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

AS-AATIC-184-2022
1 de septiembre de 2022

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

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

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

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

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

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

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

Estimados (a) señores (a):

ASUNTO:	**Oficio de Asesoría sobre la importancia del desarrollo seguro de sistemas y aplicaciones institucionales.**

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, se procede a asesorar sobre la importancia de desarrollo seguro de aplicaciones y sistemas institucionales, a efectos de disminuir el nivel de riesgo que eventualmente podrían generarse en las operaciones institucionales a raíz de los constantes ataques cibernéticos a la infraestructura tecnológica, como los materializados desde el 31 de mayo de 2022 que provocaron su desconexión de manera preventiva, así como aquellos que puedan ejecutarse en el futuro, dada la implementación de nuevas amenazas por parte de los ciberdelincuentes.

I. SOBRE EL CIBERATAQUE DEL 31 DE MAYO DE 2022

El 31 de mayo de 2022, se registró en horas de la madrugada un ciberataque contra los servidores de la C.C.S.S., el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

Como resultado de lo anterior y como medida de contención del ataque, se procedió a la desconexión de los sistemas como el Expediente Digital Único en Salud (EDUS), Sistema Central de Recaudación (SICERE), Portal Web, Sistema de Farmacia (SIFA), entre otros, además del apagado de los equipos de usuario final conectados a la red institucional, con la finalidad de proceder al diagnóstico de las afectaciones.

Adicionalmente, mediante oficio GA-CAED-0260-2022 del 02 de junio de 2022, suscrito por el Dr. Mario Vílchez Madrigal, director a.i., del Centro de Atención de Emergencias y Desastres, comunicó al cuerpo gerencial, directores de sede, directores de red integrada de servicios de salud, directores regionales de sucursales, directores generales y administrativos financieros de hospitales y directores y administradores de área de salud, la declaratoria de estado de emergencia institucional por los ciberataques, en lo que interesa indicó:

> *"(…) Procede a Validar el Estado de Emergencia Institucional, debido a los ciberataques sufridos por la Caja Costarricense de Seguro Social el 31 de mayo del 2022. De manera que, se solicita a todas las instancias aplicar las medidas necesarias para la atención de esta emergencia. Se instruye a mantener en operación los Centros Coordinadores de Operaciones Central, Regionales y Locales y aplicar los mecanismos de excepción requeridos para la continuidad de los servicios. La Dirección de Presupuesto y el CAED informarán el procedimiento excepcional que se utilizará mientras los sistemas institucionales de TI sigan desconectados, mediante el cual se aplicará el Procedimiento para la gestión de la Reserva de Contingencia del Seguro de Salud (de la Caja Costarricense de Seguro Social)."*

II. SOBRE EL DESARROLLO DE APLICACIONES SEGURAS

La seguridad de las aplicaciones[1] es una disciplina que agrupa los procesos, herramientas y prácticas que tiene como objetivo la protección ante las amenazas en todo su ciclo de vida, el propósito de estas medidas de seguridad es impedir el robo o secuestro de datos o códigos en los sistemas, e incluyen las consideraciones al diseñar y desarrollar sistemas, así como el enfoque para protegerlos después de su implementación busca desarrollar, añadir y probar características dentro de las aplicaciones para disminuir vulnerabilidades asociadas a modificaciones de datos y accesos no autorizados, entre otros riesgos comunes.

En ese contexto, la institución dispone de herramientas de software cuya funcionalidad es ejecutada mediante diversas redes de datos locales, su funcionamiento se suscribe a las unidades operativas, como las soluciones relacionadas con los servicios administrativos, el almacenamiento local de archivos y las relacionados con ofimática (procesadores de palabras hojas de cálculo, diseño de presentaciones, entre otros), no obstante, también tiene en operación en forma simultánea, sistemas cuyo ámbito es nacional e interactúan con servicios en la nube, por ejemplo: el Expediente Digital Único en Salud, provocando que aumenten las vulnerabilidades, amenazas y consecuentemente la presión para garantizar la seguridad.

De forma tal, brindar protección ante los ataques dirigidos a las vulnerabilidades intrínsecas en las soluciones desarrolladas a lo interno o contratadas a terceros, se transforma en una necesidad, que requiere la adopción de una metodología de desarrollo seguro que considere las mejores prácticas en esta materia, con la finalidad de disminuir las posibilidades de ser afectados por la materialización de ataques, cubriendo desde la fase de desarrollo hasta la implementación y puesta en producción.

