AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

N°43-06-IAO-SATI-2021

11 de enero de 2021

Licenciado
Diego Chavarría García, Jefatura
Departamento de Investigaciones Criminales
Organismo de Investigación Judicial

Estimado señor:

De conformidad con lo dispuesto en el Artículo 36 de la Ley General de Control Interno, le remito informe final correspondiente al Estudio efectuado por la Sección Auditoría de Tecnología de Información el Despacho a mi cargo, denominado "***Evaluación de la Seguridad de la Información en la Sección Especializada contra el Cibercrimen****".*

El cual tuvo como objetivo evaluar si el tratamiento de la información en la Sección Especializada contra el Cibercrimen cumple con las características de confidencialidad, integridad y disponibilidad, de acuerdo con la normativa vigente y mejores prácticas.

No omito indicar que con la implementación de las recomendaciones emitidas se pretende minimizar el riesgo de que en el futuro se presenten las debilidades detectadas. Además, es relevante señalar que, de conformidad con lo establecido en la Ley General de Control Interno, esta Auditoría efectuará en su momento un seguimiento, para asegurarse de que las acciones establecidas por las instancias competentes se hayan implementado eficazmente y dentro de los plazos definidos en cada caso.

Finalmente, en caso de que este documento deba ser facilitado a partes externas del Poder Judicial, deberá preverse lo establecido en la Ley Nº 8968 "Protección de la Persona Frente al tratamiento de sus datos personales".

Atentamente,

Roy Díaz Chavarría
Subauditor Judicial

c: Consejo Superior
Sección Auditoría Tecnología de Información
Archivo (SATI-37-2020).-

AUDITORIA JUDICIAL

Informe de auditoría para el mejoramiento del control interno relativo a la seguridad de la Información en la Sección Especializada contra el Cibercrimen

Sección Auditoría de Tecnología de Información

Enero, 2021

AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

TABLA DE CONTENIDO

AUDITORÍA JUDICIAL
TELÉFONO: 2295-3238
FAX: 2257-05-85
E-MAIL: auditoria@poder-judicial.go.cr
APARTADO: 79-1003 SAN JOSE

RESUMEN EJECUTIVO

La Auditoría de Tecnología de Información realizó un estudio de fiscalización que tuvo como objetivo evaluar si el tratamiento de la información en la Sección Especializada contra el Cibercrimen cumple con las características de confidencialidad, integridad y disponibilidad, de acuerdo con la normativa vigente y mejores prácticas. La evaluación comprendió la situación encontrada durante la auditoría en los meses de octubre y noviembre del 2020, con fecha de corte al 1 de diciembre del 2020.

Se consideró lo indicado en el numeral 1.4.5 y 4.2 de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República, de acatamiento obligatorio para el Poder Judicial, que dispone que la organización debe proteger la información de accesos no autorizados, además de asegurar razonablemente la administración y operación de la plataforma tecnológica. Cabe señalar, que el estudio fue elaborado según ciclo definido por la Auditoría Judicial.

Durante la evaluación se identificó la necesidad de mejorar los controles que permitan evidenciar el cumplimiento del contrato de mantenimiento del cortafuegos por parte del proveedor, ejecutar monitoreos constantes del tipo de paquetes o posibles ataques que puede sufrir el dicho dispositivo, así como diseñar y aplicar un procedimiento que permita la revisión, actualización y control de la documentación, con el fin de estandarizar e implementar la mejora continua de los procesos, con el propósito de que no se presenten riesgos tales como:

- Riesgos Operativos: Atraso en los procesos, Información inaccesible e información incorrecta.
- Riesgos Reputacionales: Afectación a la imagen institucional.

Por lo anterior se giraron recomendaciones en línea a subsanar las debilidades encontradas.

