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

AD-ATIC-039-2022
21 de abril de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL - 1100.

Máster
Roberto Blanco Topping, Subgerente a.i

Máster
Mayra Ulate Rodriguez, jefe
Área de Seguridad y Calidad Informática
DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Estimado(a) señor(a):

ASUNTO: Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS

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, esta Auditoría advierte sobre aspectos relacionados con la exposición a ataques cibernéticos en la Institución.

Lo anterior, al conocer del ciberataque materializado a la cuenta de Twitter de la CCSS, según informó el diario La República el 19 de abril del 2022, en nota titulada "*Hackeo a cuenta de Twitter de la CCSS y sitio alterno del Micitt se unen al del Ministerio de Hacienda", así como la noticia "Portal de Recursos Humanos de CCSS sufre ataque cibernético" publicado por el diario La Nación este 20 de abril del 2022.*

A ese respecto, contrastándolo con lo indicado en el siguiente conjunto de normas, las cuales pretenden mejorar los procesos de seguridad y obtener el mayor nivel de protección, minimizando y conociendo los riesgos a los que se pueden exponer los activos (equipamiento e información), a saber:

- Normas Técnicas para la gestión y el control de las Tecnologías de Información, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, 2021.
- Normas Institucionales de Tecnologías de Información.
- Políticas y Normas Institucionales de Seguridad Informática.
- Norma de Gestión de Seguridad de la Información ISO/IEC 27001
- Marco referencial COBIT 5 (Objetivos de Control para las Tecnologías de Información).

ANTECEDENTES

Conceptos y definiciones

Frente a la transformación digital y el uso masivo de tecnologías de información que han tenido las organizaciones, de todas las industrias y tamaños, durante los últimos años, no se puede ignorar la posibilidad que existe de ser víctima de un ataque cibernético en cualquier momento.

Es decir, a pesar de las ventajas que ofrece el uso y aprovechamiento de las Tecnologías de Información y Comunicaciones (TIC), existen riesgos inherentes asociados a la exposición a ataques por parte de los ciberdelincuentes que están atentos a las vulnerabilidades presentes en los sistemas informáticos y así generar réditos a su favor o simplemente causar daño.

En ese sentido, un ciberataque son aquellas acciones ofensivas y perjudiciales contra los sistemas de información, sea de una persona, una empresa o una entidad gubernamental. Estos sistemas pueden ser las redes, bases de datos y todos los activos que almacenen datos e información confidencial o sensible y de valor de la organización.

Para tales efectos, los expertos en estos temas recomiendan implementar estrategias y medidas orientadas a reducir la posibilidad de sufrir un ataque de este tipo o de materializarse enfrentarlo con éxito, ya que no solo pone en riesgo la reputación de la empresa sino también su operación.

Contexto actual

Ahora bien, Costa Rica no se encuentra exenta de ser objeto de estos ataques que buscan afectar, alterar, extorsionar o destruir no solo la reputación de una empresa o persona, sino también, impactar negativamente su operación o relación con los diferentes grupos de interés.

En ese sentido, recientemente se ha conocido ataques pertenecientes a la familia de los ransomware[1] y que utiliza la modalidad de extorsión con sus víctimas, según describe la nota periodística "*Grupo Conti asegura haber hackeado Ministerio de Hacienda y contar con 1 terrabyte de información de contribuyentes"* publicada por el diario La República el 18 de abril del 2022, se indicó:

> *"El grupo cibercriminal Conti, fundado en Rusia, asegura haber hackeado los sitios web del Ministerio de Hacienda y contar con 1 terrabyte de información de contribuyentes.*
>
> *Así lo dieron a conocer a través de la red social de microblogging Twitter, donde señalan que comenzarán a exponer los datos a partir del 23 de abril.*
>
> *Las plataformas que se habrían visto comprometidas son la TIC@, que utilizan importadores y exportadores nacionales, además de las agencias aduanales y el ATV, donde los grandes y pequeños contribuyentes deben presentar sus declaraciones de impuestos de la renta, de ventas, entre otras obligaciones fiscales.*
>
> *A pesar de que el ataque informático trascendió hasta el día de hoy, se habría realizado desde ayer domingo de Resurección o Pascua, cuando la mayoría de personal del Gobierno y sector privado se encontraban libres producto de la celebración de la Semana Santa"*

Posteriormente, se publicó ese mismo día una nota titulada "*Hackers piden $10 millones al Gobierno de Costa Rica por información del ministerio de Hacienda*", en el diario supracitado, donde se menciona:

> *"El grupo de hackers de origen ruso Conti, piden $10 millones al Gobierno de Costa Rica por la información sustraída aparentemente de los sitios web del ministerio de Hacienda.*
>
> *Pedimos solo 10 millones de dólares por mantener los datos de sus contribuyentes" señala una publicación de la cuenta BetterCyber en Twitter, donde se reproduce el mensaje de los ciberdelincuentes, los cuales aseguran contar con 1 terabyte de información.*
> *El ataque informático habría sido del tipo "Ransomware" que restringe el acceso a archivos de un sistema infectado al codificarlos y solicitar dinero a cambio de revertir esta situación."*

