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

AS-AATIC-125-2022
1 de julio de 2022

Máster
Idannia Mata Serrano, subgerente a.i.

Máster
Vanessa Carvajal Carmona, jefe
Subárea en Seguridad en TIC
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES -1150

Estimadas señoras:

ASUNTO: **Oficio de Asesoría sobre el comportamiento, tácticas y herramientas utilizadas por los ciber atacantes.**

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022, con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y siendo consecuentes a lo indicado en el oficio AI-874-2022 del 6 de junio del 2022, sobre el inicio de la evaluación referente al ataque cibernético sufrido en la CCSS y sus efectos a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022; procede a emitir la siguiente asesoría sobre el asunto citado en el epígrafe.

A ese respecto, es conocido que la Caja Costarricense de Seguro Social (CCSS), recibió ciberataques y le obligaron (de manera preventiva) a desactivar todos los sistemas informáticos de la Institución; habiendo ya trascurrido 30 días desde la detección de ese incidente informático a la fecha.

Aunado a lo anterior, recientemente se han restablecido algunos sistemas de información y la CCSS sigue bajo la necesidad de ejecutar el plan de gestión de crisis y/o recuperación, según corresponda; seguido de la puesta en marcha de una estrategia priorizada en ciberseguridad.

Bajo ese contexto, esta Auditoría estima pertinente dar a conocer algunos tópicos referentes a la importancia de comprender cómo consiguen los hackers atacar a las organizaciones y en qué consisten las amenazas perpetradas a los servicios tecnológicos, con el propósito de tomar ventaja en la contienda originada por los ciberatacantes.

OBSERVACIONES

A continuación, se mencionan los comportamientos, tácticas y herramientas utilizadas por los delincuentes informáticos para vulnerar a las organizaciones, aunado las siguientes observaciones que podrán ser valoradas en esa Administración para diseñar, implementar o mejorar la estrategia de ciberseguridad.

1. Los cibercriminales son especializados

La industria del cibercrimen no actúa por inercia, en estos casos los atacantes examinan la superficie de ataque, aplican técnicas y herramientas para penetrar sistemas, detectar los puntos débiles de las organizaciones e inclusive estudia el riesgo al que se expone una determinada entidad.

En ese sentido, los hackers laboran en una industria rentable que genera ganancia a partir de la vulneración de las infraestructuras críticas, lo cual les demanda mantenerse altamente especializados.

Según el canal británico de televisión abierta “BBC News” en su nota “"Los hackers nos aventajan porque hay poca gente especializada en ciberseguridad. No damos abasto": Soledad Antelada, la latina que protege al Departamento de Energía de E.E.U.U.”, publicada el 6 de julio del 2021, la especialización de los atacantes radica en:

> *“El tema es que quien está en el lado oscuro tiene mucha más intención y tiempo.*
>
> *Los que defendemos somos menos porque hay poca gente especializada. No damos abasto. Por eso a veces nos ganan la partida.*
>
> *Como te digo, igual cada vez hay más gente y se le intenta poner más recursos. Aun así, seguimos un poco a la cola.*
>
> *Hay muchos tipos de hackers, son más y tienen más tiempo. Son 24 horas intentando entrar en el sistema. Y tú tienes que estar 24 horas intentando parar esos ataques.*
>
> *No es lo mismo la ofensiva que la defensiva. La ofensiva no tiene otra cosa que hacer que entrar y al final consigue hacerlo por algún lado.”*

Así las cosas, la Institución debe reforzar el bajo nivel de especialización en ciberseguridad que posee para atender el tema de marras y disponer de mecanismos de defensa adecuados. Tal y como lo indica el diario nacional “La República” el 27 de junio del 2022 en la nota “"La falta de mecanismos de defensa del Gobierno no es falta de voluntad, sino de capacidad", Roger Brenes, especialista en delitos informáticos”, citando el experto consultado, lo siguiente:

> *“Los responsables de Tecnologías de Información de las instituciones deben tratar de ponerse al mismo nivel de conocimiento de los ciberdelincuentes; lo contrario representaría un enorme peligro a corto plazo”*
>
> *(…) Las instituciones públicas se enfocan de lleno en capacitar a sus empleados en las labores que les corresponden acorde a las plazas o puestos que cubren, mientras que no ven necesaria y en muchos casos hasta obligatoria, una efectiva gama de capacitaciones en seguridad informática para no ser presas fáciles de los ciberdelincuentes que opten en ingresar por puntos débiles a sistemas estatales y siempre es el usuario (en este caso los empleados públicos) el eslabón más débil dentro de las líneas de la seguridad informática.”*

