CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: auditoria_interna@ccss.sa.cr

AS-AATIC-190-2022
3 de octubre de 2022

Ingeniero
Esteban Zúñiga Chacón, jefe
Centro de Gestión Informática
GERENCIA MÉDICA – 2901

Ingeniero
Alexánder Solís Abarca, jefe
Centro de Gestión Informática
GERENCIA FINANCIERA – 1103

Ingeniera
Guiselle Tenorio Chacón, jefe
Centro de Gestión Informática
GERENCIA ADMINISTRATIVA – 1104

Ingeniero
Roy Ovares Valerio, jefe
Centro de Gestión Informática
GERENCIA LOGÍSTICA – 1106

Ingeniero
Giovanni Campos Alvarado, jefe
Centro de Gestión Informática
GERENCIA INFRAESTRUCTURA Y TECNOLOGÍAS – 1107

Ingeniero
Marco Vinicio Jiménez, jefe
Centro de Gestión Informática
GERENCIA PENSIONES – 9108

Máster
Idannia Mata Serrano, subgerente a.i.
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – 1150

Estimados (a) señores (a):

ASUNTO:	**Oficio de Asesoría sobre las capacidades asociadas con la gestión de incidentes de ciberseguridad.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022 y con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y siendo consecuente a lo indicado en el oficio AI-874-2022 del 6 de junio del 2022, en el cual se comunicó el inicio de la evaluación concerniente al ataque cibernético perpetrado en la CCSS, esta Auditoría asesora a esa Administración sobre el tema citado en el epígrafe.

1- GENERALIDADES y ANTECEDENTES

Cada vez más instituciones se organizan para contrarrestar la probabilidad de fallos de seguridad, los cuales puedan atentar contra la continuidad en la prestación de servicios.

Lo anterior, en aras de evitar o disminuir el impacto de la materialización de riesgos tecnológicos vinculados con ciberataques, fraude, extracción de datos, acceso no autorizado, destrucción o corrupción de la información y demás amenazas.

En ese sentido, su accionar es conducido hacia la implementación de mejoras continuas en materia de la seguridad de la información y ciberseguridad; lo cual implica eventualmente un aumento en inversión para establecer estructuras capaces de prever comportamientos de la industria, gestionar riesgos e incidentes de origen tecnológico, entre otras acciones defensivas y de monitorización constante.

En lo que respecta a inversión, la nota "7 de cada 10 empresas costarricenses invierte en ciberseguridad" publicada el 23 de mayo del 2022 por la Promotora de Comercio Exterior de Costa Rica (PROCOMER), cita:

> *"Entre la muestra analizada, siete de cada diez empresas costarricenses (73%) ha invertido o invierte actualmente en ciberseguridad, mientras que las restantes no lo han hecho nunca.*
>
> *Así quedó evidenciado en el estudio "Caracterización del uso y necesidades potenciales de ciberseguridad en empresas costarricenses", elaborado por PROCOMER, el cual perfiló también a la oferta costarricense de ciberseguridad en términos de servicios y especialización.*
>
> *Erick Apuy, analista económico a cargo del estudio, destacó que existe una población crítica de empresas, el 8% de la muestra, que a pesar de que nunca ha gastado en ciberseguridad tampoco contempla hacerlo en el corto plazo, es decir, resultan los más vulnerables y expuestos ante amenazas de seguridad.*
>
> *Para Costa Rica, son los virus, phishing y malware las infecciones más comunes, atacando en promedio a cerca de 6 de cada 10 empresas. No obstante, es el Ransomware, que ha afectado al 37% de empresas, el que señalan como su mayor amenaza; algo previsible al considerar que es uno de los ataques de mayor crecimiento en el mundo. En total, el 89% de las empresas analizadas ha estado expuesta a ciberdelincuencia.*
>
> *Para las empresas que invierten en ciberseguridad, entre las soluciones más utilizadas destacan programas habituales e imprescindibles para la seguridad cotidiana, como antivirus (91% de empresas), firewall (87%); antimalware (85%) y VPNs (81%). "Otras plataformas más exhaustivas y especializadas tienen poca participación, por ejemplo, el XDR (23%), Zero Trust (17%) o SASE (15%); sistemas hacia los que las empresas deberían de orientarse cada vez más, así como también hacia la gobernanza de la ciberseguridad", dice el analista."*

En ese sentido, la noticia detalla la inversión en términos de soluciones tecnológicas, pero también indica aspectos sobre el establecimiento de estructuras, competentes para robustecer la capacidad de la organización, atender las necesidades del negocio y consecuentemente brindar la gestión de incidentes[1] que corresponde.

