EVALUACION SOBRE LA ADMINISTRACIÓN Y CONTROL DE LA ACTUALIZACIÓN DEL SOFTWARE ANTIVIRUS.

1. INTRODUCCIÓN

1.1 Origen.

El informe se desarrolla acorde al Plan Estratégico de esta Auditoría Interna.

1.2. Aspectos objeto de estudio.

Comprobar el cumplimiento de la normativa relativa a control interno y administración de riesgos en el proceso denominado “Actualización del software antivirus”.

1.3 Alcance.

Los periodos comprendidos entre 1° de enero de 2017 al 1° de enero de 2019.

1.4 Exposición a la administración.

Según consta en el acta No. AI-007-2019 del veintitrés de agosto del dos mil diecinueve, se presentan los resultados del estudio en mención al Director General Adjunto y jefatura de la Unidad de Informática, ambos de este Instituto.

1.5 Marco de referencia

- Ley No. 8292 General de Control Interno.
- Ley No. 8204 sobre Estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, financiamiento al terrorismo, legitimación de capitales y actividades conexas y sus reformas.
- Manual de Normas de Control Interno para las entidades sujetas a las disposiciones de la Contraloría General de la República.
- Manual de Normas para el ejercicio de la Auditoría Interna promulgado por la Contraloría General de la República.
- Manual Técnico de Normas para las Tecnologías de Información de la Contraloría General de la República.

1.6 Limitación al alcance.

Criterio técnico en los aspectos de lógica del software antivirus, por cuanto esta unidad de Auditoría Interna carece de un profesional en el ámbito de sistemas de información, no obstante, se analizan los aspectos físicos para determinar mejoras sobre la administración de control y riesgo del proceso.

1.7 Generalidades.

El presente informe contiene los resultados de la evaluación del proceso denominado “Actualización del Software Antivirus, enfocado en la seguridad física de la información que se genera en el Instituto Costarricense sobre Drogas (ICD) como parte de la ejecución de los alcances del Plan Anual de Trabajo de la Auditoría Interna.

Se analizaron componentes de la seguridad física que comprenden la revisión de las licencias del software antivirus, política de seguridad de la información, sin embargo, no se suministra criterio sobre la seguridad a nivel de dominio, de bases de datos, de aplicaciones, así como otros aspectos que se consideren del área lógica por lo expuesto en el apartado de limitaciones.

Este informe incorpora un apartado denominado resultados con la descripción de un conjunto de situaciones encontradas que reflejan omisiones de control interno que no favorecen la debida protección de la información que se genera y procesa en forma automatizada en la institución.

El informe también contiene una conclusión general que expresa una opinión global sobre la gestión de la seguridad de la información que tiene implementada la institución por medio de la Unidad de Tecnologías de Información. De igual forma, se incluyen las recomendaciones que procuran orientar a la entidad para que mejore su sistema de control interno en lo relativo a la seguridad de la información.

2. RESULTADOS.

2.1 Políticas de seguridad.

El ICD realizó un importante esfuerzo que se concretó con la elaboración de un marco de seguridad de la información denominado “Normas de seguridad de datos según la aplicación de los principios de PCI DSS (Payment Card Industry) que se elaboró en octubre 2012, dirigido por el jefe de Tecnologías de Información (TI) para que fuese puesto en ejecución, según consta en el documento ICD-UI-SD001-2012.

Dicho modelo de seguridad define las relaciones con proveedores y contratistas que manejen información sensible de la institución, medidas adicionales como lo son el software antivirus que fortalezca la integridad de los datos y disminuya la vulnerabilidad de la plataforma tecnológica.

Al respecto, se tiene que el certificado de licencia actual se denomina ESET Endpoint Security + File Security con vigencia hasta el 07 de diciembre del presenta año, cuyo proveedor y distribuidor autorizado es la empresa BL ONE S.A. precisamente se hace un abordaje por el tema del antivirus institucional y consecuentemente con la política de seguridad.