2. Su objetivo es provocar caos

Los hackers al lograr acceder a sistemas críticos en la organización asumen el rol de generar caos, algunos ejemplos graves mencionados en la nota periodística ""Los hackers nos aventajan porque hay poca gente especializada en ciberseguridad. No damos abasto": Soledad Antelada, la latina que protege al Departamento de Energía de EE.UU.", publicada el 6 de julio del 2021 por el canal británico de televisión abierta "BBC News", cita:

> *"Si se te va un grid eléctrico en medio de un invierno siberiano la gente puede pasarlo muy mal.*
>
> *Algo parecido a lo que sucedió en Texas (una tormenta invernal que dejó decenas de muertos y millones sin electricidad el pasado febrero). En ese caso no fue un ataque informático, pero son consecuencias similares terribles que podrían ocurrir.*
>
> *Imagínate que ataquen un embalse. Descarguen el agua y puede inundar hasta pueblos.*
>
> *Si penetran en el sistema de control de los aviones también puede ser fatal.*
>
> *Luego, siguiendo un efecto dominó, mucha gente habla de un escenario en que se pueda caer internet. Es difícil porque se trata de una red con muchos sistemas, pero podría ocurrir un apagón grande o parcial, por países, si se ataca la red global.*
>
> *Ponte a pensar, sobre todo en este momento de la historia en que muchos hemos estado trabajando desde casa. Si se cae internet, se pierde muchísimo dinero y bajarían los sistemas productivos.*
>
> *Tampoco fue un ataque cibernético, pero mira lo que pasó en el Canal de Suez. El barco quedó atracado y se produjo un efecto dominó que afectó hasta los mercados.*
>
> *Los ataques estratégicos pueden afectar bolsas de valores y economías en el resto del mundo. Hay ataques que cuestan muy poco lanzarlos, pero generan un daño masivo."*

En ese orden de ideas, llama la atención las acciones que podrían perpetrarse en las organizaciones, sin ser la excepción el sector salud. No obstante, se podrá efectuar pruebas de penetración (consiste en comportarte como un atacante) y así analizar por dónde puede ser más fácil atacar, definir qué merece la mayor atención y cuál podría ser su objetivo.

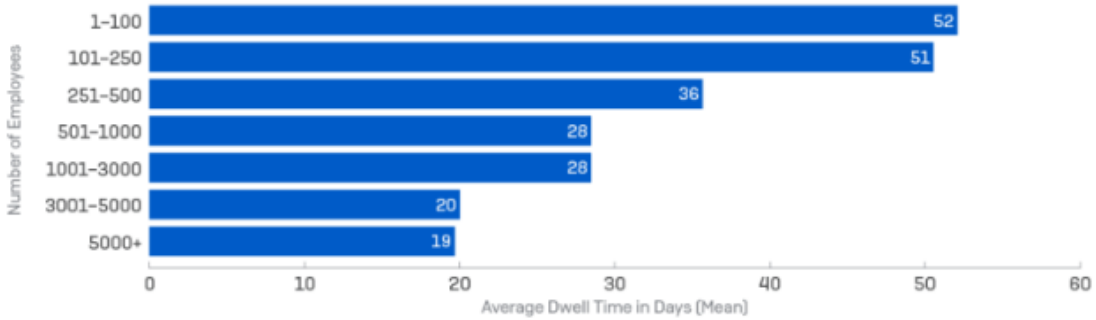
De esa manera, emulando ambientes que permitan precisar cuáles son las brechas para evitar niveles de exposición descontrolados, tales como los discurridos anteriormente.

3. Practican la intrusión silenciosa

Según las investigaciones efectuadas por empresas expertas en ciberseguridad, indican que la permanencia de los intrusos (desde que logran perpetrar a la organización) es de aproximadamente 51 días, es decir, permaneciendo en las redes de compañías con hasta 250 empleados, mientras 20 días en aquellas con entre 3.000 y 5.000 trabajadores.

