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

AS-AATIC-168-2022
17 de agosto de 2022

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
Luis Fernando Campos, gerente
GERENCIA ADMINISTRATIVA - 1104

Doctor
Esteban Vega de la O, gerente
GERENCIA LOGÍSTICA - 1106

Ingeniero
Jorge Granados Soto, gerente
GERENCIA DE INFRAESTRUCTURA Y TECNOLOGÍAS - 1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES – 9108

Estimados señores:

ASUNTO:	**Oficio de Asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento.**

Esta Auditoría, en cumplimiento de las actividades preventivas y de asesoría consignadas en el Plan Anual Operativo, para el período 2022 y con fundamento en lo dispuesto en los artículos 21 y 22 de la Ley General de Control Interno, brinda asesoría sobre la protección de datos adaptable al riesgo con un enfoque basado en el comportamiento, a fin de que sea valorado para la correspondiente toma de decisiones por parte de esa Administración.

Es de conocimiento que, en atención a la normativa aplicable, la organización debe garantizar de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Lo anterior máxime al considerar el contexto actual de la CCSS, particularmente, brindando énfasis a los ataques cibernéticos recientes y que aún afectan la dinámica habitual de los procesos institucionales.

1. GENERALIDADES Y ANTECEDENTES

1.1. Términos y definiciones

En Costa Rica el derecho a la protección de datos se regula y se protege a través de diferentes normativas, entre ellas las más importantes:

- La Constitución Política en su artículo 24. Derecho a intimidad, libertad y secreto de comunicaciones.
- Ley No. 8968 – Protección de la Persona frente al tratamiento de sus datos personales y su respectivo Reglamento No. 37554-JP.
- Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor - No 7472.
- Ley General de Telecomunicaciones No. 8642.
- Artículo 47 Código Civil: derechos y usos de imagen personal.
- Artículo 196 bis Código Penal: tutela el bien jurídico de datos personales a través de la sanción de tres años para quienes vulneren la intimidad de otra persona, es decir, que sin sus consentimientos se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino mensajes, datos e imágenes contenidas en medios electrónicos, informáticos, magnéticos y telemáticos.
- Artículo 615 Código de Comercio. “Secreto Bancario”.

Dentro de las definiciones que estipula la citada Ley No. 8968 y su reglamento, con respecto datos personales y su categorización, se encuentran las siguientes.

- **Datos Personales:** cualquier dato relativo a una persona física identificada o identificable.
- **Datos Personales de Acceso Restringido:** los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública.
- **Datos Personales de Acceso Irrestricto:** los contenidos en bases de datos públicas de acceso general, según dispongan leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.
- **Datos Sensibles:** referente al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.

Otros conceptos relacionados con la protección de datos señalan:

- La Real Academia Española, lo define como: el "Sistema legal que garantiza la confidencialidad de los datos personales en poder de las Administraciones públicas u otras organizaciones".
- El diccionario panhispánico del español jurídico cita "Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".
- En la actualidad es una función que está regulada por Ley y que persigue la preservación de la confidencialidad, integridad y disponibilidad de la información para el titular de esta.
- Es el procedimiento mediante el cual se busca prevenir la pérdida o recopilación de información; su concepto hace referencia a la protección o respaldo de datos, con el objetivo de evitar pérdidas, también comprende la recuperación de ellos en caso de que la situación lo amerite.

1.2. Productos de Auditoría

De conformidad con lo anterior, este Órgano de Control y Fiscalización, ha generado una serie de productos a la Administración Activa, con el propósito de garantizar el cumplimiento de lo estipulado en la normativo aplicable. En el informe ATIC-83-2018, del 27 de julio 2018, se evidenciaron debilidades y oportunidades de mejora en atención de ese marco legal en la institución, recomendando el establecimiento de un modelo de gestión integral de datos, en el cual se valorará:

- Definición de unidades institucionales a cargo del tema.
- Definición de roles y responsabilidades concretas según el ámbito de competencia.
- Mecanismos de coordinación entre los diferentes niveles de la organización.
- Elaboración y actualización de marcos normativos institucionales asociados a la Ley 8968 y su reglamento.
- Establecimiento de instancias y/o funcionarios encargados del monitoreo y seguimiento integral al cumplimiento de las acciones indicadas en la recomendación 3 del presente informe.
- Capacitación a nivel Institucional para los usuarios que participan en el tratamiento de datos personales, en torno a la aplicación de la Ley 8969 y su reglamento.
- Alineamiento con las iniciativas ejecutadas por la DTIC a través de la Licitación Abreviada No. 2016LA-000003-1150 "Diseñar e implementar el Modelo Meta de Gobierno de TIC y Gobierno de la Seguridad de la Información para la CCSS", lo anterior en lo que respecta a seguridad de la información en cumplimiento del marco normativo analizado en el presente informe.
- Revisión y actualización de los convenios firmados entre la CCSS e instituciones gubernamentales o empresas privadas para el acceso de información contenida en las bases de datos institucionales que contienen datos personales.

Así mismo, se señaló la necesidad de ejecutar las acciones correspondientes para elaborar un inventario institucional de todas las bases de datos que resguardan datos personales y efectuar las gestiones correspondientes para garantizar:

- Definición formal de los indicadores que deben considerarse en la clasificación de bases de datos según lo dispuesto en la Ley No. 8968.
- Categorización de las bases de datos que son internas y las que pertenecen al ámbito de aplicación de la Ley 8968, de acuerdo con lo establecido en atención del punto anterior. Al respecto, debe existir justificación suficiente, competente y pertinente sobre las bases de datos que resguardan datos personales y no forman parte del alcance del marco normativo analizado en el presente informe.
- Designación formal del responsable de cada base de datos, los encargados y el intermediario tecnológico, lo anterior en concordancia con las definiciones estipuladas en el reglamento a la Ley 8968.

Adicionalmente, se instruyó en su oportunidad, para que, a cada uno de los responsables en alineamiento al modelo de gestión establecido, ejecuten las acciones correspondientes, en aras de garantizar el cumplimiento de todas las funciones descritas en los artículos del Reglamento a la Ley 8968, a saber:

- Medio y forma de comunicación electrónica para facilitar a los titulares el ejercicio de sus derechos (artículo 16).
- Procedimientos para la inclusión, conservación, modificación, bloqueo y supresión de datos personales (artículo 27).
- Mecanismos o procedimientos establecidos para comunicar a los encargados, las obligaciones en el tratamiento de bases de datos personales (artículo 31).
- Protocolos mínimos de actuación elaborados para la recolección, almacenamiento y el manejo de los datos personales. (artículo 32).
- Medidas de seguridad, administrativas, físicas y lógicas implementadas por el responsable para la protección de datos personales (artículo 34)

Finalmente, se recomendó en el informe que una vez identificadas las bases de datos ubicadas dentro del ámbito de aplicación de la Ley 8968, se instruyan a los responsables para ejecutar las gestiones correspondientes, a fin de inscribir dichos repositorios ante la Agencia de Protección de los Habitantes según los términos solicitados.

Por otro lado, en el oficio AS-AATIC-107-2022 del 22 de junio de 2022, se informó a las Gerencias, sobre el tratamiento de los datos personales y las medidas de seguridad como consecuencia de los ataques cibernéticos generados a la institución, considerando necesario que al amparo de las acciones señaladas en el informe ATIC-83-2018 e implementadas por la Administración, se activara a la brevedad las medidas requeridas de acuerdo con las responsabilidades respectivas de cada Dirección y Unidad institucional según los aplicativos afectados, lo anterior con el fin de garantizar el cumplimiento normativo, así como la protección de los datos personales administrados por la Caja Costarricense de Seguro Social de la población usuaria.