En ese contexto, las aplicaciones con una mayor solidez y efectividad en materia de seguridad[2] son aquellas que consideran el enfoque denominado "Seguridad por Diseño" (Security by Desing, SbD) iniciando en la fase de codificación e introduciendo elementos de seguridad en una etapa temprana del proceso de desarrollo, en lugar de aplicar políticas de manera retroactiva, simplificando la atención de incidentes y disminuyendo las posibles afectaciones. Este enfoque se basa en los principios de:

[1] https://ciberseguridad.com/guias/desarrollo-seguro/
[2] Glosario de VMware, LATAM

- Reducción de la superficie de ataque, es la suma de todas las vulnerabilidades presentes en el software, aplicaciones o dispositivos que puedan servir como puntos de entrada para los atacantes. Cada nueva característica o funcionalidad ensancha la superficie de ataque, de forma tal que su reducción implica limitar el acceso de los usuarios a funciones y características específicas.

- Principio de privilegio mínimo, busca garantizar que los usuarios dispongan de lo mínimo en la aplicación para completar las tareas particulares.

- Principio de valores predeterminados seguros, el producto desarrollado debe tener medidas de seguridad predeterminadas, independientemente de las preferencias de los usuarios, tales como: cantidad de caracteres mínimos de la contraseña, frecuencias de cambio, y datos requeridos para el registro del usuario.

- Principio de defensa en profundidad, tiene como objetivo incorporar desde el origen más de una forma de hacer que el producto sea seguro, lo que implica la utilización de una serie de mecanismos diferentes para la autenticación en el acceso a una aplicación, por ejemplo, algo que conoce el usuario (contraseña), algo que tiene (mensaje a dispositivo móvil) o algo que lo identifica (huella digital).

En resumen, la aplicación de los principios de seguridad por diseño pretende la utilización de diversos procedimientos para que solo accedan a los sistemas los usuarios que se autentiquen mediante contraseñas y múltiples factores de autenticación (entre los que se consideran la generación de códigos, utilización de parámetros biométricos u otros), una vez superada esta etapa se protegen los datos mediante restricciones de acceso que permitan visualizar solamente aquellos necesarios para la ejecución de sus funciones, así mismo de la aplicación de técnicas de cifrado de datos cuando se considere necesario.

Además, este enfoque integra las mejores prácticas de ciberseguridad a lo largo del ciclo de vida del proyecto, adoptando la idea que el desarrollo y actualización de los sistemas de seguridad es un proceso continuo. De forma tal que se implementan los nuevos sistemas y se prueban continuamente los antiguos, con la finalidad de identificar las vulnerabilidades y reducirlas oportunamente. Su implementación requiere un conjunto de pautas y prácticas que permitan a los desarrolladores evitar errores e identificarlos cuando inevitablemente se pasa alguno por alto.

En ese orden de ideas, algunas formas de adoptar este enfoque entre otras son:

- Tecnología de confianza, se refiere a tecnología probada cuyos propietarios sean abiertos sobre sus prácticas de seguridad.

- Capacitación del equipo de desarrollo, si el equipo de desarrollo conoce las amenazas y vulnerabilidades de proyectos similares o de librerías de terceros, será más cuidadoso al diseñar y codificar las aplicaciones, además de dotarlos de conocimientos en ciberseguridad.

- Privacidad al frente y al centro, crear controles de seguridad para acceder y compartir datos, asegurándose que las bases de datos estén lo más aisladas posibles y con acceso mínimo.

- Inteligencia Artificial y comprobaciones manuales, comprobaciones de rutina del código mediante herramientas de inteligencia artificial que busquen errores y vulnerabilidades. Una alternativa es la utilización de pruebas internas con consultores de seguridad para tratar posibles riesgos.

Buenas prácticas de diseño, "código espagueti"[3] y código heredado[4] hacen que los proyectos sean más complicados de mantener y eliminar vulnerabilidades.

Igualmente, debe ser considerada la importancia de disponer de desarrollares de sistemas con una alta conciencia en ciberseguridad, capacitados y experimentados redundando en la disminución de vulnerabilidades en los proyectos en los que participen, además de identificar eventuales riesgos descubiertos por las herramientas automatizadas y con base en su conocimiento y criterio técnico discernir las amenazas reales y los errores que no sean advertidos previamente.