Evaluación de la Seguridad de la Información en la Sección Especializada contra el Cibercrimen

1. INTRODUCCIÓN

1.1 Trámite de los informes de auditoría según la Ley General de Control Interno

El artículo 36 de la Ley General de Control Interno, establece el tratamiento que los titulares subordinados encargados de las áreas evaluadas, deben dar a los informes de fiscalización que emite la Auditoría Interna, el cual incluye, la orden de implementación de las recomendaciones vertidas en el informe o el planteamiento de discrepancia ante el Jerarca, en el plazo de diez días hábiles a partir de la fecha de recibido el documento.

A su vez, el artículo 39 de la citada Ley advierte de la responsabilidad administrativa o civil que puede acarrear sobre los responsables, la inobservancia de las recomendaciones emitidas por la Auditoría Interna.

1.2 Origen del estudio

Estudio no programado realizado de conformidad con las competencias que son atinentes a esta Auditoría, señalado en el artículo 22 de la Ley General de Control Interno.

1.3 Objetivo general

Evaluar si el tratamiento de la información en la Sección Especializada contra el Cibercrimen cumple con las características de confidencialidad, integridad y disponibilidad, de acuerdo con la normativa vigente y mejores prácticas.

1.4 Alcance y naturaleza

La naturaleza es operativa y comprendió el análisis del resguardo y tratamiento de la información que es tratada como evidencia en las investigaciones judiciales.

Se realizó un análisis de la gestión de las directrices y documentación de los procedimientos de la Sección Especializada contra el Cibercrimen (SEC2), con el fin de verificar la facilidad de acceso y su aplicación.

Además, se analizó la gestión y funcionamiento del cortafuegos utilizado en la separación de las tres redes de dicha Sección, con el fin de verificar su actualización y mantenimiento razonable y seguro.

Finalmente, se analizó el procedimiento del manejo de la evidencia del momento en que llega a la SEC2 y que se entrega a la Fiscalía, con el fin de verificar la segregación y calidad de la información entregada.

La evaluación consideró la situación encontrada durante la auditoría, en los meses de octubre y noviembre del 2020, con fecha de corte al 1 de diciembre del 2020.

1.5 Equipo de trabajo

El estudio fue desarrollado por el profesional Javier Alfaro Valerio, bajo la supervisión de Alicia Sancho Brenes, jefatura de la Sección de Auditoría de Tecnología de Información.

1.6 Normativa técnica aplicada

Para la ejecución de este estudio se observaron las Normas para el Ejercicio de la Auditoría Interna en el Sector Público y las Normas Generales de Auditoría para el Sector Público, ambas promulgadas por la Contraloría General de la República.

1.7 Difusión verbal de los resultados

Este estudio fue puesto en conocimiento del área auditada mediante informe en borrador N° 1473-126-IAO-SATI-2020 del 1 de diciembre de 2020 y conferencia final efectuada el 17 de diciembre de 2020 en la cual participaron, de parte de la Departamento de Investigaciones Criminales del OIJ:

- Diego Chavarría García, Jefatura Departamento de Investigaciones Criminales
- Erick Lewis Hernández, Jefatura Sección Especializada Contra el Ciber Crimen
- Joaquín Morales González, Profesional Sección Especializada Contra el Ciber Crimen
- Federico Vásquez Campos, Profesional Sección Especializada Contra el Ciber Crimen

De parte de la Auditoría:

- Alicia Sancho Brenes, Jefatura de la Auditoría de Tecnología de Información
- Javier Alfaro Valerio, Profesional a cargo de la evaluación

La discusión de los resultados de auditoría tratados durante esta etapa permitió considerar las observaciones expuestas por las áreas auditadas y responsables de la implementación de las mejoras propuestas, las cuales se consideraron en el presente informe.

3. RESULTADOS DEL ESTUDIO

Como producto de la auditoría concluida, se identifican los aspectos que se detallan a continuación:

2.1 Necesidad de fortalecer la gestión de la seguridad del cortafuegos

La Sección Especializada contra el Cibercrimen (SEC2), carece de controles apropiados que le permitan garantizar razonablemente que el cortafuego se encuentra en condiciones óptimas para minimizar los riesgos de ataques electrónicos desde Internet.