1.3. Contexto institucional

En virtud de lo anterior, la institución -el 31 de mayo 2022- fue víctima de uno de los principales ataques cibernéticos presentado en el país por sus efectos, así lo destacó el diario “La Nación”, titulando “Nuevo hackeo’ en CCSS afecta atención en hospitales y EBAIS por desactivación del EDUS”, a saber:

> *"La Caja Costarricense de Seguro Social (CCSS) sufrió un nuevo hackeo la madrugada de este martes 31 de mayo, el cual obligó a desactivar todos los sistemas informáticos de la entidad de manera preventiva (…)".*

Ese mismo día, las autoridades de la Caja Costarricense de Seguro Social (CCSS) informan formalmente a la prensa que el hackeo registrado fue "excepcionalmente violento" y el Dr. Álvaro Ramos Chaves, presidente ejecutivo de la Institución, hizo el siguiente llamado ante dicho acontecimiento, citando:

> *"Pedimos paciencia porque tenemos mucho trabajo por delante. La gente razonablemente se ha acostumbrado a la agilidad con la que podemos hacer las cosas cuando tenemos recursos digitales, pero tendremos que recurrir por unos días al papel. Este fue un intento muy violento de vulnerar bases de datos, los sistemas de la Caja, tenemos que pedir paciencia en ese sentido".*

En línea con lo anterior, el Dr. Ramos insistió en que no fueron los hackers los que cerraron las bases de datos ni apagaron los sistemas, mencionando la medida tomada a nivel interno de la CCSS:

> *"Fuimos nosotros mismos, eso que quede muy claro, para que los hackers no pudieran acceder a ella. Naturalmente no tenemos certeza absoluta de que no haya exfiltración de una parte parcial de estos datos, pero estamos bastante confiados en que no fue así. Nuestros datos preliminares es que no pudieron sacar esa información, con una investigación profunda terminaremos de saberlo con certeza".*

Por su parte, el diario La República, esa misma fecha, publicó "Hackers tenían como objetivo el robo de información y las bases de datos de la Caja", según el siguiente detalle:

> *"Robar las bases de datos, así como otra información de la Caja y de los asegurados eran los objetivos de los hackers, según confirmó hoy el Ministerio de Ciencia y Tecnología, que ha trabajado con esta institución afectada por el ataque.*
>
> *La violación de los sistemas informáticos, que se realizó en horas de la madrugada, fue considerada como "especialmente violenta y devastadora", tanto en los servidores físicos, como en la nube".*

Asimismo, el 2 de junio 2022, nuevamente el diario la Nación publicó que los "'Hackers infiltraron la CCSS desde febrero", donde se amplía con mayor precisión la afectación dada en el equipo tecnológico de la CCSS e incrementa el riesgo de robo o daño de información sensible, indicando:

> *"Todos los indicios apuntan a que los hackers empezaron a gestar su ciberataque a los sistemas de la Caja Costarricense de Seguro Social (CCSS) desde febrero, pues, desde ese mes, en la llamada Internet oscura ("dark web"), comenzaron a ofrecer accesos a los sistemas informáticos de la entidad, reveló el presidente ejecutivo, Álvaro Ramos Chaves, al admitir que el daño es mayor al que calcularon el martes.*

Se sospecha que el "software" hostil que inyectaron los extorsionadores entró por alguna terminal o computadora y logró infectar a otras 9.000 (22%) de las 40.000 unidades que tiene la institución. También logró penetrar no a 30, como se dijo inicialmente, sino a 800 servidores (53%) de los 1.500 que tiene la CCSS y, ya una vez adentro, asestó el zarpazo final este 31 de mayo cuando se activó y alteró los sistemas".

En síntesis, la CCSS fue expuesta a un incidente de ciberseguridad, por el cual a la fecha no es posible el restablecimiento de toda su plataforma tecnológica, en virtud de la afectación a la continuidad en la operación de los componentes tecnológicos, e interrupción de sistemas de información que gestionan información y dan soporte a los servicios de salud, pensiones y prestaciones sociales; comprometiendo, además, los datos generados y registrados a través de los sistemas de información.

2. OBSERVACIONES

Esta Auditoría Interna se refiere al argumento citado en el epígrafe, con el objetivo de que esa Administración valore el contenido de la información que se brinda, en la definición de estrategias ante los eventos recientes y futuros. Lo anterior, dada la importancia que reviste la protección de datos y el impacto ocasionado a raíz de los ataques cibernéticos perpetrados a nivel institucional y posiblemente reiterativos.

