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

AS-AAFP-163-2022
27 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
GERENCIA GENERAL-1100

Licenciado
Gustavo Picado Chacón, gerente
GERENCIA FINANCIERA-1103

Ingeniera
Giorgianella Araya Araya, directora
DIRECCIÓN DE SERVICIOS INSTITUCIONALES-1161

Estimados(a) señores (a):

ASUNTO: Oficio de Asesoría sobre alternativa de contratación de seguro para mejorar la ciberseguridad a nivel Institucional.

De conformidad con las potestades y competencias que le confieren a los Órganos de Fiscalización y Control los artículos 21 y 22 de la Ley General de Control Interno, y en cumplimiento de los objetivos fundamentales referentes a la eficiencia, eficacia y buen gobierno de las operaciones, esta Auditoría consiente de la afectación a los Sistemas de Información Institucionales derivada del hackeo el pasado 31 de mayo 2022, expone las siguientes consideraciones, con el propósito de resaltar la importancia de disponer de diversos medios preventivos para apoyar el resguardo de la información de la CCSS ante vulnerabilidades cibernéticas que puedan afectar la prestación de los servicios con calidad y oportunidad.

Es importante mencionar que, desde el ataque cibernético a la Institución, esta Auditoría ha mantenido un seguimiento constante con la emisión de diversos productos, de los cuales recientemente se puede mencionar el oficio AS-AATIC-147-2022 del 19 de julio 2022 “sobre los roles y responsabilidades de ciberseguridad a considerar por la Caja Costarricense de Seguro Social”, que aborda entre otros asuntos los siguientes:

- Todos los niveles estratégico, táctico y operativo tienen un rol fundamental en acatar las medidas y políticas de seguridad para el resguardo de la información Institucional.
- La adaptabilidad de la organización para atender las necesidades en ciberseguridad.
- El seguimiento y supervisión de los requerimientos asociados con los roles y responsabilidades para la seguridad de la información.
- La importancia que las acciones ejecutadas incluyan los mecanismos básicos de control que aseguren la legalidad de las operaciones y acrediten documentalmente los lineamientos y directrices consideradas para dirigir adecuadamente la gestión de negocio.

En ese sentido, se tuvo conocimiento de la publicación sobre un estudio que realizó The Sate of Cyber Resilience[1] publicado el 15 de julio 2022, realizado a empresas de todo el mundo, donde entre sus resultados principales se destacó que un 73% de las compañías encuestadas han sufrido un ciberataque, y han obligado a los responsables de las organizaciones a interesarse en las políticas de ciberseguridad y marcar nuevas estrategias. En dicho estudio se resaltó también el incremento de la contratación de ciberseguros, donde el 61% de las empresas encuestadas mencionaron que tienen contratada una cobertura de seguros, siendo que este dato reflejó un incremento del 30%, con respecto a los resultados del estudio del 2019 que realizó la misma compañía.

Adicionalmente, la Promotora del Comercio Exterior de Costa Rica (Procomer) publicó el 23 de mayo 2022, en el estudio[2] "Caracterización del uso y necesidades potenciales de ciberseguridad en empresas costarricenses", donde menciona que siete de cada diez empresas costarricenses (73%) ha invertido o invierte actualmente en la ciberseguridad, además, en ese estudio se destacó que existe una población critica de empresas que equivale al 8% de la muestra, que a pesar de que no han gastado en ciberseguridad, tampoco contempla hacerlo en el corto plazo, es decir, resultan los más vulnerables y expuestos ante amenazas de seguridad. Uno de los aspectos relevantes que menciona este estudio, se detalla a continuación:

> *"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".*

En esa línea como parte de la Ciberseguridad, en el mercado surgen alternativas para administrar este tipo de riesgos relacionados con la seguridad de datos como, por ejemplo; el tema de ciberseguros, que cada vez despierta más interés por parte del sector asegurador y que es una alternativa que puede ser analizada a partir de una valoración costo-beneficio en función de las necesidades de la institución, procurando compartir el riesgo a través de la compra de contratos de seguro.

A partir de lo expuesto, con respecto a los ciberseguros como parte de la estrategia de seguridad, un experto en CISO de AGBAR Iberoamérica[3], opina que "un ciberseguro es algo complementario, es un servicio que minimiza el impacto económico en caso de un incidente de seguridad y por esto es útil sumarlo a la estrategia de seguridad, pero no reemplaza la inversión en seguridad. Además, señala que otro aspecto a considerar son las alzas en el valor en la contratación del seguro, por la alta demanda en el último tiempo con el aumento de víctimas de este tipo de amenazas desde la pandemia del 2020".
Esta opción podría constituirse en una alternativa para administrar riesgos crecientes en materia de Ciberseguridad, considerando que en el artículo 14 de la Ley General de Control Interno, referente a las obligaciones de la Administración activa en cuando a la gestión de los riesgos, se establece lo siguiente:

[1] https://cybersecuritynews.es/el-incremento-de-ciberataques-aumenta-la-contratacion-de-ciberseguros/
[2] https://www.procomer.com/noticia/
[3] La persona responsable de velar por la ciberseguridad de una empresa es el CISO (Chief Information Security Officer). También podemos conocerlo como director de seguridad de la información. Esta persona es la que se encarga de proteger la información ante posibles ciberataques y fugas de datos.

"Artículo 14.-Valoración del riesgo. En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:

a) Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.

b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.

c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.

d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar."

Así como, lo señalado en las Normas técnicas para la gestión y el control de las Tecnologías de Información versión 1.0, del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) en los numerales IV y XI:

"IV. GESTIÓN DE RIESGOS TECNOLÓGICOS

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."

"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".

Finalmente, debido a que los ataques cibernéticos han incrementado, es fundamental buscar alternativas que estén enfocadas en la innovación y apoyen las Mejores Prácticas de Buen Gobierno Corporativo, bajo un enfoque orientado a riesgos, aspecto que debe ser debidamente abordado a nivel Institucional por la alta Gerencia para una adecuada implementación de controles que permitan una gestión robusta minimizando el impacto sobre los objetivos institucionales.

Debido a lo anterior, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, se informa a esa Administración Activa, para que realice una valoración de los aspectos señalados, y se fortalezcan las medidas de control interno en cuanto al análisis de alternativas para disminuir los riesgos relacionados con la seguridad informática, desde el punto de vista de que estos riesgos puedan en parte ser transferidos a un tercero siempre y cuando se dispongan de condiciones de costo-beneficio favorables para la Institución.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)
Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.29 16:56:00 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/ACC/EMVG/FZC/lbc

C. Máster Idannia Mata Serrano, subgerente a.i., Dirección de Tecnologías de Información y Comunicación -1150.
Licenciada Auxiliadora Villalta Gómez, jefe, Área Control de Activos, Dirección de Servicios Institucionales -1161.
Auditoría