibilidad de la información, que procesa el Ministerio.

2.70. De la revisión de la CMDB, se desprende que los datos que contiene el módulo (nombre, estado, serial, entre otros), no concuerdan con la información actual. Además, del análisis de una muestra de los elementos de configuración, se evidenció que la última modificación fue realizada en el año 2016.

2.71. Adicionalmente, la estructura no es consistente con el catálogo de servicios de TIC, las categorías presentan ambigüedades y no se definieron las relaciones que permiten visualizar el mapa del servicio.

2.72. Que no se cuente con un repositorio actualizado de información de todos los componentes de un servicio, hardware, software, comunicaciones, con la visibilidad de cómo se relacionan entre sí, impide la identificación de los activos cruciales, y eventualmente, el análisis del impacto de los incidentes y cambios.

2.73. Se realizó una prueba con la colaboración de funcionarios de la Unidad de Seguridad de TIC, para verificar la fortaleza del software de los servidores, ante amenazas conocidas al día de la evaluación. Para dicho fin, se seleccionó una muestra de 34 servidores, de una población de 65 servidores en ambiente de producción relacionados con siete sistemas.

2.74. Se determinó que no se aplican actualizaciones de seguridad en los servidores del Ministerio, desde el año 2013. Al respecto, se identificaron 2.672 vulnerabilidades, de las cuales 2.160 indicaron ser críticas.

2.75. Con el fin de conocer la recurrencia de los componentes de software vulnerables y posibles ataques, se seleccionaron 250 vulnerabilidades críticas. Se encontraron 15 componentes de software con vulnerabilidades conocidas, y 9 métodos de ataque. El Cuadro Nº 1, detalla el resultado.

[13] La DTIC, tiene una herramienta de gestión de casos, que contiene un módulo para la Base de datos de Configuración (CMDB), la cual, permite registrar los elementos de configuración que conforman los servicios de TIC, así como las relaciones existentes entre ellos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Cuadro Nº 1

Recurrencia de componente de software con vulnerabilidad y método de ataque

Componente de software con vulnerabilidades	Recurrencia
1- .NET Framework	48%
2- Sistema Operativo acumulativa	13%
3- Componentes gráficos	7%
4- Internet Explorer	6%
5- Adobe Reader	6%
6- Controladores de fuentes	5%
7- Microsoft Malware Protection Engine	4%

Método de ataque	Recurrencia
1- Ejecución remota de código	46%
2- Elevación de privilegios	21%
3- Tomar el control de los equipos	12%
4- Aprovechar vulnerabilidades no reparadas	9%
5- Omisión de la característica de seguridad	6%
6- Ataques de tipo "Man in the middle"	3%
7- Denegación de servicio (DoS)	2%
8- Suplantación de identidad	2%
9- Leer y/o modificar datos	0%

Fuente: elaboración propia.

2.76. Otro aspecto crítico, que pone en riesgo la seguridad de la información que procesa y almacena la DTIC, es que el Ministerio tiene instaladas versiones de sistemas operativos sin soporte del proveedor y otras que pronto estarán fuera de soporte, por lo que ya no reciben actualizaciones de seguridad, dejándolos más vulnerables al ataque de programas maliciosos.

2.77. Proteger los servidores de la exploración y explotación de vulnerabilidades, incluye implementar parches de seguridad de la forma más expedita posible; contar con versiones de sistema operativo actualizadas; desactivar todos los puertos y servicios no utilizados; restringir los privilegios de usuarios solo a aquellos que son exigidos por el rol de cada persona. Esto le permite al Ministerio prevenir que un atacante utilice una vulnerabilidad conocida para obtener acceso no autorizado a información sensible y crítica, y a los sistemas y procesos subyacentes.

2.78. Las deficiencias relacionadas con la seguridad en las operaciones se deben en parte, a que se carece de procedimientos formalmente documentados y en operación para realizar las tareas. La DTIC indicó que los procedimientos se encuentran en proceso de elaboración y oficialización.

2.79. La DTIC señaló, que la razón de la desactualización de la CMDB, fue la migración de toda la plataforma tecnológica al Centro de Procesamiento de Datos Guatuso, en el 2018. Al respecto, se

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

destinaron todos los recursos al proyecto, así como, la implementación de nuevos esquemas de virtualización, actualizaciones y mejoras de la infraestructura.

2.80. Además que, algunos parches de seguridad o actualizaciones que se deberían aplicar, pueden incidir en el desempeño del sistema, por lo que se requiere de coordinación entre los responsables de los sistemas del Departamento de Sistemas de Información, lo que no se ha realizado.