A ese respecto, en el oficio GG-DTIC-3629-2022 de 17 de julio del 2022 se indica el direccionamiento de la CCSS en materia de gestionar incidentes de ciberseguridad, citando:

> *"En cuanto a la implementación del Centro de Operaciones de Seguridad (SOC) en la CCSS se recuerda que el mismo es parte de las iniciativas de ciberseguridad (PCS-GI-15) y que para dicho objetivo se gestiona un proceso de contratación administrativa, para el cual, la documentación está para entrar a revisión el 17 de julio según cronograma del cuadro de mandos de compras 2022 de la DTIC.*
>
> *Servicios para la gestión del Centro de Operaciones de Seguridad SOC: compra que sustituirá los servicios tercerizados de ciberseguridad actualmente con el contrato 005-2018 con Deloitte & Touché, y se agregan nuevos servicios con los que no se cuenta con el contrato actual.*
>
> *Sobre su estado actual, el mismo se encuentra en fase de estudio de mercado, y se espera presentar documentación a la Subárea Gestión Administrativa DTIC para revisión de la documentación y envío a la Gerencia General para autorización de uso de la partida 2149 servicios profesionales de ciberseguridad."*

1.1 Términos y definiciones

En lo que atañe a incidentes de ciberseguridad, resulta conveniente comprender el conjunto de términos y definiciones asociadas a esta temática, detallados a continuación:

Incidente de seguridad: en informática, es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad o disponibilidad de los datos y ciertamente violan la política de seguridad de la Información.

A partir de ello, la ***gestión de incidentes*** se define como la capacidad para administrar eficazmente sucesos o hechos (mediante la detección, registro y gestión de las amenazas), no previstos o lejanos a la operativa normal; con el objetivo de minimizar el impacto de estos.

Asimismo, su finalidad es mantener y restaurar las actividades y operaciones normales TIC dentro del límite de tiempo establecido, lo cual minimiza el costo que puede tener un incidente de cualquier naturaleza sobre la organización.

A partir de ello, la gestión de incidentes puede darse en los siguientes términos:

Tratamiento del incidente: es un servicio que involucra todos los procesos relacionados con la respuesta ante eventos adversos e implica múltiples funciones como la detección y reporte; priorización de emergencias; análisis; y atención a incidentes.

[1] La gestión de incidentes es una serie de pasos que se toman para identificar, analizar y resolver incidentes críticos que podrían provocar problemas en una organización si no se solucionan.

Gestión eficaz de incidentes incluye procesos de soporte inicial que permiten validar nuevos eventos a partir de errores y problemas conocidos con anterioridad, siendo posible identificar cualquier solución alternativa. Además, este tipo de labores suele incluir otras funciones como, por ejemplo, la gestión de vulnerabilidades y cursos de concientización sobre la seguridad, asimismo, hace hincapié en lo que respecta a la prevención.

Respuesta a incidentes es el último paso en el proceso de tratamiento, abarcando la planificación coordinación y ejecución de cualquiera de las estrategias y acciones de mitigación y recuperación.

En virtud de lo anterior, el proceso de gestión y respuesta a incidentes tiene como motivación, formar parte de los planes de ***continuidad del negocio*** (BCP, por sus siglas en inglés), al igual que la recuperación en caso de situación de desastre.

Es decir, su objetivo principal y mancomunado es impedir razonablemente la existencia de problemas y en el caso de materializarse, evitar que los mismos se transformen en desastres.

En aras de apoyar la definición conceptual de la continuidad del negocio y los planes que lo conforman (entre ellos, el Plan de Gestión de Incidentes), en la siguiente imagen se observa el entono integral acompañado del componente antes mencionado.