Lo anterior, según se evidencia en el informe "The Active Adversary Playbook 2022" de la empresa Sophos (empresa experta en ciberseguridad de última generación), la cual resume el dato supracitado, por medio de la siguiente imagen:

Imagen No. 1
Tiempo medio que un atacante permanece oculto en las redes (según tamaño) antes de su detección



Fuente: Publicación Active Adversary Playbook 2022, Sophos.

Además, en esa misma publicación se amplía como los resultados antes indicados pueden interrelacionarse con la motivación del atacante, la persistencia para obtener resultados e inclusive la competencia que puede existir ante objetivo en común (varios ciberdelincuentes atacando un mismo sitio), citando:

> *"Los atacantes consideran que las empresas más grandes son más valiosas, por lo que están más motivados para entrar, conseguir lo que quieren y salir. Por el contrario, las compañías más pequeñas tienen menos "valor" percibido, por lo que los atacantes pueden permitirse merodear por la red en segundo plano durante más tiempo. También es posible que estos ciberatacantes tuvieran menos experiencia y necesitaran más tiempo para averiguar qué hacer una vez que estuvieran dentro de la red. Por último, las empresas más pequeñas suelen tener menos visibilidad de la cadena completa del ataque para detectar y expulsar a los atacantes, lo que prolonga su presencia", comenta Shier. "Con las oportunidades que ofrecen las vulnerabilidades ProxyLogon y ProxyShell sin parchear y el aumento de los IAB, estamos viendo más evidencias de la presencia de múltiples atacantes en un solo objetivo. Si hay mucha gente dentro de una misma red, los atacantes querrán moverse rápido para superar a su competencia".*

Así las cosas, el estudio efectuado por Sophos y mencionado en la observación de marras, se encuentra en el Anexo 1 de esta misiva, en caso de requerir esa Administración profundizar en los resultados dados en la publicación.

Bajo el contexto de lo evidenciado por los especialistas en ciberseguridad, las labores de los atacantes suelen ser silenciosas, lo que les proporciona tiempo para realizar actividades maliciosas como la implantación de amenazas; movimientos laterales (infección de paciente 0 y avanzan hasta un objetivo mayor), cifrado de información, reconocimiento de vulnerabilidades, volcado de credenciales, exfiltración de datos, entre otras formas de ataques.

Por tanto, se requiere una actividad oportuna para detectar amenazas y mitigar el comportamiento de los intrusos; por medio soluciones de software, mecanismos automatizados, inteligencia artificial, así como otros elementos de apoyo a los equipos técnicos especializados, ya que en solo minutos una amenaza puede causar daños en la red y conforme pasa mayor tiempo, el infiltrado aumenta su probabilidad de extorsión mediante el cifrado, venta o publicación de los datos.

4. Conocen los eslabones más débiles

Uno de los elementos a favor de los ciber delincuentes que arremeten contra la seguridad de las infraestructuras críticas, es conocer la principal debilidad de organización sin siquiera estudiarlas.

En ese sentido, su accionar se fundamenta en la conducta generalizada que ha caracterizado al entorno institucional por años, particularmente asociado a la carencia de acciones dirigidas por el nivel estratégico en la definición de tácticas de protección; limitaciones en la formación de profesionales; mecanismos de control obsoletos o deficientes; y la ausencia de una cultura arraigada en la educación al usuario.

Tal y como lo menciona la publicación del medio de comunicación “Diario TI” en la nota “El factor humano: el eslabón más débil de la ciberseguridad” publicado el 29 de octubre del 2021, citando:

> *“La seguridad digital requiere de una mirada holística, no sólo técnica, y aquellas empresas que lo logren sin duda estarán más preparadas para gestionar este riesgo. Los planes de inversión en ciberseguridad de las empresas, ¿integran a las áreas de comunicaciones y a recursos humanos en actividades claves? Así como años atrás discutimos la importancia de incorporar la innovación como parte del ADN de las empresas, hoy es aún más relevante una cultura de ciberseguridad.*
>
> *La inversión no debe ser focalizada en las áreas de tecnología y operaciones, tenemos un factor cultural que hoy es clave. Incorporar la seguridad de nuestra data y operaciones como parte del ADN es una inversión a largo plazo. ¿Por qué no subir a la alta gerencia, comunicaciones internas, marketing, recursos humanos, mesa de compras y a todas las demás áreas de las empresas en una cultura de ciberseguridad? Aquellas firmas cuya visión articule una mirada integral y multidisciplinaria, serán capaces de enfrentar exitosamente los riesgos vinculados a la ciberseguridad.”*