Es así como Forcepoint, líder en ciberseguridad de protección de datos y usuarios a nivel mundial, hace de conocimiento una serie de observaciones con el objetivo de valorar el cambio de paradigma de ciberseguridad a través de la protección de datos adaptable al riesgo, ya sea que se busque salvaguardar los datos, obtener visibilidad del uso de la metodología de "software como servicio" (SaaS) o evitar que el software malicioso (malware) ingrese a la organización, tal y como se describe a continuación:

2.1. La ciberseguridad basada en el comportamiento

La ciberseguridad basada en el comportamiento del usuario en la interacción con los datos, le permite a la organización identificar, cuantificar y responder proactivamente al riesgo asociado a datos críticos del negocio, considerando que estos datos pueden estar en el nivel central, regional o local, en el hogar de los funcionarios o en la nube.

De esa forma, la metodología calcula continuamente la inseguridad y evalúa constantemente si el usuario o el dispositivo actúan como se espera o se encuentra en una situación comprometida. Cuando la calificación del riesgo de comportamiento alcanza el movimiento crítico, y el modelo predice que una fuga de datos está por suceder, la seguridad adaptable al riesgo aplica automáticamente políticas de bloqueo proporcionales al peligro y a la confidencialidad de los datos.

2.2. La protección de datos adaptable al riesgo, utilizando indicadores de comportamiento

La protección de datos adaptable al riesgo con un enfoque basado en el comportamiento requiere de un cambio hacia el uso de indicadores de comportamiento (IoB). El uso de IoB es un enfoque de monitoreo que analiza las actividades de los usuarios en distintos canales para entender la intención detrás de un incidente señalado. Los IoB son clave para adelantarse a la pérdida en lugar de confiar únicamente en los indicadores de compromiso (IoC) reactivos.

2.3. La prevención de pérdida datos o Data Loss Prevention (DLP)

El disponer de un control sobre los datos que vaya más allá de las defensas de protección perimetrales, extendiendo la seguridad proporcionada por un dispositivo DLP, permite bloquear la salida de información sensible de la organización vía correo electrónico y otros medios. Complementar un DLP o similar, con seguridad centrada en los datos, permite extender la vigilancia aun fuera de la red institucional, aunque esta haya sido descargada de una determinada nube.

En esa misma línea, el Centro Criptográfico Nacional (CCN) de España, mediante artículo "Ventajas de un enfoque de seguridad centrado en los datos", publicado el 7 de febrero 2021, establece sobre los beneficios de este tipo de métodos, lo siguiente:

Evita fugas de datos derivadas de acciones inapropiadas por parte de funcionarios, ya sea de forma accidental o maliciosa, la información viaja protegida y sólo los usuarios que tengan permisos sobre la misma podrán acceder a ella. Un usuario puede trabajar con la misma, pero puede no tener permisos para desprotegerla.

Facilita la colaboración segura, haciendo que la información se comparta con terceros protegida y bajo control, Se pueden compartir documentos confidenciales con un tercero, pero garantizar que su propietario sigue siendo el dueño de estos y en su caso, auditar su uso.

Ayuda al cumplimiento de regulaciones de protección de datos, regulaciones como Ley No. 8968, obligan a la institución a tener los datos personales de terceros controlados, cifrándolos y auditando su uso, independientemente de dónde se encuentren.

Protege frente a brechas de seguridad en la red que supongan una posible fuga de datos, por ejemplo, en ataques de tipo ransomware, donde se escape información y se amenaza con la publicación de estos datos, si están protegidos y cifrados, aunque se exfiltren, el atacante no podrá utilizarlos para extorsionar con su publicación.

El enfoque de una herramienta de seguridad centrada en los datos permite que la información de la institución viaje protegida y bajo control en todo momento. De esta forma, se puede tener una trazabilidad completa de acciones sobre la misma.