No obstante, los ataques cibernéticos se seguían materializando a nivel país, en este caso afectando al Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT) tal y como lo informa la página web "*el*

[1] El ransomware es un tipo de código malicioso que secuestra su información para extorsionarlo y exigirle el pago de una suma de dinero, ya sea para recuperarla o para evitar su divulgación. **Fuente**: Página Web de ESET.

mundo cr" mediante la nota "*Ataque cibernético de últimas horas a entidades públicas es «un hecho sin precedentes», asegura exministro del MICITT*" del 19 de abril de 2022, citando:

> *"El exministro del Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT), y experto en ciberseguridad Luis Adrián Salazar, aseguró que «estamos ante un hecho sin precedentes», ante los ataques cibernéticos de las últimas horas a entidades públicas.*
>
> *Según manifestó Salazar «a partir de los acontecimientos con el posible potencial hackeo del Ministerio de Hacienda y viendo el hackeo menor del Ministerio de Ciencia Tecnología y Telecomunicaciones consideró que este tema debe ser tratado de manera inmediata con la mayor atención posible del máximo nivel».*
>
> *El experto señaló que «espero equivocarme estamos ante un hecho sin precedentes y es fundamental que se tomen las acciones necesarias y de manera colaborativa entre sector público y privado se analice esta situación, pues podría tener una magnitud muy importante».*
>
> *De igual forma, agregó que «con pasar del tiempo y pues la digitalización de sistemas de información es total y completamente posible que los ataques hacia infraestructura crítica de los gobiernos sean objetivo de los ciberataques, estoy hablando de sistemas de información, estoy hablando de sistemas de energía, estoy hablando de diferentes tipos de infraestructura crítica».*
>
> *«Aquí es importante mencionar que Costa Rica ha tenido avances importantes, se tiene un clúster de ciberseguridad, existe una estrategia de ciberseguridad se ha trabajado en alianzas internacionales, pero creo sin duda que todavía no existe la conciencia de que el tema de ciberseguridad debe priorizarse como política nacional», resaltó."*

Por otra parte, el diario La República publicó el 19 de abril del 2022, la nota "*Hackeo a cuenta de Twitter de la CCSS y sitio alterno del MICITT se unen al del ministerio de Hacienda",* informando:

> *"En el caso de la cuenta de CCSS en la red de microblogging se publicaron varios mensajes de unos ciberdelincuentes que promocionaban la rifa de 5 mil bitcoins, pero la misma fue recuperada minutos después por el equipo informático de la institución."*

Finalmente, *el diario La Nación el 20 de abril del 2022, informa "Portal de Recursos Humanos de CCSS sufre ataque cibernético", citando:*

> *"Las plataformas digitales de las entidades públicas siguen siendo objeto de ataques cibernéticos. La Caja Costarricense de Seguro Social (CCSS) sufrió este miércoles una incidencia en su portal de Recursos Humanos, que obligó a activar una revisión integral de todos sus sistemas para determinar el alcance de lo ocurrido.*
>
> *El ingeniero Roberto Blanco Topping, director de Tecnologías de Información de la CCSS, detalló que una vez detectado el problema se procedió a blindar los accesos, dar de baja el portal y coordinar con los equipos técnicos para determinar si se produjo alguna extracción de información o de datos, o eventuales accesos a otras plataformas.*
>
> *"Los equipos de monitoreo, humanos y en conjunto con las herramientas tecnológicas con las que se cuenta detectaron incongruencias con respecto a la gestión de datos en el portal de Recursos Humanos de la institución y se determinó que se había producido un ataque externo", detalló mediante un comunicado.*
>
> *Blanco agregó que en este momento se encuentran en un proceso de análisis para determinar cuál fue el impacto y los pasos a seguir."*

Productos emitidos por la Auditoría Interna

Si bien es cierto la Caja ha formulado acciones relacionadas al tema, este Ente Fiscalizador ha sido insistente en diferentes momentos para señalar a la Administración las oportunidades de mejora relacionadas con la disponibilidad de estrategias avanzadas de ciberseguridad y prevención del fraude.

Por ejemplo, la temática antes indicada ha sido señalada con anterioridad mediante los siguientes productos:

Cuadro No.1
Productos emitidos Auditoría Interna sobre Seguridad de la TIC y ciberseguridad