Imagen No.1
Planes considerados en el BCP

Fuente: Proveedor tecnológico de seguridad ESET, articulo "¿En qué consiste un Plan de Recuperación ante Desastres (DRP)?" del 14 de octubre del 2014

1.2 Productos de Auditoría

En línea con lo anterior, la Auditoría Interna se ha referido a la visión general que abarca el tema de marras, específicamente al emitir criterios sobre la seguridad de la información, ciberseguridad y continuidad de negocio; los cuales fueron oficializados mediante los siguientes productos:

Cuadro No.1
Productos emitidos Auditoría Interna sobre ciberseguridad 2020-2022

Informe / Oficio No.	Fecha	Asunto
Oficio AD-ATIC-271-2020	5 de febrero del 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
Oficio 292	15 de febrero del 2019	Aspectos relacionados con seguridad de la información. (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema)
Oficio AD-ATIC-706-2020	16 de marzo del 2020	Continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 22 de octubre del 2019
AD-ATIC-1512-2020	29 junio del 2020	Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio.
AS-ASTIC-1849-2020	23 de julio del 2022	Oficio de asesoría respecto a la seguridad cibernética (ciberseguridad) ante la pandemia producida por el COVID-19.
AS-ATIC-674-2021	24 de marzo de 2021	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2021 y preparación tecnológica de la CCSS
AD-ATIC-1806-2021	26 de agosto del 2021	Oficio de Advertencia referente a evento presentado respecto de la visualización de imágenes médicas en el Hospital Nacional de Niños.
AD-ATIC-1930-2021	9 de setiembre del 2021	Oficio de Asesoría referente a la Gobernanza de Tecnologías de Información y Comunicaciones (TIC) y Seguridad de la Información en la Caja Costarricense de Seguro Social.
AS-ATIC-2313-2021	1 de noviembre del 2021	Oficio de Asesoría referente a mecanismos de control en TIC para garantizar continuidad de los servicios de salud apoyados mediante imágenes médicas.
AS- ATIC-052-2022	8 de abril del 2022	Oficio de Asesoría que refiere a las tendencias de mercado TIC para el 2022 y preparación tecnológica de la CCSS
AD-ATIC-038-2022	21 de abril del 2022	Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo de 2022.
AD-ATIC-039-2022	21 de abril del 2022	Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS.
AD-ATIC-046-2022	3 de mayo del 2022	Oficio de Advertencia referente a la priorización de la ciberseguridad en la Caja Costarricense del Seguro Social.
AD-ATIC-067-2022	31 de mayo del 2022	Oficio de Advertencia sobre la exposición reciente a ataques cibernéticos a la CCSS.
AS-AATIC-072-2022	10 de junio del 2022	Oficio de asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022.
AS-AATIC-063-2022	1 de julio del 2022	Oficio de Advertencia sobre gobierno y gestión de la ciberseguridad en la CCSS.
AI-905-2022	13 de junio del 2022	Oficio de información en relación con acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta “Mimikatz”.
AS-AATIC-088-2022	16 de junio del 2022	Oficio de asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico.
AS-AATIC-089-2022	21 de junio del 2022	Oficio de Asesoría en relación con acciones preventivas para minimizar la materialización de riesgos generados por eventuales debilidades en el Active Directory y servidores Exchange que permita la ejecución del ransomware “BlackCat”.
AS-AATIC-108-2022	22 de junio del 2022	Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico.
AS-AATIC-113-2022	27 de junio del 2022	Oficio de asesoría sobre el restablecimiento en la operación de sistemas de información y bases de datos.
AS-AATIC-122-2022	30 de junio del 2022	Oficio asesoría referente a las acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta “Log4J”.
AS-AATIC-116-2022	7 de julio del 2022	Oficio de Asesoría referente a los planes de continuidad de TIC.
AI-1043-2022	7 de julio del 2022	Oficio de Información relacionado con el riesgo de Ransomware detectado en la plataforma de Microsoft 365.
AS-AATIC-127-2022	4 de julio del 2022	Oficio de Asesoría sobre la actualización del software y la infraestructura en TIC.

Informe / Oficio No.	Fecha	Asunto
AS-AATIC-135-2022	11 de julio del 2022	Oficio de Asesoría sobre el impacto en la prestación de servicios y medidas de contingencia, producto del ataque cibernético en la plataforma tecnológica institucional.
AS-AATIC-147-2022	19 de julio del 2022	Oficio de Asesoría sobre los roles y responsabilidades de ciberseguridad a considerar en la Caja Costarricense del Seguro Social.
AS-AATIC-155-2022	19 de julio del 2022	Oficio de Asesoría relacionado con amenazas generadas por el Ransomware DeadBolt que afecta los almacenamientos en dispositivos NAS.
AI-1151-2022	3 de agosto del 2022	Oficio de información relacionado con amenazas generadas a los servidores virtuales por el Ransomware Red Alert.
AS-AATIC-168-2022	17 de agosto del 2022	Oficio de Asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento.