Adicionalmente, es recomendable la utilización de herramientas automatizadas que reduzcan la intervención e interpretación humana con la finalidad de identificar con precisión la causa de las vulnerabilidades y solucionar los defectos de seguridad subyacentes, entre los modelos de pruebas más utilizados se encuentran:

- **SAST (Static application security testing):** las herramientas de prueba de seguridad de aplicaciones estáticas analizan pasivamente (sin ejecutarlo) el código fuente o el código binario de una aplicación en busca de vulnerabilidades conocidas. Este tipo de análisis aporta ventajas como corrección de vulnerabilidades desde el origen, no impacta el entorno de producción, fomenta la higiene del código al integrarse directamente en el entorno de desarrollo y da valor a las prácticas de desarrollo seguro[5]. En contra, se pueden mencionar los aspectos relacionados con su dificultad para administrarlo fuera del equipo de desarrollo, dificultad para implementar a gran escala, se práctica fuera del tiempo de ejecución y requiere diferentes implementaciones por cada lenguaje en el que se desarrolle. Existiendo diversas técnicas para su aplicación según se muestra en la siguiente imagen:

Imagen 1
Tipos de análisis y técnicas
Análisis estático de código

- Otro aspecto para considerar corresponde a la categoría de información que se va a recolectar, así como los posibles resultados y su tratamiento, entre los que se podrían determinar defectos de violación[6], bugs[7], o vulnerabilidades[8] que comparten características entre sí.

- **DAST (Dynamic application security testing):** las herramientas dinámicas de pruebas de seguridad ayudan a las personas a probar y analizar una aplicación en ejecución en busca de comportamientos que

[3] El código espagueti es un término peyorativo para los programas de computación que tienen una estructura de control de flujo compleja e incomprensible. Su nombre deriva del hecho que este tipo de código parece asemejarse a un plato de espaguetis, es decir, un montón de hilos intrincados y anudados.
[4] Legacy code o código heredado es código fuente relacionado con un sistema operativo o una tecnología de computación sin soporte técnico. El término también puede aplicarse a código insertado en software más moderno para integrar u ofrecer soporte a una función creada en el pasado; por ejemplo, dar soporte a una interfaz en serie incluso aunque muchos sistemas modernos no tienen un puerto serial.
[5] https://ciberseguridad.com/normativa/espana/medidas/seguridad-por-diseno/
[6] Defecto de violación: Diferencia entre lo que se codificó y lo que debería codificarse según el marco teórico del lenguaje utilizado.
[7] Bugs: Deferencias entre lo que se pretendía que hiciera el software y lo que hace.
[8] Vulnerabilidad: Conjunto de violaciones relacionadas con fallos de seguridad.

indiquen posibles vulnerabilidades, pueden realizarse en procesadores virtuales o reales. La verificación puede ejecutarse para verificar si todas las salidas del sistema son correctas sin importar su procesamiento (de caja negra), en tanto también puede buscarse la verificación de los procedimientos y los resultados (de caja blanca).

- **RASP (Runtime application self-protection):** las herramientas de autoprotección están integradas en la aplicación, por lo que el software puede monitorearse a sí misma para evitar ataques en tiempo real. Esta es una categoría relativamente nueva de aplicaciones diseñadas para mejorar la seguridad. Utiliza sensores para monitorear en tiempo real y abordar vulnerabilidades especificas deteniendo las amenazas de manera automática.

- **SCA (Software composition analysis):** las herramientas de análisis de composición de software ayudan a identificar componentes de terceros que pueden contener vulnerabilidades. Las vulnerabilidades pueden ser introducidas a lo largo de la cadena de suministro del software, y las herramientas SCA lo ayudan a evaluar y monitorear todos sus componentes.

Finalmente, es conveniente indicar que la aplicación de una metodología permite fortalecer aspectos de ciberseguridad desde el diseño de las aplicaciones a través de todo su ciclo de vida, además, una eventual disminución de las vulnerabilidades en los sistemas institucionales, reduciendo la superficie de ataque y las posibilidades de ejecución de exploit[9] aprovechados por los atacantes cibernéticos, así como la protección de los datos sensibles utilizados en las aplicaciones institucionales; considerando además su valoración durante las fases de implementación y producción a efectos de reducir la posibilidad de ataques exitosos.

III. CONSIDERACIONES NORMATIVAS

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

> *"(…) se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:*
>
> *a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.*
> *b) Exigir confiabilidad y oportunidad de la información.*
> *c) Garantizar eficiencia y eficacia de las operaciones."*

Adicionalmente, 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 "Gestión de Riesgos Tecnológicos", a saber:

> *"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 este integrada al sistema especifico 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*

[9] Programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución."

Así mismo, las normas mencionadas en el apartado Desarrollo, Implementación y Mantenimiento de Sistemas de Información, establece:

"X. DESARROLLO, IMPLEMENTACIÓN Y MANTENIMIENTO DE SISTEMA DE INFORMACIÓN

La Unidad de TI debe aplicar practicas formales que permitan ejecutar un proceso consistente para la definición de requerimientos, diseño, adquisición y/o desarrollo, realización de pruebas, migración de datos e información, aprobación, integración de conocimiento e inteligencia de negocios y puesta en marcha de las soluciones, con el fin de asegurar que la institución cuente con sistemas de información y aplicaciones que permitan gestionar adecuadamente la información requerida.