Informe / Oficio No.	Fecha	Asunto
Informe de Auditoría ATIC-049-2014	09 de mayo de 2014	Gestión de la seguridad de la información institucional y el rol que cumple el Área de Seguridad y Calidad informática.
Informe de Auditoría ATIC-127-2015	15 de junio de 2015	Avance en proyectos de adquisición e implementación de software y hardware de seguridad informática.
Informe de Auditoría ATIC-45-2016	4 de abril de 2016	Fortalecimiento de la infraestructura de seguridad en Tecnologías de Información y Comunicaciones.
Oficio 47886-2017	14 de febrero de 2017	Oficio Informativo respecto al marco normativo relacionado con la Privacidad y Confidencialidad de la Información en las Comunicaciones.
Informe de Auditoría ATIC-72-2017	9 de agosto de 2017	Avance del proyecto modelo de gobernanza de las tecnologías de información y comunicaciones y de seguridad de la información de la Caja Costarricense de Seguro Social (CCSS).
Oficio 53581-2017	22 de agosto de 2017	Observaciones relacionadas con la Seguridad Informática de la Información de los servicios institucionales de Tecnologías de Información y Comunicaciones (TIC) accesados a través de dispositivos móviles.
Oficio 53708-2017	6 de septiembre de 2017	Aspectos relacionados a la Seguridad Informática de acuerdo con temas abordados en el Convenio de Ciberdelincuencia celebrado en Budapest.
Informe de Auditoría ATIC-106-2017	29 de septiembre de 2017	Gestión del análisis integral de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones ejecutado por la Dirección de Tecnologías de Información y Comunicaciones a través de una contratación directa de servicios profesionales a la Firma Consultora Deloitte & Touche.
Oficio 6441-2018	13 de abril de 2018	Observaciones relacionadas con el Gobierno de Seguridad de la Información.
Informe de Auditoría ATIC-83-2018	23 de julio de 2018	Cumplimiento de la Ley No. 8968 “Protección de la Persona Frente al Tratamiento de sus Datos Personales” y su reglamento en la Caja Costarricense de Seguro Social (CCSS).
Oficio AD–ATIC–8137–2018	24 de septiembre de 2018	Oficio de Advertencia sobre la gestión efectuada en el cumplimiento de los planes remediales para la gestión de vulnerabilidades y riesgos en TIC de la CCSS.
Oficio No. 9125	8 de octubre de 2018	Resultado informe denominado “Evaluación de carácter especial sobre la gestión efectuada en el cumplimiento de los planes remediales del Análisis Integral de Vulnerabilidades y Riesgos en TIC de la CCSS.
Oficio No. 11069	20 de diciembre de 2018	Oficio de información sobre aspectos relacionados con la Seguridad de la Información Institucional”. (Se resume un conjunto de productos realizados por este Ente Fiscalizador referente al tema).
Informe de Auditoría ATIC-246-2018	21 de diciembre de 2018	Gestión de la Gerencia de Pensiones en el cumplimiento a las Normas de Seguridad Informática Institucional.
Oficio AI-2328-2019	9 de agosto de 2019	Dispositivos móviles institucionales.

Informe / Oficio No.	Fecha	Asunto
Oficio AD-ATIC-271-2020	5 de febrero de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
Oficio 292	15 de febrero de 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, 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-896-2020	22 de abril de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1239-2020	20 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1322-2020	25 de mayo de 2020	Controles de acceso y niveles de seguridad en equipos de tecnologías de información y comunicaciones (TIC).
AD-ATIC-1512-2020	29 junio de 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-2062-2020	13 de agosto del 2020	Oficio de asesoría respecto al uso de VPN en la CCSS.
AI-202-2021	28 de enero del 2021	Oficio que refiere a los resultados de una revisión sobre el tema de “Amenazas de Correo Electrónico”, con el objetivo de fortalecer el uso del correo electrónico bajo los principios de eficiencia, eficacia, ordenamiento jurídico y técnico.
AI-573-2021	11 de marzo del 2021	Oficio respecto a vulnerabilidad en Microsoft Exchange Server
AI-608-2021	15 de marzo del 2021	Oficio en el cual se emiten recomendaciones ante la exposición al ataque cibernético denominado “Solar Winds”
AS-ATIC-674-2021	24 de marzo del 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-2298-2021	1 de noviembre del 2021	Oficio de Asesoría respecto a los tipos de amenazas que afectan a las organizaciones por medio del accionar de los ciberdelincuentes.
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-2503-2021	30 de noviembre del 2021	Oficio de asesoría respecto a la preparación de los sistemas de información para la prevención al fraude.
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

OBSERVACIONES

Así las cosas, es menester de este Órgano Fiscalizador hacer un recordatorio a esa Administración sobre la importancia de mantenerse alerta ante el constante aumento de ataques maliciosos que buscan sustraer datos sensibles u ocasionar otros daños.

En ese sentido, algunas recomendaciones basadas en las mejores prácticas para atender el escenario actual son:

Sobre los incidentes recientes

Ante los hechos evidenciados, la Institución se vio afectada por ataques de hackers y particularmente debe gestionar acciones correctivas y preventivas, considerando al menos los siguientes elementos:

- Garantizar la adecuada gestión de contraseñas, esto incluye el cambio las mismas, no utilizar dicha contraseña para diferentes sitios, estructurarlas mediante secuencias de caracteres complejos (incentivando contraseñas robustas, que no sean rastreables), activar factores de doble autenticación.

  Además, redoblando esfuerzos en concientizar a los usuarios al evitar dejar sesiones abiertas en los navegadores; no abrir enlaces sospechosos; mantener los sistemas actualizados y monitorear minuciosamente el comportamiento de equipamiento o software con nivel de obsolescencia tecnológica; identificar tráfico inusual; entre otras previsiones de seguridad.