Fuente: Elaboración propia, Auditoría Interna

2- OBSERVACIONES

En atención al asunto mencionado en el epígrafe, esta Auditoría se refiere a la gestión y respuesta de incidentes cibernéticos, con el propósito de que las observaciones detalladas puedan ser valoradas al afrontar los eventos con rapidez y eficacia; se incentive el desarrollo de capacidades y estructuras en la organización; y se tenga un buen entendimiento tanto conceptual como práctico de la temática.

- Es conocido que los eventos pueden interrumpir las operaciones y provocar una situación de inactividad temporal en un proceso e inclusive contribuir a la pérdida de datos o productividad. Por ello, cada vez resulta de mayor importancia que las organizaciones implementen prácticas de gestión de incidentes, ante el crecimiento de exposición al riesgo de ciberataques.

  Tal y como lo menciona la compañía de software especializada en ciberseguridad ESET, en la publicación “Importancia de la gestión de incidentes para la seguridad de la información” compartida el 7 de enero del 2013, al citar:

  “La gestión de los incidentes de seguridad es un aspecto muy importante para lograr el mejoramiento continuo de la seguridad de la información de cualquier compañía, el principal inconveniente es que muchas organizaciones no lo utilizan adecuadamente.

  A pesar de que la norma ISO 27001, hace mención de este tema como uno de los dominios fundamentales, se les presta más importancia a temas de índole tecnológico dejando de lado los temas de gestión. En la búsqueda del mejor estándar para gestionar la seguridad de la información en una compañía, es vital tener presente que la revisión y la mejora continua del sistema son muy importantes para garantizar la disponibilidad, integridad y confidencialidad de la información.

  Cuando se habla de la gestión de incidentes, la norma hace referencia a recomendaciones relacionadas con la notificación de eventos y puntos débiles de seguridad de la información y los procedimientos y responsabilidades que se deberían asignar para la gestión de incidentes y mejoras de seguridad de la información.”

En cuanto a ese asunto, la página web “abogados.com.ar” en su publicación “Ciberseguridad: Prevención y gestión de incidentes” emitida el 3 de febrero del 2022, refiriéndose a la generalidad del tema y exponiendo un caso concreto de cibercrimen, citando:

> *“Ahora bien, la pregunta que pocas veces nos hacemos es si estamos preparados para ello y si entendemos que la contracara de mayor conectividad es mayor vulnerabilidad.*
>
> *Y lo más probable es que la respuesta sea sí, pero parcialmente. No obstante, generalmente ignoramos el "parcialmente" y nos quedamos con el sí. Ello porque Internet nos parece inocuo o, al menos, sus ventajas nos hacen pensar (falsamente) que los posibles riesgos y el impacto son insignificantes o que no los sufriremos nosotros. Lo peligroso es que entonces ignoramos aquello a lo que estamos expuestos y sus posibles consecuencias.*
>
> *De esta combinación de (i) hiperconectividad, (ii) mayor inversión del tiempo en Internet (y no en el mundo tangible), y (iii) la ignorancia -al menos parcial- de las amenazas virtuales, es que surge el aumento de incidentes de seguridad. El mundo virtual es cada vez más atractivo y el foco de atención para perpetuar ataques.*
>
> *El Sector Público Nacional no ha quedado exento del impacto de la tecnología en el desenvolvimiento de la actividad de las entidades y jurisdicciones que lo componen, tanto en lo que se refiere a la gestión interna como a los servicios que prestan a la sociedad.*
>
> *Como consecuencia del incremento sustancial en el uso de las TIC en dicho ámbito, el Sector Público también se ha vuelto blanco de ataque para los cibercriminales. Así, sobre todo el final del año 2021 y el comienzo del 2022 han traído numerosos ejemplos de incidentes de seguridad. Entre ellos, destacamos el acaecido en el ámbito del Registro Nacional de las Personas ("RENAPER"), el secuestro del sistema del Poder Judicial del Chaco (a través de un ransomware) y el del Senado de la Nación.”*

Así las cosas, los incidentes deben gestionarse para asegurar que se resuelvan en tiempo y forma, cumpliendo con las expectativas del cliente y los usuarios finales; respetando los acuerdos de servicio e implementando prácticas especializadas en la administración de incidentes; aspectos que sin lugar a duda deben pasar por un ciclo de mejora continua en aras de garantizar que las causas, los tratamientos y la solución de dichos eventos sirvan para la implementación de acciones correctivas y preventivas oportunas en casos similares que pudieran presentarse en un futuro.