3. CONSIDERACIONES FINALES

Una vez descrito lo anterior, y considerando el futuro que depara la protección datos para las organizaciones, especialmente para la institución, producto del crecimiento vertiginoso de ataques cibernéticos que buscan robar o secuestrar información, es fundamental para las autoridades –mediante un análisis de riesgos continuo- evaluar soluciones o metodologías, que se adapten a las necesidades actuales, pensando en el volumen y la criticidad de los datos que administra la CCSS.

Proteger todos esos datos cada vez es más difícil y, por eso, en la actualidad, el mayor desafío al que se enfrentan las Gerencias, Unidades y la Dirección de Tecnologías, es la complejidad de llevar los procesos de almacenamiento antiguos a la modernidad con el menor impacto posible. Anteriormente, el enfoque de la protección consistía en guardar la información en caso de que sucediera algo. Ahora, el accionar actual trata de prevenir proactivamente factores adversos en los sistemas de almacenamiento, antes de que ocurran, mediante actualizaciones de rutina, mejor tecnología y análisis predictivo, esto en aras de disponer de soluciones capaces de aportar valor cuando se presenten amenazas contra los datos de la organización, de manera que podamos adelantarnos a la pérdida y a la actividad maliciosa con la oportunidad requerida.

Los encargados de seguridad de la información enfrentan cada vez más retos derivados de las limitaciones presentes en un enfoque basado únicamente en la seguridad perimetral, que pareciera actualmente no ser suficiente con tenerla protegida en un servidor dentro de la red, la realidad refiere a mantener la defensa incluso aunque haya salido de la esfera de la organización y esté en manos de un tercero.

Es así como la visibilidad juega un papel fundamental en esta operación, existen diferentes herramientas para monitorizar el acceso a determinadas aplicaciones o dispositivos, la organización deberá controlar quien ingresa a los datos independientemente donde se encuentren y los intentos por parte de personas que no deberían tener privilegios cuando estos ya han sido enviados a un tercero, o están en un equipo no controlado por la organización.

Dentro del perímetro de seguridad de la organización, se pueden bloquear a determinados equipos o aplicaciones por parte de usuarios internos, pero se deberá garantizar lo mismo con la información institucional distribuida fuera de la organización o de las aplicaciones y la de los usuarios en sus equipos. Lo acelerado del trabajo hace que el volumen de datos sensibles en formato digital sea cada vez más, sin embargo, el procedimiento no es poner barreras a la agilidad de las operaciones, sino ser capaz de detectar cuando está en riesgo y poder tomar acciones inmediatas para evitar una posible fuga, el tiempo de respuesta ante un incidente de seguridad es vital.

Existe una gran diferencia en una organización entre lo que la gente puede hacer y lo que realmente hace. La seguridad es normalmente vista por los usuarios como un freno al negocio, por eso es fundamental intentar no bloquear los flujos de trabajo normales y permitirles seguir trabajando con sus herramientas habituales, pero controlando en todo momento que el nivel de seguridad es adecuado.

El reto es reducir las brechas que los proyectos de transformación digital generan, un buen camino para hacerlo es apoyándose en herramientas que agilicen y simplifiquen la protección de los activos críticos de la organización.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, dentro de los procesos del marco de gestión de TI, en lo correspondiente a:

> "*Gestión de TI"*
>
> *"(…) Investigación sobre tecnologías emergentes que permitan a través de su eventual incorporación, la innovación y mejora continua al nivel institucional para el logro de los objetivos y la entrega de valor público (…).*

"Seguridad y Ciberseguridad"

(...) 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 (…)."

Finalmente, esta Auditoría informa sobre lo anterior con el objetivo de que se analice la información expuesta y se profundice en el tema de así requerirlo, recordando la necesidad de implementar medidas de seguridad en cuanto a la protección de datos, considerando adicionalmente alternativas de ciberseguridad como la que se planteada en el presente documento, de forma tal, que se reduzca la posibilidad en la materialización de riesgos asociados con el tratamiento de los datos personales e información de la gestión institucional, en cumplimiento del marco normativo.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.08.17 21:27:46 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OCHA/lbc

C. Máster Idannia Mata Serrano, subgerente a.i., Dirección de Tecnologías de Información y Comunicaciones - 1150.
Auditoría