  Lo anterior, en apego a lo establecido en las Normas Institucionales de Seguridad Informática, TIC-ASC-SEG-0002, versión 1.0 de abril 2008, en la cual se detalla un conjunto de políticas de control de acceso a los recursos institucionales, específicamente los incisos 6.1 "*Normas para la política correcto uso de contraseñas de parte de los usuarios de red y Aplicaciones*" y 6.6 "*Normas para la política de confidencialidad de la información institucional y trato con terceros.*"

- Generar informes forenses para determinar las causas del incidente, consecuencias y costo de la afectación a nivel económico y reputacional que apoyen la toma de decisiones en los diferentes niveles organizacionales.

  Lo anterior, para determinar la ruta a seguir en la mitigación del riesgo, identificar la filtración de datos, restablecimiento del servicio, implementación de estrategias de ciberseguridad y prevención del fraude, identificación de responsabilidades, ajustes a los procesos o procedimientos, así como otros elementos a incluir dentro del plan de acción.

- Verificar las autorizaciones de acceso a redes sociales y/o sistemas de información a nivel institucional, de manera que se establezcan roles y responsabilidades formalmente definidos, orientados al manejo de esas plataformas de comunicación, particularmente incluyéndose lo correspondiente a los mecanismos de seguridad, el cumplimiento de normas, así como otros aspectos propios del asunto.

Exposición a ciberataques de diferente índole

Tras el aumento de la digitalización y automatización de los procesos a nivel organizacional, los líderes y usuarios finales de sistemas, donde se gestiona información, deben asumir las condiciones propuestas por el entorno tecnológico, el cual incluye la exposición a amenazas cibernéticas (riesgo implícito al utilizar las tecnologías).

Tal y como lo expone el Máster Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para América Latina en Kaspersky, en la publicación del 18 de noviembre del 2021, titulada "Pronóstico de ciberamenazas 2022 para América Latina", mencionando:

"El cibercrimen está en constante evolución, por ende, ni las empresas ni los consumidores pueden bajar la guardia. Estemos en pandemia o no, los atacantes están siempre atentos a las últimas tendencias y tecnologías para enganchar al mayor número de víctimas. Sin embargo, hemos notado que los ataques han pasado de ser básicos y masivos a más complejos y selectivos, lo que nos da a entender que los cibercriminales están afinando sus tácticas y procedimientos para evitar dar golpes al aire"

No obstante, el incremento de amenazas de seguridad es abrumador, lo cual pone sobre la palestra la necesidad inminente de acatar recomendaciones básicas en primera instancia, para abordar la exposición a vulnerabilidades, entre ellas

- Ser vigilante del cumplimiento del marco normativo que refiere a seguridad TI y de la información, así como de los marcos de referencia o estándares de calidad aplicables.
- Identificar los activos críticos que necesitan protección inmediata.
- Mantener actualizado el software vinculado a la plataforma tecnológica principal y equipamiento local.
- Estar informado de las vulnerabilidades descubiertas en el hardware o software y que puedan ser un fallo de seguridad o generar oportunidades para los ciber atacantes.
- Verificar la eficiencia y eficacia de los planes de contingencia, continuidad, realización respaldos y pruebas, entre otros elementos.
- Generar informes expeditos con el análisis de la causa, impacto y la activación del correspondiente plan de acción (detallándose actividades, plazos y responsables) para mitigar la exposición al riesgo en el menor tiempo posible.
- Si una vulnerabilidad es descubierta activar de forma inmediata el plan de acción a nivel interno y en caso de existir un tercero involucrado o contratado, acercarse al proveedor o fabricante del servicio o equipo para conocer sus recomendaciones, precauciones y demás acciones que aporten valor a la organización.
- Activar y/o preparar un plan de recuperación, previendo que, en caso de presentarse un desafortunado desastre, la organización disponga de un proceso documentado para evaluar los daños, reparar sistemas, equipos y restablecer sus operaciones.
- Previo al restablecimiento de los servicios afectados, verificar la eliminación de rastros secundarios del ataque; efectuar pruebas de penetración en los servicios, aplicaciones, código fuente, bases de datos o infraestructura de red del cliente; lo anterior, para tener la certeza de haber mitigado el riesgo.
- Mantener al personal informado y/o capacitado sobre como atender los temas relacionados con ciberseguridad.
- Solicitar la integración de niveles superiores para la adopción de recomendaciones aplicables a la CCSS y advertir al grupo de involucrados en materia de ciberseguridad la necesidad de doblar esfuerzos.

De esa forma, estos puntos aunados a otros de carácter estratégico y técnico permitirán enfrentan el panorama de amenazas cambiante y creciente que hoy en día demanda un plan de ciberseguridad sostenible a largo plazo, con un enfoque holístico de seguridad para protegerse tanto de los ataques dirigidos intencionadamente, como de los errores humanos de procedencia interna.

Lo anterior, con el objetivo de responder adecuadamente a las amenazas inherentes a la gestión de las TI y del negocio, esto basado en el tratamiento continuo de riesgos y considerando el marco normativo que le resulte aplicable para garantizar la continuidad razonable de los procesos y ante una eventual interrupción no se vea afectados significativamente los usuarios.