Lo anterior, aunado a fallas de seguridad en los controles, configuraciones débiles o inseguras y malas prácticas que explotan los cibercriminales, tales como:

- No habilitar la autenticación multifactor.
- Asignar accesos y permisos de forma incorrecta.
- Uso de software desactualizado.
- Mantener las credenciales de acceso que vienen por defecto.
- Falta de controles en servicios de acceso remoto.
- Uso de contraseñas débiles o múltiples contraseñas (una para cada sistema institucional).
- Servicios en la nube sin protección
- Servicios expuestos a internet mal configurados o puertos abiertos.
- Error al detectar un correo de phishing.

- Respuesta limitada de productos de seguridad instalados.
- Falta de supervisión o análisis sobre las aplicaciones de software instaladas en los equipos.
- Entre otros.

A ese respecto, la apreciación emitida es ratificada, según una publicación del medio de comunicación "Diarioti" en la nota "Factor Humano: ¿El Eslabón Más Débil en la Seguridad?" publicado el 26 de agosto del 2016, citando:

> *"El cibercrimen dejó de ser una cuestión de aficionados. Hoy estamos frente a verdaderas organizaciones, muchas de ellas internacionales, dedicadas con tiempo y recursos exclusivos a explotar las vulnerabilidades de seguridad de la información en todos sus niveles, para realizar fraudes online, estafas electrónicas, robos y captura de datos, así como suplantaciones de identidad, muchas de las cuales afectan a empresas. Muchos gerentes creen que sus organizaciones están protegidas por tener los sistemas tradicionales de resguardo, olvidándose de considerar de manera más directa a los usuarios.*
>
> *Los usuarios sin una conciencia sobre la seguridad de la información, sin capacitación, constituyen un alto riesgo para las organizaciones, pues, además del riesgo que conlleva la clásica 'ingeniería social', hoy las personas acceden a un mayor número de dispositivos conectados a Internet, donde muchas veces portan o manejan también información de su empresa.*
>
> *En ese contexto, es cada vez más frecuente que usen dispositivos móviles de su propiedad, los cuales suelen no ser tema de injerencia o preocupación por parte la empresa en la que trabajan. La tendencia a usar smartphones, notebooks y tablets en donde se accede a datos de la empresa es universal; por lo tanto, las empresas deben adaptar y/o ampliar sus políticas de seguridad a dichos dispositivos, los cuales pueden controlarse de manera transparente para los usuarios y sin afectar su privacidad."*

Así las cosas, es imperativo que la Institución sea cada vez más consciente de la importancia de la ciberseguridad y por ende menos predecible; fortaleciendo su postura de control y monitoreo siendo garante del adecuado uso y aprovechamiento de las Tecnologías de Información y Comunicaciones (TIC), como de la correcta gestión de los riesgos tecnológicos.

5. Técnicas y tácticas de ataque

Según la publicación de ESET[1] del 19 de mayo del 2022, titulada "Métodos más utilizados por cibercriminales para lograr acceso a redes corporativas", cita las técnicas utilizadas por los hackers para aprovechar debilidades y obtener acceso a los sistemas de una organización, a saber:

> *"**La explotación de aplicaciones públicas en Internet**: como pueden ser sitios web o servidores, bases de datos o protocolos y servicios utilizados para la administración de servicios de red. En definitiva, cualquier aplicación accesible desde Internet. Para más información ver la descripción de Mitre ATT&CK.*

[1] ESET, s.r.o., es una compañía de software especializada en ciberseguridad. Los productos de seguridad de ESET se fabrican en Europa 1 y proporcionan software de seguridad en más de 200 países y territorios en todo el mundo, y su software está disponible en más de 30 idiomas.