El 11 de junio de 2019 por medio de una entrevista realizada al jefe de la unidad objeto de evaluación, que consta en el acta No. AI-027-2017 esta unidad le consulta a dicho funcionario sobre el objetivo principal del proceso evaluado, el cual responde:

> *“Protección de la información de los usuarios y servidores de la institución contra el software malintencionado.”.*

Además, indica[1] que él es el responsable de la actualización y administración del antivirus contratado; y en cuanto a la política de seguridad, afirma tener el documento, que se hace una revisión todos los años y que actualmente no se ha |actualizado, se hace en el segundo semestre, ya está programado.

Mediante el trabajo de campo se conoció el documento Normas de Seguridad de Datos, cuenta con una versión, que data del año 2012 y no constan las

[1] Acta No. AI-027-2019 del 11 de junio 2019.

modificaciones y actualizaciones descritas por el jefe de TI en la entrevista ejecutada por esta unidad. Dicho manual contiene requisitos que deben ser cumplidos para una correcta gestión de la información, los cuales se mencionan de seguido:

- ✓ Instalar y mantener una instalación adecuada de firewall.
- ✓ No utilizar contraseñas u otros parámetros provistos por los proveedores.
- ✓ Utilizar y actualizar regularmente el software o los programas antivirus.
- ✓ Desarrollar y mantener sistemas y aplicaciones seguras.
- ✓ Datos institucionales.
- ✓ Probar con regularidad los sistemas y procesos de seguridad
- ✓ Mantener una política de seguridad de la información.

A priori de analizar los requisitos, es importante señalar que dada las limitaciones de esta unidad, para realizar auditorías de sistemas ante la ausencia de un profesional en esa materia, no se profundizará en temas relacionados con la lógica del sistema, se tratará la etapa de documentación en donde se visualizó omisión a las acciones ejecutadas relativas a frecuencia de las tareas, tiempos, avances, porcentajes de cumplimiento para desempeñar a cabalidad los requisitos y, aspecto que no fue posible su comprobación por cuanto TI no respalda los procedimientos de prueba contenidos en el documento que sustenta la política por parte de la unidad evaluada.

Lo anterior, compromete la vulnerabilidad de la información significativamente afectando la gestión de la plataforma tecnológica del ICD, con el riesgo de que no se cumplan los objetivos planteados por la unidad de Tecnologías de Información.

La seguridad de la información comprende una extensa área de la informática, donde se ven involucrados aspectos relacionados a los dispositivos de hardware como de software, el entorno físico donde se almacenan y resguardan los datos, así como el control de acceso a las instalaciones. Es prudente recordar que las Tecnologías de Información constituyen uno de los principales instrumentos que apoyan

la gestión de las organizaciones mediante el manejo de grandes volúmenes de datos necesarios para la toma de decisiones y la implementación de soluciones para la prestación de servicios agiles y de gran alcance.

Los ataques o intentos por violentar la seguridad de la información pueden provenir de factores tan diversos que comprenden desde accesos no autorizados a la red, ingreso a dispositivos de seguridad, virus, malware entre muchos otros, haciendo de la labor de seguridad, una tarea que debe ser meticulosa y muy bien planificada. Al respecto la norma 1.4 Gestión de la seguridad de la información establece:

> *"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 perdida u otros factores disfuncionales.".*

Consecuentemente, la norma 1.4.2 Compromiso del personal con la seguridad de la información señala:

> *"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.".*

Ambas normas puntualizan aspectos relevantes, razonabilidad y compromiso, no se trata exclusivamente de establecer documentos que incluyan políticas, manuales, protocolos, la administración deber ser proactiva y llevar a la practica todos aquellos aspectos que estén reflejados en un documento.

Esta Auditoría considera que sin el uso de indicadores de desempeño no es posible medir si los esfuerzos de alineamiento y el cumplimiento de metas de TI está generando valor para la entidad, si está reduciendo los riesgos que enfrenta la organización y si está posibilitando un uso óptimo de recursos.

En virtud de lo anterior, debe la unidad de Tecnologías de información establecer mediante indicadores de desempeño las medidas necesarias para concretar en la práctica todos los requisitos establecidos en su política de seguridad de la información, además actualizarla con el propósito de demostrar las acciones de implementación que dan cumplimiento a la misma.