Tal y como se cita en el marco de referencia COBIT 5 (Objetivos de Control para las Tecnologías de Información), en la descripción del proceso DSS04, DSS04.02 y DSS04.04, a saber:

"establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.".

(…) evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción.".
(…) probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera.".

Fuentes de información en materia de ciberseguridad

En atención a la disposición de herramientas que permitan identificar tendencias o recomendaciones afines con la ciberseguridad, se comparte a manera de ejemplo los anexos citados a continuación:

- Anexo 1: Publicación emitida por la empresa Forcepoint, especializa en ciberseguridad, comparte las predicciones y los desafíos en esta área para el 2022.
- Anexo 2: Artículo expuesto por la empresa Kampersky, especializa en ciberseguridad, con el detalle del pronóstico de ciberamenzas 2022 para América Latina.
- Anexo 3: Resultados de estudio, realizada por KPMG a más de 600 directivos en múltiples industrias de la región, confirma la evidencia anecdótica de los efectos de la pandemia sobre estas tres amenazas interconectadas, revelando que el fraude, los problemas de incumplimiento y los ciberataques son comunes, pero graves, y se espera un aumento en la frecuencia de incidentes.

Lo anterior, con el objetivo de informarse, investigar y planificar sobre la necesidad de adoptar prácticas que busquen un tipo de inmunidad para administrar, resistir y luego poder responder a ataques o interrupciones que se atraviesa a nivel mundial.

En ese sentido, siendo consecuentes con lo indicado en las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en su artículo III "Planificación Tecnológica Institucional", donde se cita:

"La Institución debe instaurar un modelo estratégico formal que permita establecer la dirección organizacional, iniciativas a corto, mediano y largo plazo, incorporando las necesidades y oportunidades tecnológicas que permita establecer los requerimientos al nivel tecnológico para la sostenibilidad de las operaciones institucionales, así como cambio y mejora a los recursos tecnológicos instalados y las oportunidades de crecimiento y entrega de valor público. Adicionalmente, que incorpore indicadores que permitan valorar el nivel de cumplimiento de los objetivos estratégicos, las acciones de revisión y ajuste a la estrategia.

La Unidad de TI debe disponer de un plan de infraestructura e inversiones que permita proyectar los requerimientos de licenciamiento, mantenimiento de infraestructura tecnológica (preventiva, por obsolescencia, mejora), adquisición de nuevos recursos tecnológicos, basados en la línea estratégica institucional establecida. (…)"

Consideraciones finales

Bajo ese contexto, la CCSS no es la excepción y está en un punto donde no hay retorno, nos encontramos en medio de una gran revolución tecnológica, caracterizada por una creciente tendencia hacia la digitalización, aspecto que impacta cada aspecto de los procesos Institucionales.

De esa manera, esos avances conllevan a exponenciales oportunidades, pero también importantes retos, ya que hoy en día cualquier organización con un solo dispositivo conectado al Internet, puede ser víctima de un ciberataque y los atacantes ven esa situación como una oportunidad.

Así las cosas y considerando los antecedentes citados en esta misiva, se debe mitigar la posibilidad de ser potenciales blancos de los cibercriminales; lo cual, hace resaltar la importancia y prioridad de los asuntos relacionados a la ciberseguridad.

En ese sentido, parte del análisis desarrollado en el presente oficio surge con el propósito de informar sobre algunos aspectos relevantes del asunto citado en el epígrafe, pero de manera consensuada se debe examinar todas las aristas y generar acciones orientadas a establecer compromisos para el progreso incremental del tema de marras.

Lo anterior, en apego a lo indicado 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", a saber:

> *"**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."*

Bajo ese contexto, es fundamental que el tema de ciberseguridad sea considerado como parte integral de los sistemas de TI y del negocio dentro de la Institución, porque quizás los ataques recientes no generaron un alto impacto, pero a futuro podría tratarse de datos sensibles en materia de salud, pensiones o recaudación patronal.

En otras palabras, la sofisticación y la escala de los ciberataques seguirán en aumento y se debe planificar para adelantarse a las amenazas, siendo proactivos y no dejando ningún activo sin proteger, o se correría el riesgo de convertirse en la próxima víctima de complejos ataques.

De lo anterior se deriva, la inevitable necesidad de direccionamiento en lo correspondiente a modelos de gobernabilidad TI y seguridad de la información, creación de nuevas infraestructuras digitales, gestión del cambio, entre otros elementos que permitirán a la CCSS generar la maximización de los beneficios y el uso responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación y sostenibilidad de las soluciones tecnológicas.

En virtud de lo expuesto, se previene y advierte a esa Administración con el propósito de que se adopten las medidas pertinentes, a fin de contribuir con la divulgación de información contemplada en este oficio y así contribuir en la mitigación de vulnerabilidades, las cuales deben ser sometidas a valoración y revisión según corresponda.