***Servicios de acceso remoto expuestos a Internet**: esta técnica está relacionado al uso de VPN y otros servicios que permiten a un usuario conectarse a una red corporativa desde una ubicación externa. Los actores maliciosos suelen apuntar a estos servicios de acceso remoto para lograr acceso a una red.*

***Phishing**: la vieja y conocida técnica de enviar correos electrónicos para engañar a potenciales víctimas con archivos adjuntos y enlaces maliciosos sigue siendo efectiva. A través del phishing muchas organizaciones sufren la infección de algún tipo de código malicioso luego de que algún miembro desprevenido cae en la trampa de ingeniería social.*

***Explotación de relaciones de confianza**: esta técnica consiste en lograr acceso a una organización a través de terceras partes que tienen un vínculo o conexión, como puede ser un proveedor que administre la seguridad o servicios de IT, y aprovechar el acceso que tienen a la red de la organización que desean atacar.*

***Cuentas válidas**: la quinta técnica más utilizada tiene que ver con el uso de credenciales de acceso válidas para obtener acceso inicial, mantenerse dentro de una red, intentar escalar privilegios o modificar la configuración de los mecanismos de defensa de la víctima."*

Aunado a lo anterior, las pretensiones de los delincuentes informáticos para acceder a la red de las organizaciones, valora los recursos económicos, cuantía de la información, cantidad de profesionales, así como otros factores de relevancia; los cuales podrían determinar cuál táctica utilizar para perpetrar la infraestructura critica. Entre las más comunes se encuentra el acceso inicial a red (punto de apoyo inicial); ejecución sospechosa de aplicaciones, equivalente a un 31%; y la persistencia en el intento de acceso; según se evidencia en el informe "The Active Adversary Playbook 2021" de la empresa Sophos, la cual resume los datos analizados, por medio de la siguiente imagen:

Imagen No. 2
Tácticas de ataque por cibercriminales, 2020/21

Fuente: Publicación Active Adversary Playbook 2021, Sophos.

A pesar de existir diferentes técnicas y tácticas utilizadas por los criminales, también se pueden encontrar recomendaciones consignadas para minimizar las posibilidades de que intrusos accedan a los sistemas informáticos.

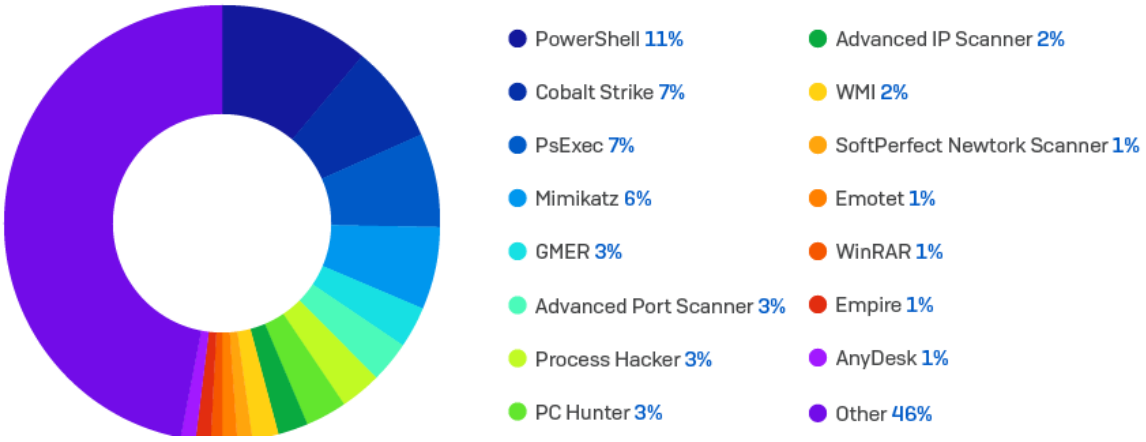
En otras palabras, las tácticas por aplicar variarán, pero de forma general debe incentivar la formación y concientización de los usuarios; detección de amenazas por medio de seguridad perimetral, protección contra código malicioso, políticas de seguridad y la configuración segura de dispositivos; prevaleciendo la intrusión como un medio para gestionar vulnerabilidades, supervisar procesos, controlar accesos, entrenar a usuarios; entre otras prácticas orientadas a impulsar la disposición de controles eficaces y eficientes.

6. Protocolos y herramientas utilizadas

Finalmente, resulta conveniente conocer cuáles son las herramientas utilizadas por los ciberatacantes para vulnerar la red, aspecto que nos brindará una oportunidad de prevenir acciones sospechosas o revisar los ajustes en la configuración de algunas de ellas, las cuales sorprendentemente forman parte del software incluido en los sistemas operativos.