2.81. La dirección de la DTIC indicó que la situación sobre la gestión de respaldos y de licencias, es el resultado de la reestructuración de las áreas de tecnología del Ministerio de Hacienda. Por un lado, la nueva unidad que asumió la gestión de respaldos, recibió los diferentes medios sin contar con un inventario claro y con problemas de etiquetado y los almacenó, tal cual se recibieron; por otro lado, las debilidades relacionadas con el inventario de software y el repositorio de acuerdos de licencia, refleja una práctica que se seguía en la antigua Dirección General de Informática.

2.82. Las debilidades expuestas, relacionadas con los estudios de vulnerabilidades y su seguimiento, son atribuibles, a la falta de gestión de la definición, seguimiento y control del plan de remediación del estudio.

3. Conclusiones

3.1. En la auditoría se determinaron deficiencias significativas de control interno, así como inobservancias de la normativa técnica que regula el accionar del Ministerio de Hacienda, las cuales deben ser objeto de atención por parte de la Administración, con el fin de tomar las acciones correctivas pertinentes para prevenir su ocurrencia, y garantizar de manera razonable, la confidencialidad, integridad y disponibilidad de la información.

3.2. Al respecto, se detalla en el Anexo 1 del informe los criterios que se cumplían parcialmente, así como los que no se están cumpliendo, con la finalidad de que el Ministerio identifique los riesgos que de materializarse pueden afectar significativamente el cumplimiento de los objetivos.

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, Nro. 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución Nro. R-DC-144-2015, publicados en La Gaceta Nro. 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

AL MINISTRO DEL MINISTERIO DE HACIENDA O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar y aprobar un plan de continuidad de negocio para el Ministerio de Hacienda. (ver párrafos del 2.1 al 2.16). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor:

A más tardar el 13 de diciembre de 2019, un cronograma con las acciones, los responsables y los plazos para la elaboración del plan de continuidad.

A más tardar el el 30 de abril de 2020, un reporte con el nivel de avance de las acciones según el cronograma de la elaboración del plan de continuidad.

A más tardar el 30 de septiembre de 2020, una certificación donde conste que el plan de continuidad de negocio para el Ministerio de Hacienda fue aprobado.

A ALICIA AVENDAÑO RIVERA EN SU CALIDAD DE DIRECTORA DE TECNOLOGÍA DE INFORMACIÓN O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.5. Elaborar, aprobar, e implementar los planes de contingencia tecnológica, los acuerdos de nivel operativo (OLA) y los acuerdos de nivel de servicio (SLA) del Ministerio de Hacienda. (ver párrafos del 2.1 al 2.16). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor:

A más tardar el 31 de enero de 2020, un cronograma con las acciones, los responsables y los plazos para la elaboración de los planes de contingencia tecnológica y los acuerdos de nivel operativo.

A más tardar el 30 de junio de 2020, una certificación que haga constar el nivel de avance de acuerdo con el cronograma de la elaboración de los planes de contingencia tecnológica y los acuerdos de nivel operativo.

A más tardar el 30 de noviembre de 2020, una certificación donde conste que los planes de contingencia tecnológica y los acuerdos de nivel operativo fueron elaborados y aprobados.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

A más tardar el 18 de diciembre del 2020, una certificación que haga constar que los planes de contingencia tecnológica y los acuerdos de nivel operativo están implementados.

A más tardar el 26 de febrero de 2021, un cronograma con las acciones, los responsables y los plazos para la elaboración de los acuerdos de nivel de servicio.

A a más tardar el 30 de junio de 2021, una certificación que haga constar el nivel de avance de acuerdo con el cronograma de los acuerdos de nivel de servicio.

4.6. Migrar la totalidad de los sistemas y equipos de acuerdo con el calendario establecido que se encuentran en Oficinas Centrales y en el Edificio Efitec. (ver párrafos del 2.17 al 2.23) Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor, a más tardar el 30 de junio de 2020, una certificación que haga constar que se migró la totalidad de los sistemas y equipos que se encuentran en Oficinas Centrales y en el Edificio Efitec.