- Al preguntarse los encargados de la seguridad de la información y ciberseguridad de una organización (tanto para involucrados del negocio como en la parte técnica), cuáles son los pasos para gestionar incidentes, pueden encontrar diferentes referencias a marcos metodológicos que apoyan esa consulta y son aplicables a la mayoría de instituciones, sin importar su fin o madurez en el proceso.

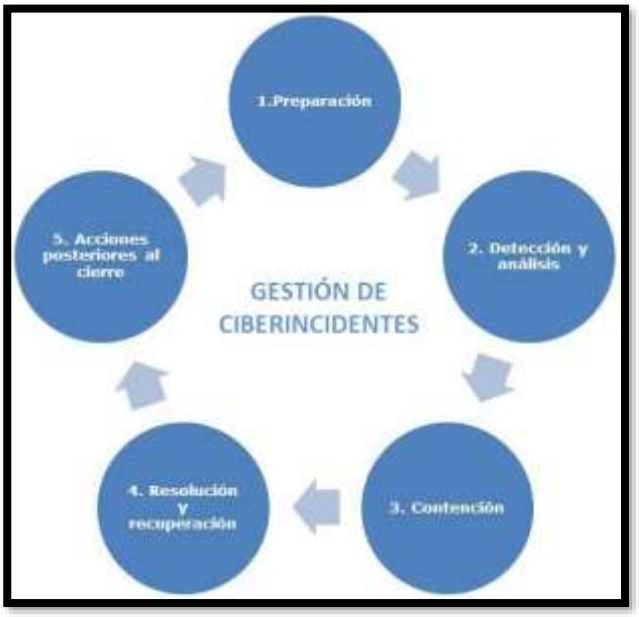
En cualquier caso, la documentación contenida en el Marco de Ciberseguridad NIST, Norma internacional ISO 27001[2], ISO 27035[3], ITIL[4] y otros estándares para la seguridad de la información, reafirman la necesidad vigente de las TIC por implementar una gestión oportuna de incidentes, involucrando diferentes etapas con las particularidades del proceso y los requerimientos considerados en su diseño.

Particularmente, un ciclo básico para gestionar incidentes estaría compuesto por cuatro o más etapas (según el diseño funcional y adopción de prácticas), orientado a:

- Preparación o registro, donde se da el establecimiento de capacidad de respuesta a incidentes.
- Detección (notificación) y análisis (escalamiento), enfocándose en la identificación de signos indicadores (reactivo) y precursores (preventivo), así como el análisis del nivel de riesgo, priorización, cumplimiento de SLA, entre otros datos relacionados.
- Contención resolución y recuperación, etapa donde se da la eliminación de componentes relacionados al incidente y consecuentemente, las actividades de recuperación. En ese sentido, se puede granular esa última tarea en la clasificación, priorización, investigación y diagnóstico del evento.
- Acciones posteriores al cierre: especializándose en el análisis de impacto y estudio de posibles mejoras.

El cual es representado gráficamente, de la siguiente forma:

Imagen No.2
Gestión de Ciber incidentes



Fuente: elaboración propia, Auditoría Interna.

[2] ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información.
[3] La Norma Internacional ISO / IEC 27035:2011 de gestión de incidentes de seguridad de la información.
[4] La Biblioteca de Infraestructura de Tecnologías de Información (o ITIL, por sus siglas en inglés)

Es decir, de gestionarse los incidentes (de índole tecnológica y aplicable a cualquier ámbito de resolución: central, regional, local) la CCSS podría mapear cuales serían las actividades macros a realizar en cada caso; tomando como guía la imagen anterior, en la cual se especifican, los procedimientos (mínimos o esenciales) para afrontar un ciberataque y/o gestionar de manera adecuada los incidentes de diferente índole.

- Previo a la definición de un enfoque orientado a gestionar incidentes se recomienda por parte de los expertos, identificar las capacidades o estructuras que apoyarán a esos objetivos y metas; por ejemplo, la administración de recursos y/o activos institucionales.

  En lo que respecta a activos, no se debe olvidar que la información es uno de ellos. De esa forma, se ha de identificar cuáles son los datos más críticos y el costo de estos; cuáles son las vulnerabilidades que pueden afectar a la Institución desde el ámbito técnico y del negocio.