Finalmente, es relevante manifestar que esta Auditoría se encuentra en la mayor disposición de apoyar la gestión que desarrolle esa Administración ante la temática expuesta, conforme nuestras potestades y competencias.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para la administración del riesgo y atención de la situación comunicada, en el plazo de un mes a partir del recibido de este documento.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.04.21 11:04:23 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/jfrc

Anexos: 1- Forcepoint lanza las tendencias en ciberseguridad para 2022
2- Pronóstico de ciberamenazas 2022 para América Latina
3- Resultados de estudio, realizada por KPMG (Documento adjunto a esta misiva)

C. Doctor Randall Álvarez Juárez, gerente, Gerencia Médica U.P.1100
Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera U.P. 1103
Licenciado Luis Fernando Campos, gerente, Gerencia Administrativa U.P.1104
Doctor Esteban Vega de la O, gerente, Gerencia Logística U.P. 1106
Ingeniero Jorge Granados Soto, gerente, Gerencia Infraestructura y Tecnología U.P. 1107
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia de Pensiones U.P.9108
Licenciada Xinia Fernández Delgado, directora, Dirección de Comunicación Organizacional U.P. 1115
Licenciado Walter Campos Paniagua, director, Direccion Administración y Gestión de Personal U.P.1131
Auditoría

Referencia: ID-73962

Anexo 1

Forcepoint lanza las tendencias en ciberseguridad para 2022

Autor: Adam Bennett
Fecha de publicación: diciembre 15, 2021, 5:11 am CST

Con el año próximo ya a la vuelta de la esquina, Forcepoint presenta sus Future Insights 2022, las proyecciones de lo que nos deparará el futuro en los diversos sectores de la sociedad, teniendo siempre en cuenta el rol que tendrá la ciberseguridad.

Lo cierto es que estamos terminando un 2021 desafiante, en el que se multiplicaron las amenazas, no solo en número, sino también en creatividad y espacios en los que se concretaron. Actualmente todos estamos expuestos, desde los consumidores hasta las grandes corporaciones.

En este sentido, vale la pena preguntarse cuáles serán los sectores que estarán más expuestos al accionar de los ciberdelincuentes y cuáles serán los modos en los que se concretarán los ataques. Para dar respuesta a esto, es que Forcepoint presenta un análisis de cómo se moverá el mercado en 2022:

La seguridad de las áreas de seguridad: Una de las señales de alerta que destacan desde Forcepoint es que los ataques cibernéticos puedan convertirse en un elemento básico de los arsenales militares a partir de 2022. Las herramientas, las técnicas y los procedimientos utilizados en los ataques de ransomware están perfectamente estructurados para lograr convertirse en parte central de estos ciber armisticios, dado que tienen bajo costo y bajo riesgo.

Un detalle sumamente importante es que, al igual que en las ofensivas con armas de fuego, estos ataques también afectan significativamente a las poblaciones, dejándolas vulnerables al privarlas de servicios básicos como electricidad, comida, agua, entre otras cosas.

Ciudades inteligentes: Las ciudades inteligentes serán cada vez más frecuentes, pero también significarán más espacios que pueden ser atacados. A medida que más aspectos de una ciudad tradicional estén conectados a Internet, como el transporte, la iluminación y la gestión de recursos, más riesgo corre esa metrópolis de sufrir un ataque cibernético. Es que la conectividad genera conveniencia para los consumidores de servicios, pero también para los atacantes. Y Si bien existe cada vez más conciencia respecto de esta tendencia, se ha hecho poco por detenerla.

El código abierto requiere la vigilancia de todos: Los proyectos de código abierto siguen creciendo exponencialmente. Es cierto que la seguridad del software de código abierto mejoró drásticamente en la última década, sin embargo, también los ataques a esta cadena de suministro están aumentando a una velocidad alarmante.

Sonatype estimó que en 2021 ocurrieron 12.000 ataques a proyectos de código abierto, lo que representa un incremento del 650% de un año al siguiente. Por lo tanto, es imperativo que tanto en el sector público como en el privado prioricen la seguridad en sus proyectos de código abierto. Un arma clave en la lucha contra las actualizaciones de software maliciosas es abordar la deuda técnica, es decir, la brecha entre lo que se invierte en seguridad y lo que realmente se necesitaría.

El factor humano: En 2022 el trabajo híbrido incrementará, ello obligará a las empresas y colaboradores a delinear nuevas reglas respecto a la ciberseguridad corporativa y personal. Por eso, es necesario apuntar a definir comportamientos deseables para los colaboradores y las tecnologías que utilizan en su día a día laboral, estableciendo cuidadosamente límites y conjuntos de reglas mediante políticas y directrices.

Sin los límites, resulta difícil determinar si un comportamiento inusual o inesperado representa una amenaza a los sistemas o si es completamente normal. Por ejemplo, a las personas que trabajan desde sus casas les resulta casi imposible separar su vida personal de la profesional y pueden acceder a sitios sospechosos sin intenciones maliciosas. Las organizaciones enfocadas en crear arquitecturas de seguridad resilientes entienden que deben comprender y proteger sus activos, así como entender a sus empleados.