4.7. Elaborar, aprobar e implementar procedimientos para, la asignación, modificación y revocación de permisos de acceso; la parametrización de contraseñas y bloqueo de usuarios; realizar respaldos y recuperación de información, el manejo y almacenamiento de la información, la eliminación segura de medios de respaldo; la documentación de los estudios de vulnerabilidades y su seguimiento; la actualización de la base de datos de configuraciones y el software de los servidores; realizar y actualizar un inventario de software que contemple los términos contractuales de uso y un repositorio que contenga todo el detalle de licenciamiento. (ver párrafos del 2.24 al 2.82). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor:

A más tardar el 28 de febrero de 2020, una certificación que haga constar que se elaboraron y aprobaron los procedimientos para, la asignación, modificación y revocación de permisos de acceso; la parametrización de contraseñas y bloqueo de usuarios; realizar respaldos y recuperación de información, el manejo y almacenamiento de la información, la eliminación segura de medios de respaldo; la documentación de los estudios de vulnerabilidades y su seguimiento; relacionados con la actualización de la base de datos de configuraciones y el software de los servidores; realizar y actualizar un inventario de software que contemple los términos contractuales de uso y un repositorio que contenga todo el detalle de licenciamiento.

A más tardar el 30 de junio de 2020, una certificación que haga constar que están siendo aplicados los procedimientos para, la asignación, modificación y revocación de permisos de acceso; la parametrización de contraseñas y bloqueo de usuarios; realizar respaldos y recuperación de información, el manejo y almacenamiento de la información, la eliminación segura de medios de respaldo; la documentación de los estudios de vulnerabilidades y su seguimiento; relacionados con la actualización de la base de datos de configuraciones y el software de los servidores; realizar y actualizar un inventario de software que contemple los términos contractuales de uso y un repositorio que contenga todo el detalle de licenciamiento.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

4.8. Elaborar, un inventario de software que contemple los términos contractuales de uso; un repositorio que contenga todo el detalle de licenciamiento; y un inventario de los medios de respaldo. (ver párrafos del 2.37 al 2.82). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor:

A más tardar el 31 de marzo de 2020, una certificación donde conste que el inventario de medios de respaldo que tiene el Ministerio fue elaborado y que se procedió con la conservación y/o destrucción de los mismos, según corresponda.

A más tardar el 31 de julio de 2020, una certificación donde conste que, se cuenta con un inventario de software que contempla los términos contractuales de uso y un repositorio que contenga todo el detalle de licenciamiento.

4.9. Actualizar, la información de la Base de Datos de Configuración (CMDB); las cuentas de usuario que contiene la aplicación que almacena los usuarios de red y los gestores de cuentas de usuarios de los sistemas del Ministerio; y el software de servidores, en cuanto a, parches de seguridad críticas y renovación de las versiones de los sistemas operativos sin soporte del proveedor. (ver párrafos del 2.24 al 2.82). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor:

A más tardar el 28 de febrero de 2020, un cronograma de las acciones, los responsables y los plazos para realizar la actualización de la información de la Base de Datos de Configuración (CMDB); de las cuentas de usuario que contiene la aplicación que almacena los usuarios de red y los gestores de cuentas de usuarios de los sistemas del Ministerio; y el software de servidores, en cuanto a, parches de seguridad críticas y renovación de las versiones de los sistemas operativos sin soporte del proveedor.

A más tardar el 30 de junio de 2020, un reporte con el nivel de avance de las acciones según el cronograma de la actualización de la información de la Base de Datos de Configuración (CMDB); las cuentas de usuario que contiene la aplicación que almacena los usuarios de red y los gestores de cuentas de usuarios de los sistemas del Ministerio; y el software de servidores, en cuanto a, parches de seguridad críticas y renovación de las versiones de los sistemas operativos sin soporte del proveedor.

A más tardar el 30 de noviembre de 2020, un reporte con el nivel de avance de las acciones según el cronograma de la actualización del software de servidores, en cuanto a, parches de seguridad críticas y renovación de las versiones de los sistemas operativos sin soporte del proveedor.

A más tardar el 30 de noviembre de 2020, una certificación que haga constar que la CMDB; y la aplicación que almacena los usuarios de red y los gestores de cuentas de usuarios de los sistemas del Ministerio se encuentran actualizados.

4.10. Elaborar una estrategia para regularizar la situación relacionada con el uso de licencias del software base, que no cuentan con versiones actualizadas y parches de seguridad, y también, del software de prueba para “emulador de terminales”. (ver párrafos del 2.59 al 2.68). Para dar cumplimiento a esta disposición, deberá remitirse a este Órgano Contralor a más tardar el 31 de

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

marzo de 2020, una certificación donde conste que se elaboró la estrategia para regularizar la situación relacionada con el uso de licencias del software base, que no cuentan con versiones actualizadas y parches de seguridad, y también, del software de prueba para “emulador de terminales”.