  Tal y como se ejemplifica en el blog del Instituto Nacional de Ciberseguridad de España, a través de la publicación del 29 de diciembre del 2016, titulada “Inventario de activos y gestión de la seguridad en SCI”, refiriéndose al Sistema de Gestión de la Información y coincidiendo con el objetivo de identificar el valor de los activos y el impacto de ejercer la labor asociada con la mitigación del riesgo en la gestión de incidentes, citando:

  “El inventario de activos conforma el primer elemento de la cadena en un sistema de gestión de la seguridad de un sistema. Un inventario de activos se define como una lista de todos aquellos recursos (físicos, software, documentos, servicios, personas, instalaciones, etc.) que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

  Para proteger adecuadamente los sistemas de control industrial, las organizaciones ya no pueden confiar estrictamente en enfoques tradicionales basados en TI o el sistema físico para la gestión de activos de ciberseguridad. Las amenazas evolucionan continuamente y los ataques a infraestructuras críticas y sistemas de control industrial son cada vez más sofisticados y frecuentes.

  Es habitual encontrar un inventario de activos incompleto o inexistente en entornos de sistemas de control, lo que constituye uno de los grandes inconvenientes a la hora de abordar otras mejoras de la seguridad de estos sistemas. No se puede proteger lo que no se conoce, por eso es muy importante disponer de un inventario de activos convenientemente actualizado y revisado. (…)

  Para facilitar el manejo y mantenimiento del inventario, es conveniente clasificar los activos por categorías, según su naturaleza:

  Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen. Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.).

  Aplicaciones: El software que se utiliza para la gestión del proceso. Sistemas SCADA, herramientas de desarrollo de HMI, aplicativos desarrollados, sistemas operativos, firmware de dispositivos, etc.

Hardware industrial: Equipos físicos necesarios para desarrollar la labor industrial (terminales remotas, PLC, IED, PC, servidores, dispositivos móviles o de mano, etc.).

Red: Dispositivos de conectividad de redes (routers, switches, concentradores, pasarelas, etc.)

Tecnología: Otros equipos necesarios para gestionar las personas y el negocio de la empresa (servidores, equipos de usuario, teléfonos, impresoras, routers, cableado, etc.).

Personal: En esta categoría se encuentra tanto la plantilla propia de la organización como el personal subcontratado, personal de mantenimiento y, en general, todos aquellos que tengan acceso de una manera u otra a la industria.

Instalaciones: Lugares en los que se alojan los sistemas relevantes del sistema (oficinas, edificios, instalaciones eléctricas, vehículos, etc.).

Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, SAI, etc.).”

En ese orden de ideas, para asegurar el aporte de valor en la gestión de incidentes, este tipo de labores orientadas a proveer inventarios y análisis de la información, proporcionan una visión precisa del entorno e indirectamente fortalecen los procesos que así lo requieran.

- En lo referente al servicio tecnológico que soporta el proceso citado en el asunto de esta misiva, existe un componente funcional que se encuentra ligado a equipos y flujos de trabajo, los cuales deben tener la capacidad de abordar los incidentes.

  Lo anterior, basándose en la correlación de tareas a realizar, algunos ejemplos son:

  - Inteligencia de amenazas: proporciona un enfoque integral para investigar, analizar, monitorear y validar las notificaciones de amenazas, así como los riesgos de explotación relacionados con ellas.

  - Gestión de Eventos e Información de Seguridad (comúnmente conocido como SIEM por sus siglas en inglés), integra y centraliza el monitoreo de la red, accede a los registros de auditoría de los sistemas de información para crear reglas de reciprocidad, con el fin de emitir alertas, entre otras acciones asociadas con incidentes y amenazas.

  - Monitoreo y Clasificación: permite determinar si se ha producido un incidente de seguridad y, de ser así, identificar el tipo, alcance y magnitud del problema.

  - Este proceso es muy importante, debido a que los incidentes de seguridad se originan a través de un gran número de fuentes y en cualquier momento; por ello, el servicio se suele brindar de forma continua bajo modalidades 24/7.

- Respuesta a incidentes: de manera sistemática dirige las medidas de seguridad apropiadas para ayudar a minimizar la pérdida o el robo de información, así como la interrupción de los servicios, esto para reducir considerablemente el impacto comercial de un evento en ciberseguridad.

- Detección de amenazas, consiste en realizar búsquedas de forma proactiva e interactiva en el entorno tecnológico de una organización para detectar y aislar eventos de seguridad existentes que han evadido las medidas de ciberseguridad implantadas.