Según detalla el informe "The Active Adversary Playbook 2021" de la empresa Sophos las quince soluciones más utilizadas por los hackers en los equipos infectados, son los que se pueden observar en la siguiente imagen:

Imagen No. 3
Herramientas más utilizadas por ciberatacantes



Fuente: Publicación Active Adversary Playbook 2021, Sophos.

En ese sentido, los resultados evidencian una amplia gama de herramientas e inclusive llama la atención que algunas de ellas pueden ser utilizadas por profesionales de TI con fines benignos. Precisamente, esa condición es la que hace a los atacantes utilizarlas, porque les permiten implementar actividades como el robo de credenciales, el movimiento lateral y la ejecución de programas, mientras se mezclan con la actividad de TI cotidiana.

Así las cosas, el estudio efectuado por Sophos y mencionado en la observación de marras, se encuentra en el Anexo 2 de esta misiva, en caso de requerir esa Administración profundizar en los resultados dados en la publicación.

Por otra parte, este Órgano Fiscalizador ha emitido productos que refieren a esas herramientas y/o vulnerabilidades detalladas en el estudio, por ejemplo:

Cuadro No. 1
Productos de Auditoría referentes a herramientas y/o amenazas cibernéticas

No. Oficio	Asunto
AI-573-2021 del 11 de mayo del 2021	Oficio respecto a vulnerabilidad en Microsoft Exchange Server
AS-AATIC-089-2022 del 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”.
AI-905-2022 del 13 de junio del 2022	Oficio de información en relación con acciones preventivas para minimizar la materialización de riesgos generadas por la herramienta “Mimikatz”.

Fuente: Auditoría Interna, elaboración propia.

Por ello, la Administración debe mantenerse receptiva ante las alertas emitidas por entes especializados, proveedores de servicios, entre otros profesionales que notifican sobre estos y otros aspectos con el objetivo de minimizar los efectos de las amenazas dirigidas por ciberdelincuentes.

En ese orden de ideas, a nivel institucional se debe verificar la configuración de los dispositivos, la necesidad de disponer de ese tipo de herramientas y/o regular su uso, lo cual resulta un desafío para las instancias especialistas en TIC al tener que diferenciar las actividades maliciosas y legítimas en la red. No obstante, esa labor podría ser soportada mediante la premisa de garantizar una estrategia basada en actividades preventivas y utilizado la tecnología acorde a las necesidades institucionales.

CONSIDERACIONES FINALES

El mundo del cibercrimen se ha vuelto altamente especializado e inclusive han desarrollado estrategias para vulnerar a un objetivo. En este panorama de amenazas, la institución debe mantenerse al día con las herramientas y enfoques que utilizan los atacantes.

En ese sentido, es vital que el accionar de la CCSS asuma un rol “protector” con precisión y dedicación por comprender el comportamiento del hacker (a manera general y predictiva) para detectar y neutralizar los ataques lo más pronto posible.

En virtud de lo anterior, la inversión para efectuar esa tarea no es solo cuestión de dinero, sino de tiempo, capacitación y disponibilidad de herramientas digitales que hagan posible el salvaguardar los activos de la institución ante ataques cibernéticos, cada vez más comunes a nivel mundial.

Ahora bien, se pretende que a partir de las observaciones inmersas en esta misiva y los criterios emitidos en productos de Auditoría que refieren a la temática de ciberseguridad, puedan valorarse en la definición, puesta en marcha o mejora de una estrategia ajustada a los requerimientos específicos de la Caja.

De esa manera, marcando la diferencia para futuros incidentes en cuanto no perjudicar las actividades sustantivas, disminuir el daño de la imagen institucional o en caso de materializarse el riesgo, prever de forma anticipada una solución conforme a las necesidades de los procesos.

Además, siendo consecuentes a lo estipulado en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que establecen dentro de los procesos del marco de gestión de TI, lo correspondiente a la "Seguridad y Ciberseguridad", citando:

> *"**XI. SEGURIDAD Y CIBERSEGURIDAD***
>
> *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."*

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio, con el objetivo de incentivar la capacidad de la Institución para recuperar, restablecer el componente TI y mejorar la estrategia de ciberseguridad a seguir.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.06 11:13:32 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

Anexos (1)

1- Estudio “The Active Adversay Playbook 2022”- Sophos
2- Estudio “The Active Adversay Playbook 2021”- Sophos

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General-1100.
Auditoría