Agtech, posibilita y pone en riesgo: En los últimos años el sector agropecuario ha buscado eliminar gastos de mano de obra mediante la automatización, por ende, los productores de alimentos y agricultores indirectamente han cimentado sus empresas en un sistema cada vez más frágil. Y si los últimos años nos han enseñado algo, es que la cadena de suministro es delicada. Estas son muy malas noticias para una industria que enfrenta un punto de presión único con el ransomware: si los sistemas no funcionan, el suministro de alimentos para la mayor parte de la población se paraliza.

Además, es preciso pensar que los hackers pueden aprovecharse de esta automatización para buscar dañar una población en específico o un Estado en un conflicto bélico. También se puede atacar a estos sistemas buscan llamar la atención sobre el consumo de determinado alimento que consideran perjudicial para la salud o el medio ambiente, por ejemplo.

El cambio a la prevención 100 %: Los datos son el sistema nervioso central de una organización. Por eso, al hablar de ciberseguridad las empresas deben reconsiderar el perímetro a proteger, porque éste ahora está en dónde se utilicen los datos, sin importar el lugar físico en el que el colaborador se encuentre.

Las herramientas de análisis son sumamente útiles para ayudar a identificar posibles riesgos, pero todavía es como encontrar una aguja en un pajar. Por este motivo la prevención 100 % se convertirá en la norma a medida que las organizaciones acepten plenamente los principios de Zero Trust (Cero Confianza). ¿A qué nos referimos? Los equipos cibernéticos supondrán que todo es malo, limpiarán todo y garantizarán el acceso con menor privilegio.

Fuente: https://www.forcepoint.com/es/newsroom/2021/forcepoint-future-insights-2022?utm_source=marketo&sf_src_cmpid=7011G000000Kerj&utm_medium=email&utm_content=FutureInsights_2022_EmBlast_ES&mkt_tok=MDE4LU5LRi0wMDgAAAGB991IILIor9xVj25m2aIcFQJrOmJlALGb5fDXBDZkcrJNz0kU5In3pNuDpSABiPxqe07A9UkIZAdi_SlzIBqf8T5Cs9qlS--ixTnixY7lNOOH9_c

Anexo 2

Pronóstico de ciberamenazas 2022 para América Latina

Autor: Hernán Diaz Granados
Fecha de publicación: noviembre 18, 2021

Expertos de la empresa señalan que los cibercriminales serán aún más selectivos, tanto con las herramientas de ataque como con sus víctimas para garantizar ganancias

Es evidente como la pandemia aceleró la adopción de la tecnología durante los últimos 18 meses y como las tendencias que emergieron a raíz de esta impulsaron la adaptación de las tácticas de ataque de los cibercriminales. Sin embargo, a medida que las campañas de vacunación avanzan en la región y se retoman las actividades que solíamos realizar previo al confinamiento, nuestros expertos advierten que los delincuentes cibernéticos han cambiado de rumbo nuevamente, centrándose en herramientas y en aquellas victimas que maximicen sus esfuerzos y ganancias.

“El cibercrimen está en constante evolución, por ende, ni las empresas ni los consumidores pueden bajar la guardia. Estemos en pandemia o no, los atacantes están siempre atentos a las últimas tendencias y tecnologías para enganchar al mayor número de víctimas. Sin embargo, hemos notado que los ataques han pasado de ser básicos y masivos a más complejos y selectivos, lo que nos da a entender que los cibercriminales están afinando sus tácticas y procedimientos para evitar dar golpes al aire“, comenta Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky.

Los pronósticos 2022 de nuestro Equipo de Investigación y Análisis de Kaspersky América Latina para la región son los siguientes:

La consolidación del desarrollo de troyanos bancarios y troyanos de acceso remoto (RATs) para Android. Con el crecimiento y la madurez de la banca móvil, es altamente probable que los grupos cibercriminales que tradicionalmente atacan a los sistemas basados en Microsoft Windows, amplíen su portafolio para incluir implantes móviles. En general, dichos troyanos y RATs serán más sofisticados en cuanto a la madurez del código y también más diversificados en cuanto a sus objetivos.

Los InfoStealers se abrirán un nicho en el mercado cibercriminal de la región. Debido al bajo costo de licenciamiento y amplia disponibilidad de versiones crackeadas, así como la facilidad de uso y la eficacia para recopilar y exfiltrar datos sensibles de sus víctimas, los troyanos infostealers se convertirán en una de las herramientas de ataque preferidas a nivel regional. Los cibercriminales buscan un balance entre sus esfuerzos y ganancias y los infostealers suplirán esta necesidad. Veremos un auge en su uso sin importar las motivaciones finales, ya sean financieras o para la recopilación de información inicial antes de lanzar ataques más complejos.
El Ransomware dirigido será aún más selectivo. La cultura de la región impide que los criminales persuadan a sus víctimas a que paguen por recuperar sus datos cifrados. Por esta razón, este tipo de operaciones no resulta atractiva para los afiliados de Ransomware ya que su objetivo final es hacer que la víctima pague. Al enfrentar esta situación, los afiliados serán más selectivos, centrándose en potenciales víctimas que puedan enfrentar fuertes multas si se llegase a filtrar información personal de sus clientes.