La Unidad de TI debe asegurar la disponibilidad de estándares para programación, gestión de la calidad del software en desarrollo o mantenimiento, cambios por excepción y/o emergencia, llevando un adecuado control de cambios y versiones."

Adicionalmente, en su apartado Seguridad y Ciberseguridad, la norma citada indica:

"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".

IV. CONSIDERACIONES FINALES

Considerando que el ciberataque sufrido por la institución el 31 de mayo de 2022 tuvo cuyo resultado fue la suspensión de los servicios y sistemas institucionales como medida de protección temporal, los cuales han sido progresivamente restituidos, además la ejecución de diversas acciones con la finalidad de disminuir los riesgos asociados, esta Auditoría considera conveniente la implementación de una metodología para disminuir, detectar y eventualmente subsanar las vulnerabilidades en los sistemas desarrollados institucionalmente y/o por terceros que incluya las mejores prácticas en esta materia, así como la utilización de herramientas automatizadas, a fin de fortalecer la seguridad durante todo el ciclo de vida.

En ese orden de ideas, la aplicación de principios de seguridad desde el diseño tales como: reducción de superficie de ataque, privilegio mínimo, valores predeterminados y defensa de profundidad en todo el ciclo de vida del software, permite fortalecer y abordar con mayor eficacia y eficiencia el manejo de los ataques, así como la resolución de los puntos débiles eventualmente aprovechados por las organizaciones que buscan dañar la operación normal de la institución en esta materia y exponer los datos sensibles de los asegurados como una forma de obtener ganancias

Adicionalmente, resulta conveniente valorar el uso de herramientas con la finalidad de ejecutar procesos de revisión automatizados del código de las aplicaciones, considerando las posibilidades con las que cuenta actualmente la institución, a efectos de identificar en las fases de desarrollo, implementación y producción de los sistemas, posibles errores, debilidades y vulnerabilidades con la finalidad de ser subsanadas.

En virtud de lo expuesto, y con el fin de aportar elementos de juicio adicionales, con la finalidad de coadyuvar en la adecuada toma de decisiones, se da conocer la información descrita, con el propósito de ser sometida a valoración y revisión por esa Administración, de forma tal que se fortalezca la seguridad en las aplicaciones institucionales desarrolladas internamente o por terceros, mediante la implementación de una metodología de desarrollo seguro considerando las mejores prácticas en esa materia, permitiendo identificar y subsanar vulnerabilidades mediante la introducción de este elemento a efectos de minimizar las posibilidades de éxito de eventuales ataques futuros.

Es importante que adicionalmente a la atención directa de los temas señalados, puedan hacer de conocimiento el contenido del presente oficio a las unidades que gestionan desarrollo de aplicaciones informáticas dentro de la estructura organizacional donde se encuentran adscritos, con el fin de minimizar los riesgos de ciberseguridad que se presenten en ese sentido, así como otros asociados a la gestión de las tic y seguridad de la información.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.09.02 12:58:17 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/AAM/lbc

C. Doctora Maria Eugenia Villalta Bonilla, gerente a.i, Gerencia General -1100.
Doctor Randal Álvarez Juárez, gerente, Gerencia Médica 2901.
Licenciado Gustavo Picado Chacón, gerente. Gerencia Financiera – 1103.
Doctor Esteban Vega de la O, gerente, Gerencia Logística – 1106.
Ingeniero Jorge Granados Soto, gerente, Gerencia Infraestructura y Tecnologías – 1107.
Licenciado Gilberth Alfaro Morales, gerente a.i, Gerencia Administrativa – 1104.
Licenciado Jaime Barrantes Espinoza, gerente, Gerencia Pensiones – 9108.
Auditoría

Fuentes consultadas:

- https://ciberseguridad.com/guias/desarrollo-seguro/
- www.vmware.com/latam/topics/glossary/content/application-security.htmluridad de las aplicaciones? | Glosario de VMware | LATAM
- https://www.microfocus.com/es-es/what-is/application-security
- https://www.nutanix.com/es/info/what-is-application-security
- https://www.b-secure.co/blog/herramientas-y-principios-para-la-seguridad-de-aplicaciones
- https://snyk.io/learn/application-security/
- https://www.welivesecurity.com/la-es/2021/01/18/analisis-estatico-codigo-fuente-orientado-a-seguridad/
- https://ciberseguridad.com/normativa/espana/medidas/seguridad-por-diseno/
- https://www.checkpoint.com/cyber-hub/cloud-security/what-is-runtime-application-self-protection-rasp/
- https://www.a2secure.com/blog/herramientas-de-prueba-de-seguridad-de-aplicaciones-ast/