2.2 Relativo a la gestión de riesgos asociados a la seguridad de la información.

La institución por su naturaleza y la necesidad que tiene de garantizar la protección de la información debe considerar dentro de su análisis de riesgos los eventos a los que está expuesta la organización, relativos a posibles fugas de datos sensibles y la pérdida de información, para determinar que las medidas de mitigación implementadas sean congruentes con el riesgo definido.

La revisión de los procesos de gestión implementados por la entidad mediante la herramienta (SIGMA) mostró que se ha omitido la identificación y valoración de eventos de riesgo que amenacen la información que administra la institución. No fue posible para esta unidad comprobar la administración del riesgo en relación con el nivel, impacto, y mitigación de este, por cuanto se carece de métricas que permitan conocer si la entidad cuenta con un adecuado nivel de protección de sus datos contra posibles incidentes; y a la vez determinar si los controles implementados están resultando eficaces o carece de registros de eventos materializados que afecten información sensible de la entidad.

Lo indicado muestra que la institución ha omitido el análisis y valoración de eventos de riesgo fundamentales para su accionar desaprovechando los procesos de gestión de riesgo para fortalecer el sistema de control interno en un componente relevante. Los párrafos anteriormente descritos se fundamentan en afirmaciones realizadas por el jefe de TI mediante una entrevista que esta Auditoría aplicó el pasado 11 de junio del presente año, el cual indica:

> *"Tenemos diferentes barreras de seguridad en ese sentido, tenemos un nivel superior o de frente a la institución que es un muro de fuego, ahí se establecen políticas de acceso, luego en ese mismo muro de fuego, tenemos un IDS (Sistema de detección de intrusos) y hay un complemento que se llama IPS (Sistema de prevención de intrusos). Además de eso hay políticas de control de acceso, donde se filtra el tipo de comunicaciones que vamos a permitir en la institución. Luego un sistema de control de contenido, lo que nos permite catalogar el tipo de contenido que entra y que sale de la institución. En el nivel más bajo esta el antivirus, que protege las estaciones de trabajo y las cuentas de correo electrónico.".*

Por lo anterior, no se obtuvo evidencia en el Sistema de Gestión y Monitoreo de actividades (SIGMA) sobre riesgos identificados a las barreras de seguridad anteriormente descritas por la jefatura de TI.

Existe una serie de efectos negativos los cuales maximizan el riesgo de TI y vulneran componentes tales como: servidores físicos, virtuales, aplicaciones internas y externas, software de oficina (correo electrónico) enrutadores, swicht, firewall, y otros, en el tanto no estén identificados los riesgos inherentes a las barreras de seguridad implementadas por TI para la protección de la plataforma tecnológica institucional que puede derivar en perdida o robo de información, hackeo de la red por medio de la incursión de intrusos y daño en los componentes electrónicos.

La norma 1.3 Gestión de riesgos del manual de normas técnicas para la gestión y el control de las tecnologías de información señala:

> *"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos* ***que esté integrada al sistema específico de valoración de riesgos institucional y considere el marco normativo que le resulte aplicable*** *(el subrayado y la negrita es nuestro).".*

Es prudente que el jefe de la unidad de TI administre de forma oportuna y correcta los riesgos asociados a las barreras de seguridad que actualmente mantiene la institución, los incorpore a la herramienta que corresponda, con el propósito de identificarlos, conocer la probabilidad, impacto, nivel y acciones para mitigarlos y afinidad a los riesgos institucionales contemplados en el Sistema Específico de Valoración de Riesgos.

2.3 Datos sensibles residentes en medios de almacenamiento.

La evaluación realizada determinó que no se ha formalizado, ni reglamentado el uso de este tipo de herramientas (medios de almacenamiento fijos o removibles). Actualmente los funcionarios del ICD tienen acceso a la red institucional e incorporar en dispositivos USB, memorias extraíbles (discos duros independientes), discos compactos y celulares la información almacenada en las carpetas de las unidades del ICD, tanto en el dominio público como en cada unidad.

Lo anterior, muestra que la institución está expuesta a que se extraiga de estaciones de trabajo, portátiles, discos duros externos o memorias tipo USB información sensible que esté almacenada ahí, por cuanto se carece de procesos y herramientas definidas que reduzcan los riesgos de fuga de información.