La comercialización exportada de activos. Los cibercriminales, con raíces en Latinoamérica, han aprendido que el mayor provecho que le pueden sacar a los datos robados es vendiendo la información de sus víctimas en las plataformas internacionales donde otros criminales la puedan comprar. Por lo tanto, algunos criminales locales se especializarán en comprometer las redes de sus víctimas, exfiltrar la información sensible y ponerla directamente a la venta en el mercado clandestino, ya sea en inglés u otro idioma.

Exploración y explotación del mercado PoS. Al retomar las actividades habituales previo a la pandemia, el uso de los puntos de pago (PoS) aumentará. Este es un mercado creciente ya que existen varios fabricantes que ofrecen

este tipo de tecnologías a los negocios en general. No obstante, aunque las tecnologías pueden variar, lo que los PoS tienen en común es que son dispositivos con poca seguridad contra los programas de código malicioso y es ahí donde los criminales continuarán apostando. Adicionalmente, los atacantes seguirán buscando oportunidades para explotar los pagos electrónicos realizados desde el celular a través de plataformas digitales.

Intensificación de web skimmers extranjeros en la región. A lo largo de la pandemia, los consumidores de la región se han acostumbrado a realizar compras en Internet, incluyendo víveres y otros artículos de primera necesidad. Varios sitios de comercio electrónico que ofrecen ropa, bebidas, dispositivos electrónicos y otros artículos, serán comprometidos desde el exterior para integrar código malicioso al estilo de Web skimmers (Magecart) con el objetivo de robar los datos de pago de los clientes. Este será un reto para los administradores Web de la región ya que detectar dichas amenazas exige conocer cómo funcionan los códigos maliciosos y saber sus técnicas de ofuscación.

Ataques dirigidos avanzados, principalmente desde el exterior, con el fin de obtener información de terceros y países aliados. Al observar la polarización que existe actualmente a nivel mundial, anticipamos que habrá ataques estilo APT que se dirigirán a las infraestructuras críticas de varios países, aliados del mundo occidental. Dichas agresiones tendrán el objetivo de exfiltrar información de interés para los atacantes, así como para los rivales de países aliados a Latinoamérica.

Fábricas de trolls en redes sociales. Pronosticamos una especie de legitimación en el uso de cuentas tipo trolls o zombie por parte de diferentes actores políticos en el poder y aquellos que buscan llegar al poder. Dicho uso se intensificará durante periodos de elecciones y momentos críticos que atraviesen las sociedades, como conmociones nacionales por sucesos de grandes proporciones.

Estafas con las criptodivisas. Con el aumento de la pobreza y la devaluación de las monedas nacionales, más personas buscarán formas de sobrevivir o de asegurar sus fondos en criptodivisas. Lamentablemente, al no ser expertos en el tema y por cultura, querrán apoyarse en personas y compañías en Internet que les ofrezcan invertir de una manera fácil. Sin embargo, esas compañías captarán los fondos y dejarán a muchos con las manos vacías; si no al comienzo, entonces después de un tiempo de haber pagado las comisiones por las supuestas ganancias. Ataques por medio de códigos QR. En 2021, se identificaron varios ataques por medio de códigos QR, los cuales son cada vez más comunes por sus diferentes usos, entre estos: para publicidad en espacios de transporte público, menús en restaurantes, acceso a promociones o para ubicar tiendas en centros comerciales. Este método de ataque combina la ingeniería social con la facilidad que esta tecnología ofrece a los usuarios para que, desde sus dispositivos móviles, puedan acceder de forma inmediata a sitios web. Sin embargo, en algunos casos, estos pueden contener código malicioso que se descarga e instala en los dispositivos de los usuarios o hasta pueden redireccionar a sitios de phishing donde los cibercriminales roban las credenciales de acceso a diferentes servicios.

“Como en la vida real, el ambiente digital también se está preparando para el mundo ‘hibrido’. Aunque en 2022 presenciaremos ataques que aprovechen tecnologías centradas en esta tendencia, como infecciones a través de los códigos QR y RATs, no hay que subestimar las ciberamenazas que han hecho ruido este 2021, como ataques a criptodivisas y el ransomware”, comenta Bestuzhev. “De hecho, a medida que estos se vuelven más selectivos y complejos, se vuelven más peligrosos, aumentando la probabilidad de altas pérdidas financieras y daños a la reputación de sus víctimas. Si algo hemos aprendido durante estos últimos 18 meses de confinamiento y transformación digital es que tanto empresas como usuarios finales deben contar con un conocimiento básico de ciberseguridad y practicar buenos hábitos digitales. En el caso de las empresas, estas también deben conocer las técnicas y procedimientos de los actores de ataques, contar con una visibilidad técnica en sus redes para identificar a los atacantes por medio de las anomalías en logs, así como con una inteligencia de amenazas accionable”.

Fuente: https://latam.kaspersky.com/blog/pronostico-de-ciberamenazas-2022-para-america-latina/23426/?mkt_tok=ODAyLUlKTi0yNDAAA