El cortafuego es un dispositivo de seguridad utilizado para minimizar los ataques contra los computadores ubicados dentro de la red del Poder Judicial. Dicha Sección lo utiliza para aislar de forma lógica las tres redes que posee, las cuales son:

- De investigación: con línea independiente y de libre acceso a Internet.
- Forense: solo de uso local.
- Institucional: con restricción a Internet, acceso a equipos y sistemas del Poder Judicial.

Adicionalmente, se cuenta con un contrato de mantenimiento para este artefacto con la empresa SEFISA que incluye: Soporte técnico mediante la modalidad de 24 horas, 7 días y 365 días por 3 años. Corresponde a la atención de fallas en el equipo y actualización de software.

Pese al contrato, esta Auditoría no tuvo acceso a información que permitiera evidenciar que la empresa ejecuta las actualizaciones del sistema operativo oportunamente.

Otro control relevante de la seguridad del equipo es realizar monitoreos constantes del tipo de paquetes o posibles ataques que puede sufrir la pared de fuego. En este caso particular, la Dirección de Tecnología de Información (DTI) lo ejecuta por ser parte del esquema institucional de seguridad, sin que esta actividad y su comunicación con la SEC2 se haya oficializado.

Sobre este tema, las Normas técnicas para la gestión y el control de las Tecnologías de Información **(N-2-2007-CO-DFOE)** de la Contraloría General de la República, de junio 2007 y acatamiento obligatorio para el Poder Judicial, establecen:

> ***1.4.5 Control de acceso***
>
> *La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:*
> *[…]*
> *c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.*
>
> ***4.2 Administración y operación de la plataforma tecnológica***
>
> *La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
> *b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
> *c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*

Los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT) en su versión 5, apartado DSS05 Gestionar Servicios de Seguridad, manifiestan:

> *DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.*
> *Usando herramientas de detección de intrusos, supervisar la infraestructura para detectar accesos no autorizados y asegurar que cualquier evento esté integrado con la supervisión general de eventos y la gestión de incidentes.*

La carencia de los controles antes mencionados obedece a las siguientes razones:

1. A pesar de que la SEC2 posee personal especialista en informática, no tiene como función ni la experticia en el análisis y mantenimiento de un dispositivo de seguridad.

   Si bien la DTI custodia el funcionamiento de este tipo de equipos que se encuentran bajo su responsabilidad, el cortafuego de la SEC2 es de uso exclusivo del OIJ e independiente de la DTI.

2. Debido a que el equipo está en garantía y hay un contrato de mantenimiento, los encargados confían en que el proveedor del producto procede, en caso de que se presenten actualizaciones, por lo que no se ha visto necesario evidenciar esta actividad.

Las causas antes mencionadas pueden provocar situaciones adversas tales como:

Al carecerse de evidencia sobre el cumplimiento del contrato de mantenimiento de la pared de fuego por parte del proveedor, se dificulta garantizar dicha responsabilidad y su reporte al Departamento de Proveeduría en caso de incumplimiento, aumentando la probabilidad que se presenten los riegos que se buscaron evitar con el pago del contrato.

La carencia de un procedimiento de monitoreo del cortafuego puede presentar riegos, tales como intentos de hackeo[1] o ataques de denegación de servicio y la SEC2 no estaría enterada de la situación o podría reaccionar de forma letárgica, facilitando la ocurrencia de escenarios negativos para la seguridad informática.

Lo anterior aumenta la probabilidad de que se presenten:

- Riesgos Operativos: Atraso en los procesos e Información inaccesible.
- Riesgos Reputacionales: Afectación a la imagen institucional.

2.1 Importancia de actualizar la documentación de los procesos de la Sección Especializada contra el CiberCrimen

La SEC2 cuenta con diferentes procedimientos documentados para realizar funciones específicas, sin embargo, se identificó que algunos de ellos se hallan desactualizados y otros se encuentran en procedo de documentación.