- Análisis forense, actividad asociada a la recopilación, preservación y análisis de información contenida en el equipo para descubrir el origen de un delito. Este puede ser tanto un ataque informático, un virus, una intrusión e incluso ser necesario para dar apoyo a una investigación policial o a instancias mayores.

- Los equipos especializados de abordaje (por ejemplo: Purple Team), efectúa estudios con los resultados de pruebas de penetración, análisis de vulnerabilidades, entre otros insumos con el detalle de las evidencias asociadas en determinar la necesidad de implementar medidas de protección que hagan la infraestructura tecnológica más robusta y evite problemas de seguridad en el futuro.

Por todo lo anterior, el comprender la importancia de las posibles funciones de un proceso especializado en la gestión de incidentes, podría brindar elementos para desarrollar estrategias, plantear iniciativas o reclutar a un equipo de trabajo.

- Como se mencionó anteriormente, la gestión de incidentes tiene un enfoque reactivo, pero el proceso puede ser parte de una estrategia avanzada que detecte, analice y corrija los eventos a través de un centro de operaciones de seguridad (SOC, por sus siglas en inglés), encargado de las labores de prevención detección y respuesta.

  Lo anterior, alineado a estructuras que otras instancias técnicas gestionan en Costa Rica, tales como CERT[5], CIRT[6] y CSIRT[7], las cuales formar parte de un SOC y buscan fortalecer la estructura con capacidades de proteger a servicios, tecnología, procesos, personas y negocios.

  Tal y como se menciona en la publicación efectuada el 21 de agosto del 2022 por el diario “CR Hoy” titulada “Proyecto quiere crear Agencia de Ciberseguridad, pero mantener el CSIRT-CR y con más instituciones”, citando:

  > *“Una iniciativa de ley pretende crear la Agencia Nacional de Ciberseguridad (ANC), pero a la vez mantener el Centro de Respuesta a Incidentes de Seguridad (CSIRT-CR) y crear más instituciones.*
  >
  > *Se trata del proyecto N°23.292, Ley de Ciberseguridad de Costa Rica, impulsado por el diputado José Joaquín Hernández, del Partido Liberación Nacional (PLN).*

[5] CERT significa equipo de respuesta (o preparación) para emergencias informáticas
[6] CIRT puede representar al equipo de respuesta a incidentes informáticos o, con menor frecuencia, al equipo de respuesta a incidentes de ciberseguridad.
[7] CSIRT significa equipo de respuesta a incidentes de seguridad informática

La propuesta quiere instalar la ANC como un órgano adscrito al Ministerio de Ciencia, Tecnología y Telecomunicaciones (Micitt).

La Agencia funcionará como un Centro de Operaciones de Ciberseguridad (SOC) del país, "encargado de la gestión preventiva, reactiva y proactiva de las amenazas e incidentes que, a través del uso de datos, puedan generar un riesgo de seguridad para la población costarricense", indica el documento legislativo.

La entidad estará conformada por una Dirección General que la dirigirá, con apoyo de un Consejo Asesor.

Además, ANC tendrá a su cargo 3 unidades operativas, todas independientes entre sí: el Centro de Intercambio y Monitoreo de Redes (CIMR-CR); el mismo CSIRT-CR y Centro de Inteligencia de Datos en Ciberseguridad (CID-CR).

En el caso del CIMR-CR tendrá la función preventiva y monitoreo continuo de alertas provenientes de los dispositivos del entorno, así como la responsabilidad de correlacionar, analizar y reportar todo patrón de riesgo identificado durante el monitoreo de amenazas y vulnerabilidades. Tiene a su cargo garantizar el proceso permanente de datos del entorno provenientes de los sensores de seguridad en conjunto con las organizaciones y sus proveedores.

Mientras tanto, el CSIRT-CR, que ya existe, tendrá una función reactiva, consistente en gestionar los canales de comunicación para la recepción de alertas informáticas, realizar la clasificación de dichas alertas, mantener el registro de incidentes creado en esta ley y el nivel de riesgo actualizados, así como la responsabilidad de investigar y proveer soporte a las instituciones afectadas por algún incidente que así lo requieran, emitir los boletines de alerta y generar las campañas de concientización en ciberseguridad.

Finalmente, CID-CR tendrá una función proactiva, consistente en proporcionar datos e información predictiva a la Agencia para facilitar la toma de decisiones, asegurar el cumplimiento de las misiones y objetivos a largo plazo, reducir la superficie de ataque, crear ejercicios de simulación de amenazas y modelado de adversarios, así como mantener a la ANC y quienes utilicen sus servicios permanentemente actualizados en nuevas amenazas del entorno nacional e internacional."