Una de las alternativas que está disponible para la protección de datos sensibles que se manejen en computadoras de escritorios, equipos portátiles, discos duros externos o unidades de memoria tipo USB es el uso de software de encriptación que permiten cifrar el contenido de discos duros completos, carpetas o archivos individuales según las necesidades que se tengan.

Dado que la entidad maneja información de carácter confidencial que puede residir en cualquiera de estos dispositivos que se señalaron, se procedió a evaluar si se ha definido de manera oficial las herramientas de encriptación que pueden ser utilizadas y determinar si se ha capacitado a los funcionarios para que las usen y, además, verificar que se estén usando.

En relación con el tema, se consultó al jefe de la unidad de Tecnologías de Información[2] sobre si la institución mantiene contratos en relación con la integridad, el uso, la divulgación y modificación de la información, a lo cual respondió:

> *"No se mantienen contratos. No podemos hacer acuerdos de información de la cual no somos los dueños.".*

Si bien es cierto, la información que se genera en el ICD corresponde al accionar de todas las unidades que lo integran, no puede omitir la unidad de TI las medidas necesarias para proteger dicha información del uso y la divulgación en forma inadecuada.

Esta Auditoría no comparte técnicamente la afirmación anterior del jefe de la unidad evaluada, fundamentados en los siguientes criterios que corresponden al Manual de Normas Técnicas de Tecnologías de información.

[2] Acta No. AI-027-2019 del 11 de junio de 2019.

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."./

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 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.".

Por tanto, corresponde al jefe de Tecnologías de Información establecer mecanismos de protección y control que aseguren la autenticidad, integridad y confidencialidad de las transacciones y la transferencia o intercambio de datos, con el propósito de prevenir el uso indebido y la fuga de información que atente contra los propósitos y razón de ser institucional.

Es necesario que la jefatura de TI realice un estudio para valorar en conjunto con las jefaturas y la dirección general, que cantidad y cuáles funcionarios requieren utilizar puertos USB, dispositivos fijos o removibles para extraer información institucional producto de sus funciones, sin que ello implique efectos negativos para la institución.

2.4 En el tema de comunicación de la política de seguridad.

La implementación de lineamientos en materia de seguridad de la información demanda de un proceso de divulgación, sensibilización y concientización que permita a los funcionarios de la entidad que tengan acceso a información sensitiva conocer y entender para que el contenido del marco sea aplicado.

En consecuencia, con las oportunidades de mejora señaladas anteriormente, se determina que la institución no consideró las implicaciones que tiene la promulgación de lineamentos de esta naturaleza, situación que es afirmada por el jefe

de TI[3], al consultarle sobre los aspectos de mejora relativos a las normas de seguridad de la información en la institución, pues indica que “las políticas en cuanto a seguridad, deberían proveer y garantizar la capacidad de acceso, uso y desvío de la misma.

Además, agrega que la institución debería estar de acuerdo con el marco de seguridad o debería establecer su marco de seguridad considerando la criticidad[4] de la información. Aspectos relacionados con demanda de recursos para hacer replanteamientos de funciones, y que tiene efectos sobre crear puestos de trabajo, establecer perfiles de usuarios de la información, asumir tareas que están implícitas a la implementación del marco, formalizar acuerdos de confidencialidad con funcionarios y proveedores y supervisar que se cumplan.

Por ello es importante que los canales de comunicación que utilice la unidad de TI sean idóneos para que estén disponibles y en conocimiento oportuno de todos los funcionarios del ICD y de los usuarios de la información externos a la institución.

Cabe destacar que no se determinó que la administración por medio de la Dirección General y las TI mantenga oportunamente comunicada la política de seguridad creada por Informática, debido al desconocimiento general de dicha política, situación que debilita y pone en riesgo el manejo de la información por parte de todos los funcionarios y de aquellos usuarios externos a la institución.