[1] Hackeo: Ingresos no autorizados a la infraestructura de la organización.

Tal es el caso del “Manual de Procedimientos Generales de la SDI”, que fue creado en el 2007 y no reporta actualizaciones posteriores. El manual indica: “Procedimiento para las verificaciones previas a la creación de la imagen de un Disco Duro”, el cual describe lo que se debe hacer con los computadores portátiles más conocidas de la época, sin embargo, no se consideran equipos Apple, los cuales han crecido en popularidad o la utilización actual de sistemas operativos diferentes al Windows, por ejemplo: Linux y sus derivaciones, Chrome, etc.

Adicionalmente, la jefatura de la Sección bajo estudio manifestó que al finalizar este año se esperan concluir los procedimientos para:

- Abrir, visualizar y analizar la información contenida en un reporte en formato UFDR
- Apertura y respaldo de información de indicios informáticos
- Generar Hash con FTK IMAGER

Al respecto, las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), de la Contraloría General de la República instituyen:

> ***1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI***
>
> *La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.*
>
> *En el cumplimiento de esa responsabilidad las autoridades citadas deben dar especial énfasis a áreas consideradas relevantes con base en criterios tales como su materialidad, el riesgo asociado y su impacto en la consecución de los fines institucionales, incluyendo lo relativo a la desconcentración de competencias y la contratación de servicios de apoyo. Como parte de ello, deben contemplar, entre otros asuntos, los siguientes:*
>
> *[…] c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta.*

Sobre este tema, las Normas técnicas para la gestión y el control de las Tecnologías de Información **(N-2-2007-CO-DFOE)** de la Contraloría General de la República, de junio 2007 y acatamiento obligatorio para el Poder Judicial, establecen:

> ***4.2 Administración y operación de la plataforma tecnológica***
>
> *La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*

Entre las razones por las cuales se presenta la situación de comentario, se encuentran las siguientes:

1. La herramienta principal utilizada para los estudios forenses de los datos decomisados tiene operaciones bien definidas por la empresa fabricante del programa forense, por lo que no se ve la necesidad de actualizar los procedimientos existentes relacionados con las técnicas antes y después del uso del instrumento.

2. Los auditados manifestaron que se cuenta con manuales de casos específicos e inducciones con personal de experiencia que permite guiar a los nuevos funcionarios en los procesos de la SEC2.

La ausencia de documentación escrita y actualizada dificulta la mejora continua de los métodos e incrementa la posibilidad de errores.

La falta de estandarización de las técnicas puede crear confusión, reducir la eficiencia y calidad de los productos finales, aumentando la probabilidad de que se presenten riesgos operativos como: Atraso en los procesos e información incorrecta.

4. CONCLUSIONES DEL ESTUDIO

De la evaluación desarrollada se puede concluir que la Sección Especializada contra el Cibercrimen cumplen con las características de confidencialidad, integridad y disponibilidad, con respecto a la información que gestiona, sin embargo, se identifican debilidades relacionadas con la gestión de la documentación, el mantenimiento y monitoreo del cortafuego.

5. RECOMENDACIONES DEL ESTUDIO

A la Jefatura de la Sección contra el Cibercrimen

5.1. Establecer y oficializar los mecanismos que permitan evidenciar el cumplimiento oportuno del contrato por parte del proveedor en lo relacionado con las actualizaciones, con el propósito de garantizar razonablemente la seguridad del dispositivo.

Plazo sugerido de implementación: inmediato

5.2. Establecer un procedimiento de monitoreo del cortafuego, de tal forma que se visualice su actividad y se minimicen los riegos de seguridad del equipo.

Plazo sugerido de implementación: inmediato

5.3. Diseñar y aplicar un procedimiento que permita la revisión, actualización y control de la documentación, con el fin de estandarizar e implementar la mejora continua de los procesos.

Plazo sugerido de implementación: 6 meses