JULISSA SAENZ LEIVA (FIRMA) Firmado digitalmente por JULISSA SAENZ LEIVA (FIRMA) Fecha: 2019.11.18 15:39:54 -06'00'

Julissa Sáenz Leiva
Gerente de Área

KAREN VANESSA GARRO VARGAS (FIRMA) Firmado digitalmente por KAREN VANESSA GARRO VARGAS (FIRMA) Fecha: 2019.11.18 15:38:57 -06'00'

Karen Garro Vargas
Asistente Técnico

ALEJANDRO ZUÑIGA GOMEZ (FIRMA) Firmado digitalmente por ALEJANDRO ZUÑIGA GOMEZ (FIRMA) Fecha: 2019.11.18 15:33:45 -06'00'

Alejandro Zúñiga Gómez
Coordinador

MILENA PATRICIA BULGARELLI FUENTES (FIRMA)

Milena Bulgarelli Fuentes
Colaborador

JONATHAN ALONSO ESCALANTE JIMENEZ (FIRMA) Firmado digitalmente por JONATHAN ALONSO ESCALANTE JIMENEZ (FIRMA) Fecha: 2019.11.18 15:35:13 -06'00'

Jonathan Escalante Jiménez
Colaborador

kmm

Ci.: Archivo auditoría

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo 1 Cumplimiento de Normas, Políticas de Seguridad y Prácticas

Continuidad de Negocio y Contingencia Tecnológica

No.	Criterio	Detalle	Cumple
1	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)	1.4.7 Continuidad de los Servicios de TI	No
2	Política General de Seguridad de la Información (MH-DOM-PRO01-POL-001)	6.3.7 Continuidad de las actividades del Ministerio	No
3	Política para la Gestión de la Contingencia Tecnológica (DTIC-POL-036)	Numeral 6, Declaratoria	No

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo 1 Cumplimiento de Normas, Políticas de Seguridad y Prácticas (continuación)

Seguridad Física y ambiental

No.	Criterio	Detalle	Cumple
4	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)	1.4.3 Seguridad física y ambiental, incisos a, b, d, e, f, h	No
5	Política de Seguridad Física y Ambiental (MH-DOM-PRO01-POL-003)	6.1 Perímetro de Seguridad Física 6.2 Controles e Acceso Físico 6.3 Protección de edificios, Oficinas e Instalaciones 6.5 Aislamiento de las Áreas de Recepción y Distribución 6.7 Suministros de Energía 6.8 Seguridad del Cableado 6.9 Mantenimiento de Equipos 6.13 Retiro de Bienes	No
6	Técnicas de Seguridad - Sistemas de gestión de la seguridad de la información - Requisitos (INTE/ISO/IEC 27001:2014)	9.1.1 Perímetro de Seguridad Física 9.1.2 Controles acceso físico 9.1.4 Protección contra amenazas externas y de ambiente 9.2.2 Elementos de Soporte 9.2.3 Seguridad en el cableado 9.2.4 Mantenimiento de Equipo	No

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo 1 Cumplimiento de Normas, Políticas de Seguridad y Prácticas (continuación)

Seguridad Lógica

No.	Criterio	Detalle	Cumple
7	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)	1.4.5 Control de acceso, incisos a, b, c, e, f	Parcial
8	Política de Seguridad para el Control del Acceso Lógico (MH-DOM-PRO01-POL-006)	6.1 Aspectos generales sobre el control de acceso lógico 6.2 Administración de accesos de usuarios	No
9	Política de seguridad para la finalización de relaciones laborales o cambio de funciones o dependencia (DTIC-POL-023)	6.3 Revocación de derechos de acceso	Parcial
10	Política de seguridad para el uso de métodos de autenticación (DTIC-POL-029)	6.1 Sistemas de autenticación 6.2 Reglas sobre el cambio de contraseñas 6.3 Reglas para el uso de métodos de autenticación	Parcial
11	Tecnologías de Información. Código de prácticas para la gestión de la seguridad de la información (ISO/IEC 27002:2009)	8.3.3 Remoción de derechos de acceso	No

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo 1 Cumplimiento de Normas, Políticas de Seguridad y Prácticas (continuación)