Al respecto, la norma 5.7 “calidad de la comunicación del Manual de Normas Generales para el Sector Público establece:

> *“El Jerarca y los titulares subordinados, según sus competencias, deben establecer los procesos necesarios para asegurar razonablemente que la comunicación de la información se da a las instancias pertinentes y en el tiempo propicio, de acuerdo con las necesidades de los usuarios, según los asuntos que se encuentran y son necesarios en su esfera de acción. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.”.*

En concordancia, la norma 5.7.1 Canales y medios de comunicación indica:

[3] Acta No. 027-2019

[4] Es una metodología que permite jerarquizar sistemas, instalaciones y equipos, en función de su impacto global, con el fin de tomar decisiones.

"Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna, a los destinatarios idóneos dentro y fuera de la institución.".

Es conveniente que la administración activa por medio de la Dirección General y la jefatura de TI establezcan canales de comunicación asertiva, oportuna y comprensible para los funcionarios, con el propósito de aclarar los alcances y limitaciones que deben respetar los usuarios a la hora de acceder información pública y privada de la institución cumpliendo a cabalidad con la política de seguridad correspondiente.

3. CONCLUSIONES.

Se conoció el documento Normas de Seguridad de Datos, cuenta con una versión, que data del año 2012 y no constan las modificaciones y actualizaciones descritas por el jefe de TI en la entrevista ejecutada por esta unidad.

Se omite la etapa de implementación referida a las acciones ejecutadas por la administración para cumplir a cabalidad la política de seguridad de la información, por cuanto, no se plasma la gestión documental correspondiente a acciones relativas frecuencia de las tareas, tiempos, avances, porcentajes de cumplimiento, y los resultados concretos que puedan dilucidar el correcto desempeño de las responsabilidades asumidas por la unidad de Tecnología de Información relativas a la política.

La revisión de los procesos de gestión implementados por la entidad mediante la herramienta (SIGMA) mostró que se ha omitido la identificación y valoración de eventos de riesgo que amenacen la información que administra la institución. Se carece de métricas que permitan conocer si la entidad cuenta con un adecuado nivel de protección de sus datos contra posibles incidentes; y a la vez determinar si los controles implementados están resultando eficaces y se carece de registros de eventos materializados que afectaron información sensible de la entidad.

En relación con datos sensibles residentes en medios de almacenamiento, no se ha formalizado el uso de discos compactos, celulares, USB, memorias extraíbles tanto en el dominio público, así como en los dominios de cada unidad.

Además, no se ha considerado las implicaciones que tiene la promulgación de lineamientos relativos a Seguridad de la Información los cuales deben proveer y garantizar la capacidad de acceso, uso y desvío de la información.

4. RECOMENDACIONES.

Al JEFE DE TECNOLOGIAS DE INFORMACION.

1. Debe la unidad de Tecnologías de información establecer mediante indicadores de desempeño las medidas necesarias para concretar en la práctica todos los requisitos establecidos en su política de seguridad de la información, con el propósito de demostrar las acciones de implementación que dan cumplimiento a dicha política **(Ver punto 2.1 de este informe)**

2. Es prudente que el jefe de la unidad de TI administre de forma oportuna y correcta los riesgos asociados a las barreras de seguridad que actualmente mantiene la institución, los incorpore a la herramienta que corresponda, con el propósito de identificarlos, conocer la probabilidad, impacto, nivel y acciones para mitigarlos, asegurando la afinidad a los riesgos institucionales contemplados en el Sistema Específico de Valoración de Riesgos. **(Analícese punto 2.2 de este informe)**

3. Corresponde al jefe de Tecnologías de Información implementen mecanismos de protección y control que aseguren la autenticidad, integridad y confidencialidad de las transacciones y la transferencia o intercambio de datos, con el propósito de prevenir el uso indebido y la fuga de información mediante dispositivos USB, fijos o removibles. **(Refiérase al punto 2.3 de este informe)**

4. Es conveniente mantener canales de comunicación asertiva, oportuna y comprensible para con los funcionarios del ICD, con el propósito de aclarar los alcances y limitaciones que deben respetar los usuarios a la hora de acceder información pública y privada de la institución cumpliendo a cabalidad con la política de seguridad correspondiente. **(Ver punto 2.4 del presente informe)**

DEYANIRA BERMUDEZ CALDERON (FIRMA)

Firmado digitalmente por DEYANIRA BERMUDEZ CALDERON (FIRMA)
Fecha: 2019.09.03 14:44:36 -06'00'