Ahora bien, la seguridad como el activo más importante que se puede presentar a los usuarios debe estar respaldado por equipos de ciberseguridad altamente calificados en gestionar las incidencias. Pero, también es posible disponer de estructuras con mayores beneficios, tal como un servicio SOC que asegure una respuesta a las amenazas, ayudando a prevenir cualquier brecha de seguridad.

3- CONSIDERACIONES NORMATIVAS

Al respecto, el artículo 8 de la Ley General de Control Interno, respecto al sistema de control interno, establece:

"(…) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
b) Exigir confiabilidad y oportunidad de la información.
c) Garantizar eficiencia y eficacia de las operaciones."

Además, las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, descrito en el apartado la "IV. Gestión del Riesgos Tecnológicos", refieren:

"La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.

La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."

Por otra parte, esas mismas normas en el apartado "XI, Seguridad y Ciberseguridad", indican:

"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

La Unidad de TI debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales."

Lo anterior, en alineamiento a lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, en el apartado "XII. Administración Infraestructura Tecnológica", en el cual refiere:

"La institución debe implementar prácticas formales que permitan mantener identificados y actualizados los activos de TI, mediante inventarios de recursos tecnológicos instalados en la organización (hardware, software, aplicaciones, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas."

Finalmente, en el apartado "XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos", indica:

"La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas."

4- CONSIDERACIONES FINALES

La Caja Costarricense del Seguro Social (CCSS), dentro de su gestión y servicios que presta a la ciudadanía depende de la información, sistemas y soluciones tecnológicas, ante ello surge la necesidad de establecer una estrategia acorde a las obligaciones institucionales.

Sin ser la excepción, la gestión de incidentes de seguridad, necesaria para poder minimizar el impacto de forma rápida ante cualquier amenaza que vulnere a la Institución.

En ese sentido, la CCSS debe buscar de forma constante la mejora en la atención de incidentes (bajo las condiciones actuales) y el fortalecimiento de la estrategia orientada a especializarse en el manejo de eventos (considerando las iniciativas planificadas o a desarrollar a futuro).

Lo anterior, en aras de valorar esta temática como una de las columnas esenciales dentro de las actividades citadas en el cuerpo normativo que refiere a seguridad de la información y ciberseguridad. Debido a esto, es relevante incorporar estas metodologías a nivel táctico y técnico, en el ámbito de resolución: central, regional y local e incluso en lo que corresponda para los proveedores de servicios tecnológicos.

Por otra parte, es conocido que la CCSS actualmente puede prevenir ciertos eventos, pero habrá otros que requieren de un mayor alcance, aumentar el impacto, minimizar la probabilidad de ser afectados por una amenaza en ciberseguridad, objetivos que sin duda refieren a las oportunidades de mejora citadas en esta misiva.

A ese respecto, es relevante definir roles acordes a las necesidades institucionales; escalar de forma oportuna los incidentes; permitir la visibilidad durante la atención del evento (mantenerse informado); detectar patrones y estandarizar soluciones; crear y consultar reportes con regularidad; usar los recursos con eficiencia; gestionar las lecciones aprendidas, entre otros aspectos que pueden aportar productividad y calidad al servicio.

No obstante, para implementar esas operaciones es fundamental comprender las etapas desde la preparación hasta la contención y resolución de incidentes; incluyendo las acciones posteriores al cierre.

Es decir, a partir del razonamiento de estas metodologías, se pretende incentivar a los involucrados en la definición de diferentes planes (mejorarlos o implementarlos) que involucren tanto la respuesta a incidentes, como la recuperación de la organización frente a la ocurrencia de algún evento adverso.

En virtud de lo indicado, este Ente Fiscalizador hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio; con el objetivo de ratificar o comenzar a discurrir al menos los temas detallados en la misiva, referentes a la gestión de incidentes.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.10.03 17:38:05 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General – 1100.
Doctor Randal Álvarez Juárez, gerente, Gerencia Médica -2901.
Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera -1103.
Licenciado Jorge Granados Soto, gerente a.c., Gerencia Administrativa -1104.
Doctor Esteban Vega de la O, gerente, Gerencia Logística - 1106.
Ingeniero Jorge Granados Soto, gerente, Gerencia Infraestructura y Tecnologías – 1107.
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia Pensiones – 9108.
Auditoría