Seguridad de Operaciones

No.	Criterio	Detalle	Cumple
12	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)	1.4.4 Seguridad en las operaciones y comunicaciones, inciso a, b, c 4.1 Definición y administración de acuerdos de servicio 4.2 Administración y operación de la plataforma tecnológica, inciso h, b,c, d	No
13	Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE)	4.4.1 Documentación y registro de la gestión institucional	No
14	Decreto No. 37859-H Estructura Organizacional de la Dirección de Tecnologías de Información y Comunicación	Artículo 13, incisos j, l Artículo 17 Artículo 37, inciso d Artículo 44, inciso b Artículo 48, inciso h	No
15	Procedimiento para ejecturar estudios de vulnerabilidades y auditorías de cumplimiento (MH-DTIC-PRO01-PCD-001)	Numeral 5, Procedimientos	Parcial
16	Política de Seguridad para la gestión de comunicaciones y operaciones (MH-DOM-PRO01-POL-008)	6.6 Administración de la seguridad de los medios de almacenamiento	No
17	Política de seguridad para el manejo y destrucción de medios de almacenamiento de datos (DTIC-POL-016)	Numeral 6, Declaratoria	Parcial
18	Política para la Gestión de los Servicios TIC (DTIC-POL-033)	Numeral 6, Declaratoria	Parcial
18	Política de Control de Software Autorizado (DTIC-POL-041)	6.3 Contratos de licenciamiento 6.12 Actualización de software de servidores 6.15 Inventario de software 6.16 Revisión de inventario de software	Parcial

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Glosario

Acuerdo de Servicio: Los acuerdos de servicios, mejor conocidos como convenios o acuerdos de nivel de servicio (“SLA’s” por sus siglas en inglés de “Service Level Agreement”) son contratos escritos, formales, desarrollados conjuntamente por el proveedor del servicio de TI y los usuarios respectivos, en los que se define, en términos cuantitativos y cualitativos, el servicio que brindará la dependencia responsable de TI y las responsabilidades de la contraparte beneficiada por dichos servicios. (N-2-2007-CO-DFOE)

Amenaza: Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado. (ISO/IEC 13335)

Base de Datos: Colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la organización.(N-2-2007-CO-DFOE)

Base de datos de configuraciones (CMDB por sus siglas en inglés de “Configuration Management database”) Base de datos utilizada para almacenar los registros de configuración a lo largo de su ciclo de vida. En la CMDB también se conservan las relaciones entre los registros de configuración. (ITIL V4)

Confidencialidad de la información: Protección de información sensible contra divulgación no autorizada. (N-2-2007-CO-DFOE)

Continuidad de negocio: Prevención, mitigación y recuperación contra las interrupciones. También se pueden usar en este contexto los términos "planes de reanudación de negocios", "planes de recuperación de desastres" y "planes de contingencia"; todos se concentran en los aspectos de recuperación de la continuidad. (ISACA 2015)

Contingencia: Riesgo que afecta la continuidad de los servicios y operaciones. (N-2-2007-CO-DFOE)

Disponibilidad de la información: Se vincula con el hecho de que la información se encuentre disponible (v.gr. utilizable) cuando la necesite un proceso de la organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere. (N-2-2007-CO-DFOE)

Hardware: Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan (software). (N-2-2007-CO-DFOE)

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Integridad: Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio. (N-2-2007-CO-DFOE)

Migración: Proceso de traslado de datos o sistemas entre plataformas o entre sistemas. (N-2-2007-CO-DFOE)

Parche de seguridad: Aplicativo que permite realizar ajustes a los programas para corregir errores o introducir nuevas funcionalidades de seguridad.

Procesamiento de datos: captura almacenamiento y transformación de grandes cantidades de datos para convertirlo en información valiosa, la acumulación y manipulación de elementos de datos para producir información significativa. (N-2-2007-CO-DFOE)

Riesgo: La combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 73)

Seguridad de información: Garantiza que dentro de la empresa la información esté protegida contra la divulgación a usuarios no autorizados (confidencialidad), la modificación indebida (integridad) y el no acceso cuando se requiere (disponibilidad).

Seguridad Lógica: Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Software: Los programas y documentación que los soporta que permite y que facilitan el uso de la computadora. el software controla la operación del hardware. (N-2-2007-CO-DFOE)

Sistema de alimentación ininterrumpida (UPS por sus siglas en inglés de “Uninterruptible Power Supply”): Sistema de suministro de energía de respaldo de corto tiempo proveniente de baterías para un sistema de computadora cuando falla la energía eléctrica o la misma cae a un nivel no aceptable de voltaje. (ISACA 2015)

Vulnerabilidad: Deficiencia en el diseño, implementación, operación o el control interno de un proceso que podría exponer al sistema a las adversidades de eventos de amenazas. (ISACA 2014)

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica