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

**AS-AATIC-127-2022**
4 de julio de 2022

Doctor
Roberto Cervantes Barrantes, gerente
**GERENCIA GENERAL, 1100**

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

Estimado(a) señor(a):

**ASUNTO: Oficio de Asesoría sobre la actualización del software y la infraestructura en TIC.**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo 2022 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se informa sobre la actualización del software y la infraestructura en TIC, como medidas de contingencia y protección de la plataforma institucional, ante los ataques informáticos ocurridos contra la institución el 31 de mayo de 2022, a fin de que sea valorado para la toma de decisiones y acciones que compete a esa administración activa.

En ese sentido, la Auditoría, efectuó una revisión de los productos de auditoría emitidos a nivel institucional, donde se mencionaron aspectos de vulnerabilidades y riesgos de la seguridad en tecnologías de información y comunicaciones, además, se consultó a 58 unidades institucionales (hospitales, áreas de salud y sucursales), sobre la actualización de sistemas operativos y antivirus en los equipos TIC. Lo anterior, con el propósito de efectuar un diagnóstico situacional y posibles medidas que se podrían adoptar en esta temática.

Al respecto, los resultados obtenidos son los siguientes:

## I. ANTECEDENTES

En declaraciones efectuadas el 17 de mayo de 2022, a medios de comunicación nacional e internacional, el presidente de Costa Rica, Rodrigo Alberto Chaves Robles, afirmó que el país se encontraba en “guerra” contra los “terroristas cibernéticos” del grupo Conti, que el pasado 17 de abril comenzaron una serie de ataques de los que el país aún sufre las consecuencias, *“Estamos en guerra y esa no es una exageración. Costa Rica está sufriendo un ataque terrorista cibernético y por eso hemos decretado estado de emergencia nacional para enfrentar esa amenaza”.*

Las entidades públicas - Ministerio de Hacienda, Ministerio de Ciencia Tecnología y Telecomunicaciones (MICITT) y la Caja Costarricense de Seguro Social- han sido blanco de múltiples ataques tipo ransomware, que impide a los usuarios e instituciones acceder a sus sistemas o archivos y que exige el pago de un rescate para poder disponer nuevamente de ellos, situación que llevó al país a publicar una declaratoria de emergencia nacional en todo el sector público (mediante Decreto No. 43542-MP-MICITT) e institucional (mediante oficio GA-CAED-0260-2022 del 02 de junio de 2022).

En este contexto, 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 realizar una desactivación controlada de los servicios TI institucionales, de acuerdo con los informes presentados por la Dirección de Tecnologías de Información y Comunicaciones al Centro Coordinador de Emergencias Institucional (CCEI).

Este tipo de ciberataques, en su mayoría se presentan debido a debilidades en la infraestructura tecnológica dentro de las que se encuentra la aplicación de actualizaciones de software y parcheado de seguridad.

La CCSS depende de equipos con software que se utilizan para el cumplimiento de los objetivos planteados para la gestión médico – administrativa; durante su funcionamiento y vida útil, en estos programas o sistemas operativos, se descubren fallos de seguridad o vulnerabilidades que podrían ser aprovechados por los ciberdelincuentes para introducirse en ellos, dejarlos inactivos, infectarlos y robar todo tipo de datos (credenciales de acceso, datos confidenciales, etc.).

En relación con lo anterior, según datos extraídos de los sitios web forbescentroamerica.com y ciberseguridad.com, a continuación, se indican 6 casos de ciberataques relevantes (a nivel mundial) durante el 2021:

**1. Solar Winds:** La compañía dedicada al software recibió un ataque con malware, el cual contaminó una de sus actualizaciones, de esta forma los ciberdelincuentes recopilaron grandes cantidades de información de sus clientes. Más de 18,000 organizaciones entre las que destacan varias agencias gubernamentales y del sector privado de EE.UU, se vieron afectadas en este ataque que duró meses antes de ser descubierto a finales de 2020.

**2. Microsoft Exchange Server:** La violación de Microsoft Exchange ocurrió cuando el grupo de piratería Hafnium, con sede en China, aprovechó una falla de día cero previamente desconocida en los sistemas de Microsoft para robar datos de las redes objetivo. En un ejemplo de un ataque bajo y lento, se estima que los piratas informáticos han tenido acceso a los sistemas desde finales de 2020.

The Wall Street Journal informa que decenas de millas de organizaciones se han visto afectadas, y una fuente sugiere que el número total de empresas afectadas podría ser superior a 250.000.

Más tarde se conoció que la Autoridad Bancaria Europea se había visto comprometida en el ataque, y la BBC informó que desconectó todo su sistema de correo electrónico para evaluar cualquier daño potencial.

**3. Colonial Pipeline:** El sistema de oleoductos de productos refinados más grande de los EE. UU., recibió en mayo 2021 uno de los ciberataques considerados más importantes en el que se vieron interrumpidos sus procesos de distribución, lo que llevó a escasez de combustibles en parte del país y cambios en los precios del petróleo a nivel mundial. Para solucionarlo la compañía debió pagar al grupo de ransomware DarkSide casi 5 millones de dólares.

**4. ACER:** Con operaciones en Xizhi, New Taipei City, Taiwán, Acer es líder mundial en electrónica avanzada; sin embargo, en marzo de 2021, sufrieron una de las demandas de ransomware más costosas registradas. Los detalles más críticos conocidos sobre el ataque incluyen:

- El 18 de marzo, el grupo de ciberdelincuentes REvil publicó datos robados de Acer en un sitio que supuestamente opera, Happy Blog. Los datos robados incluían información personal sobre clientes de Acer, formularios de pago y otros documentos financieros críticos para el personal y la clientela.
- REvil exigió un rescate de 214,151 XMR en criptomoneda, aproximadamente equivalente a
  $ 50 millones. Esta suma sería la más grande de la historia, si se recauda. Sin embargo, Acer aún no ha revelado si pagaron o no el rescate.

Si bien se desconocen en gran medida las causas específicas del ataque, los expertos en ciberseguridad sospechan que REvil accedió a Acer a través de una debilidad en Microsoft Exchange ProxyLogon. Este tipo de vulnerabilidades son comunes en el software de terceros; por lo tanto, la gestión de riesgos de terceros es fundamental.

**5. Kaseya:** REvil atacó una actualización de VSA, un software de la empresa de gestión informática en julio 2021, esto afectó a agencias gubernamentales y pequeñas empresas debido a que los primeros afectados eran distribuidores de servicios.

En este caso Kaseya no pagó por el desencriptador universal de 70 millones de dólares que REvil había propuesto, la compañía dijo que usó un desencriptador gracias a un tercero.

**6. Ejecutivo del Servicio de Salud de Irlanda (HSE):** El 14 de mayo 2021, la organización gubernamental que administra todos los servicios de salud pública en Irlanda, cerró los sistemas de TI a raíz de un importante ataque de ransomware. Si bien los sistemas HSE se desconectaron por la fuerza solo como medida de precaución, y los Servicios Nacionales de Ambulancia funcionaban con normalidad, se interrumpió el acceso a muchos servicios de salud.

No fue hasta el 30 de junio que se restableció el registro en línea para las tarjetas médicas. Además, los centros de salud pedían a los pacientes que trajeran documentos en papel, ya que los registros informáticos eran inaccesibles. A pesar de las interrupciones, la red de salud pública de Irlanda dijo que no pagaría el rescate y tampoco lo haría el gobierno.

Sin embargo, hubo evidencia de que se accedió a la información del paciente y del personal en el ataque cibernético y que se filtraron algunos de los datos. Los datos personales filtrados pueden incluir nombres, direcciones, números de teléfono de contacto y direcciones de correo electrónico. La información médica podría incluir registros médicos, notas e historiales de tratamiento.

Ha aparecido una pequeña cantidad de datos de HSE en la 'web oscura', una parte de Internet a la que solo se puede acceder mediante programas especiales.

Recientemente se publicó el informe Threat Labs Report (abril 2022) de la empresa dedicada a la ciberseguridad Trellix, en éste se destacó que los consumidores individuales son el objetivo número 1 de los ciberdelincuentes. En este reporte que estudia el comportamiento de los ciberdelincuentes en los últimos seis meses, se notó de igual forma **que el sector sanitario, fue el segundo objetivo de ciberataques** y que otros sectores como en el del transporte, el envío, la fabricación y la tecnología de la información presentaron un aumento de amenazas.

Todo el software tiene un ciclo de vida, por lo que llegado el momento puede quedar desactualizado, obsoleto o sin soporte oficial por parte del fabricante. En ese momento es un blanco fácil para los ciberdelincuentes y se debería de actualizar o dejar de utilizar.

Para solucionar estas vulnerabilidades, los fabricantes de software publican actualizaciones de seguridad que se deben de instalar para parchear los fallos de seguridad descubiertos.

Los beneficios de actualizar el software son múltiples, entre ellos, se citan los siguientes:

- Una actualización mantendrá los equipos a salvo de los agujeros de seguridad (ya conocidos por los proveedores). Cuando se detectan nuevas vulnerabilidades, comienza el trabajo para encontrar una solución y ofrecer una nueva versión del software a los clientes, de manera que puedan seguir utilizándolo de forma segura.

- Con cada actualización del software, se publica una lista de elementos parcheados. Dicha lista es pública, de manera que un potencial atacante puede saber exactamente qué problemas tenía el software, antes de la actualización. Si la organización no ejecuta dicha actualización, ese potencial atacante puede sacar provecho de ello y perjudicar enormemente.

- Por otro lado, la organización tendrá un software con una mejor funcionalidad; muchas actualizaciones no son solo de seguridad, sino que optimizan el producto, o lo hacen más estable. De la misma manera, con la actualización se podrá disponer de un producto libre de errores, ya que a medida que los diferentes usuarios reportan fallos o comportamientos inesperados, estos se van corrigiendo y obteniéndose productos más eficientes.

- Uno de los aspectos más importantes es que, en el fondo, no estamos solos, se trabaja en una red corporativa, donde se comparten archivos entre compañeros, clientes y proveedores. Un fallo de seguridad en un dispositivo con credenciales de acceso a la red, o a zonas críticas, pone en serio peligro a toda la empresa y los datos; por lo tanto, el mantenimiento es fundamental, es una de las partes más importantes del ciclo de vida del software.

Debido a lo anterior, está auditoría considera importante mencionar que, en el *"Boletín seguridad de empresas"* emitido por el Instituto Nacional de Ciberseguridad de España (junio 2022), en lo relativo a vulnerabilidades y afectaciones en productos software, se indica lo siguiente:

***"Boletín mensual de Microsoft - junio 2022***

***(…) Descripción***

*El boletín mensual de junio de Microsoft, informa de **93 vulnerabilidades** en sus productos, de las cuales 3 son de severidad crítica, 54 de severidad alta, 3 de severidad media, 1 de severidad baja y 32 sin severidad asignada.*

***Solución***

*En la mayor parte de los casos, el software afectado se actualizará automáticamente por defecto. No obstante, en el caso de que no se realizase dicha actualización de forma automática, Microsoft pone a disposición de los usuarios un portal web con toda la información relacionada, así como los parches de los productos afectados para descarga.*

*Se recomienda actualizar lo antes posible el software afectado a la última versión y activar las actualizaciones automáticas en caso de que no se estén aplicando por defecto (...)*

***Detalle***

*Las vulnerabilidades publicadas se corresponden con los siguientes tipos: denegación de servicio, ejecución remota de código, escalada de privilegios, omisión de características de seguridad, divulgación de información y suplantación de identidad.*

***Múltiples vulnerabilidades que afectan a productos Cisco***

***(…) Descripción***

*Cisco ha publicado 2 vulnerabilidades de severidad crítica y un alta que afectan a los productos citados en 'Recursos afectados'.*

***Solución***
*Cisco ha publicado actualizaciones y, en algunos casos soluciones alternativas, que abordan las vulnerabilidades descritas en este aviso.*

*En cualquier caso, Cisco advierte de que cada empresa debe asegurarse de que los dispositivos que se van a actualizar contienen suficiente memoria y confirmar que las configuraciones actuales de hardware y software seguirán siendo compatibles con la nueva versión. Ante cualquier duda, se aconseja a los clientes que se pongan en contacto con el Centro de Asistencia Técnica (TAC) de Cisco o con sus proveedores de mantenimiento contratados (...)*

***El detalle de las vulnerabilidades es el siguiente:***

- *Una vulnerabilidad de severidad crítica en la funcionalidad de autenticación externa de Cisco Secure Email and Web Manager, anteriormente conocido como Cisco Security Management Appliance (SMA), y Cisco Email Security Appliance (ESA) **podría permitir a un ciberdelincuente remoto, no autenticado, saltarse la autenticación e iniciar sesión en la interfaz de gestión web de un dispositivo afectado.***

*• Una vulnerabilidad de severidad alta en la interfaz de gestión web de Cisco Secure Email and Web Manager, anteriormente Cisco Security Management Appliance (SMA), y Cisco Email Security Appliance (ESA)* ***podría permitir a un ciberdelincuente remoto, autenticado, recuperar información sensible de un servidor de autenticación externo Lightweight Directory Access Protocol (LDAP) conectado a un dispositivo afectado.***

*• Una vulnerabilidad de severidad crítica en la interfaz de gestión basada en web de los routers Cisco Small Business RV110W, RV130, RV130W y RV215W* ***podría permitir a un ciberdelincuente remoto, no autenticado, ejecutar código arbitrario o hacer que un dispositivo afectado se reinicie inesperadamente, dando lugar a una condición de denegación de servicio (DoS).***

***Actualiza Zoom para corregir estas vulnerabilidades***

*(…)* ***Descripción***

*Zoom ha solucionado dos vulnerabilidades, una de ellas de criticidad alta, que podrían permitir a un ciberdelincuente realizar inyección DLL o unirse a una reunión sin consentimiento del anfitrión.*

***Solución***

*Zoom ha publicado actualizaciones para los productos afectados que solucionan estas vulnerabilidades (...)*

***Detalle***

*Las vulnerabilidades solucionadas en esta actualización podrían permitir a un ciberdelincuente:*

- *Realizar una inyección DLL en el instalador de Zoom Opener cuando un usuario lo descarga desde la página de inicio de reunión e intenta unirse a ella sin tener instalado el cliente de reuniones.*
- *Unirse a una reunión sin autorización del anfitrión, debido a una incorrecta comprobación de los permisos".*

Lo anterior, representa un riesgo latente para las organizaciones y una ventajosa oportunidad para los ciberdelincuentes, que se encuentran a la espera de cualquier oportunidad o debilidad para introducirse, infectar y atacar uno de los activos más valiosos en la actualidad, la información.

## II. RESULTADOS OBTENIDOS

### 2.1 Productos emitidos por la Auditoría:

La Auditoría Interna ha señalado a la administración activa la importancia de garantizar la contingencia de los servicios tecnológicos y fortalecer las medidas para atender las oportunidades de mejora, establecidas en aspectos de vulnerabilidades y riesgos en TIC de la CCSS. En el anexo 1, se indican algunos de los productos en los que se abordaron, la temática anteriormente mencionada.

En relación con lo anterior, es importante mencionar lo señalado mediante el oficio AS-AATIC-108-2022 del 22 de junio de 2022, respecto a la evaluación y priorización de riesgos, indicándose, lo siguiente:

> *"(…)* ***2.1 Inventario de los activos TIC***
>
> *El plan de recuperación ante desastres siempre debe comenzar con un inventario de todos los activos de TI, a nivel de equipamiento y software, este paso es necesario para visualizar la complejidad del entorno y evitar omitir algún detalle en el restablecimiento de los servicios (...)*
>
> *En consecuencia, considerando todos los activos, incluidos los servidores, terminales de almacenamiento, aplicaciones, datos, equipamiento de red, puntos de acceso y dispositivos de red que deben ser valorados y certificados en relación con su escaneo e inmunización (según corresponda); en aras de tener certeza sobre la mitigación de los riesgos asociados con las amenazas identificadas por los equipos técnicos de la CCSS en materia de ciberseguridad u otras vulnerabilidades a las que pueda estar expuesta la Institución.*
>
> *En ese sentido, visibilizar la ubicación física de cada activo, condición lógica, interconexión a la red y de más aspectos, generará un insumo valioso para identificar los elementos primordiales de la plataforma tecnológica, nivel de dependencia de los usuarios, así como otras variables propias de los activos que son utilizadas para la toma de decisiones.*
>
> ***2.2 Evaluación y priorización de riesgos***
>
> *(…) Seguido al mapeo de todos los activos de TIC, el identificar las posibles amenazas internas y externas (actuales y venideras) es necesario dentro de un plan de recuperación, en aras de estimar de manera progresiva, cuáles serían los escenarios y el accionar de la Administración.*
>
> *En ese sentido, los expertos recomiendan incorporar o verificar los niveles de probabilidad de que ocurran las amenazas, estimar su impacto desde el ámbito de negocio y/o tecnológico; esto con el objetivo de priorizar las actividades a seguir según los planes de continuidad y contingencia.*
>
> *Además, examinando la oportunidad que tienen los mecanismos en materia de ciberseguridad, ya implementados en la Institución, en función de mitigar los riesgos tecnológicos detectados. Lo anterior, considerando el contexto actual de la CCSS y determinando si existen recomendaciones básicas por atender o requieren de una labor prioritaria en su ejecución, tales como:*
>
> *(…) Garantía de sistemas operativos y de información actualizados (…)*
> *Labor entorno a campañas de educación a los usuarios sobre los riesgos de ciberseguridad, manejo de correo, detección de alertas en los equipos finales, tipos de vulnerabilidades, entre otros elementos".*

## 2.2 De la información aportada por unidades institucionales, referente a la actualización de software y sistemas operativos:

Esta auditoria les consultó a 58 unidades institucionales (áreas de salud, hospitales y sucursales), sobre la implementación de un procedimiento interno para la actualización de sistemas operativos y antivirus en los equipos TIC (previo al ciberataque suscitado el 31 de mayo del 2022), respondiendo 48 (83 %) de ellas que "Sí" efectuaban la actualización, 6 (10 %) que "No" y en 4 (7 %) no aplicaba dicha pregunta.

A continuación, se transcribe algunas de las respuestas emitidas:

**Cuadro 1**
**Implementación de procedimiento interno para la actualización de sistemas operativos y antivirus, en unidades institucionales periodo de consulta del 6 al 15 de junio de 2022**

| Nombre de la unidad consultada | ¿De previo a este evento, tenía establecido un procedimiento interno para la actualización de sistemas operativos y antivirus en las computadoras de esta unidad? |
|---|---|
| Hospital Monseñor Sanabria Martínez | Sí. Aproximadamente de forma bimensual se están revisando las actualizaciones de sistemas operativos y antivirus. Además, a nivel institucional se dispone de una herramienta SCCM, la cual se supone fuerza las actualizaciones en los equipos. |
| Sucursal de Esparza | Sí. De hecho, estaban actualizados, únicamente la de consulta a usuarios externos estaba desactualizada, ya que se utiliza poco y no la tiene en uso ningún funcionario en específico |
| Área de salud de Guápiles | No. Dependemos de las actualizaciones automáticas porque no tenemos CGI. |
| Área de Salud Alajuela Norte | Sí. Con las actualizaciones del nivel central, esto no se hace localmente. |
| Área de Salud Los Chiles | Sí. Desde el nivel central se envían las actualizaciones. |
| Sucursal de Upala | N/A. El CGI de la Dirección tiene estos controles. |
| Área de salud Goicoechea 2 | Sí. estábamos en proceso de actualización de Windows server y SQL |
| Sucursal CCSS Turrialba | Si. Había un cronograma de actualizaciones administrado por nivel central, el cual realizaban remotamente." |
| Área de Salud Aserrí | Sí. Los únicos equipos que no estaban actualizados del todo son los del Laboratorio por la particularidad de los mismo. |
| Sucursal de San Ignacio de Acosta | A nivel del CGI de la Gerencia Financiera al final de mes se distribuyen los paquetes más importantes para actualizar los equipos incluido el Windows Defender. El lunes 30 de mayo 2022 ya algunos equipos tenían la vacuna de Micro Claudia. |
| Hospital San Juan de Dios | Políticas DTIC. SCCM se hace de manera escalonada y en las tardes. |
| Área de Salud Dr. Ricardo Moreno Cañas | Nosotros tenemos un WSUS que fue brindado por la Institución, el mismo es un servidor de actualizaciones, pero es administrado por la CCSS. |
| Área de Salud Paraíso-Cervantes | No. Las actualizaciones por política se realizan a nivel central. |
| Área de Salud Oreamuno-Pacayas-Tierra Blanca | No. Por política se realiza en el nivel central, si no hay directriz no se puede realizar. |
| Sucursal Cartago | Sí. mensualmente se realizar actualizaciones a nivel general, que comunica previamente el CGI de la Gerencia Financiera. |
| Hospital Dr. Rafael A. Calderón Guardia | No. porque todo es política de la CAJA, ellos nos informan cuando se dispone de actualizaciones |

**Fuente:** Elaboración propia de auditoría, información suministrada por unidades institucionales en consulta efectuada del 6 al 15 de junio de 2022.

Del cuadro anterior, se establece que, según lo indicado por las unidades consultadas, las actualizaciones de software y antivirus son comunicadas, enviadas o distribuidas por los CGI Gerenciales o autoridades institucionales en TIC (nivel central), algunas de éstas se ejecutan de manera automática mediante herramientas como el SCCM[1] y otras se aplican de forma manual en el nivel local, cuya periodicidad es variable.

Asimismo, en consulta efectuada, el 07 de junio de 2022, al Ing. Marco Vinicio González Jiménez, jefe del Área de Gestión Informática de la Gerencia de Pensiones, respecto a las posibles causas que contribuyeron a minimizar la afectación o infección (por ransomware) en los equipos de cómputo, indicó:

> *"(…) inmediatamente que recibimos la notificación del ataque, el 31 de mayo de 2022 a las tres de la mañana, se apagaron servidores, lo que permitió contener un poco la afectación; desde el punto de vista técnico, hemos revisado el 100 % de los equipos de usuario final de la Gerencia de Pensiones y dentro de los protocolos de revisión que nos han indicado efectuar, se ha logrado determinar que, no tenemos ni un solo equipo afectado, esto se debe posiblemente a la política que tenemos nosotros de mantener los sistemas actualizados, además, que ya muchos de los equipos tenían instalado el Micro Claudia, lo cual, pudo haber generado actualizaciones que pudieron presentar una barrera, ante el ciberataque del 31 de mayo de 2022 (…)".*

**2.3 Sobre el restablecimiento de los sistemas de información y el uso de los equipos de cómputo en instalaciones de la CCSS:**

En relación con lo anterior, es de conocimiento de esta Auditoría que, la institución ha iniciado con el restablecimiento, de manera gradual, de algunos sistemas de información, tal y como se ha indicado en diversos comunicados emitidos en la plataforma Instagram, mediante el sitio digital **"Somos CCSS"**, según se muestra a continuación:

> *"Alerta CCSS*
>
> ***Pago de pensiones de junio se realizará sin inconvenientes** (14 de junio de 2022)*
>
> *• Tanto beneficiarios del IVM como RNC recibirán su pensión en la fecha programada.*
> *• En el caso del aumento aprobado este se realizará una vez que las operaciones se normalicen.*
>
> *Autoridades de la Gerencia de Pensiones de la CCSS informaron este lunes que el pago regular de pensiones para el mes de junio se mantiene para la fecha programada a finales de mes gracias a las acciones de contingencia que han logrado establecer.*
>
> *El licenciado Ubaldo Carrillo Cubillo, director de Pensiones de la CCSS, detalló que "se avanza hacia el pago ordinario de la pensión de junio sin mayor inconveniente para los beneficiarios". Esto aplica para tanto para pensionados del régimen de Invalidez, Vejez y Muerte (IVM) como del Régimen no Contributivo de Pensiones (RNC).*

[1] System Center Configuration Manager (conocido en sus siglas como SCCM) o, desde la versión 1910, Microsoft Endpoint Configuration Manager (ECM) es el nombre comercial de la línea de software de Administración de Cambios y Configuraciones de computadoras, servidores, dispositivos móviles y software, desarrollado por Microsoft.

*Carillo Cubillo explicó que en relación con el pago del aumento aprobado a las pensiones y programado para junio este cálculo y depósito se realizará una vez que se puedan retomar las operaciones de manera regular pues "en este momento están concentrados en garantizar el pago de las pensiones al 100% de beneficiarios para finales de junio".*

*En el caso de nuevas pensiones la Gerencia se encuentra de igual forma trabajando en establecer el mecanismo que permita incluirlas para el pago lo antes posible".*

*"**SICERE y página web rehabilitadas** (21 de junio de 2022)*

*Gracias al gran trabajo de los compañeros de la DTIC, Gerencia Financiera y Comunicación, esta mañana se reactivaron la página web de la CCSS (una versión simplificada) y el Sicere para patronos y trabajadores".*

*"**Pagamos incapacidades y se restablece sistema para pagos de manera regular** (24 de junio de 2022)*

*La Gerencia Financiera de la Caja Costarricense de Seguro Social (CCSS) informó que logró restablecer su sistema de pagos de incapacidades lo que permitirá ejecutar los pagos de manera ordinaria a partir de este lunes 27 de junio.*

*De igual este jueves se acreditaron en las cuentas bancarias de los beneficiarios los pagos de incapacidades y licencias continúas otorgadas antes del 30 de mayo del 2022 por un monto de ¢2,651.6 millones de colones y que corresponden a 11,605 casos".*

Asimismo, se han efectuado comunicados respecto al uso de los equipos de cómputo en instalaciones de la CCSS:

*"Alerta CCSS*

***Uso de equipo de cómputo en instalaciones de la CCSS** (23 de junio de 2022)*

*La Dirección de Tecnologías de Información y Comunicaciones viene trabajando de la mano con los Centros de Gestión Informática de todo el país, en las actualizaciones de los programas "Windows Defenfer" y la instalación de "microClaudia".*

*Es por eso que los funcionarios deben encender sus equipos hasta que los compañeros del Centro de Gestión Informática les den el visto bueno de hacerlo".*

*"**Estado de situación** (24 de junio de 2022)*

*• Se continua con el trabajo de revisión y protección de toda la red informática.*
*• Cuando sea seguro se procederá con la habilitación paulatina de servicios.*
*• En las unidades institucionales los equipos de informática brindarán acompañamiento e instrucciones para el uso de los equipos.*
*• Las computadoras deben mantenerse apagadas o desconectadas de la red hasta que se brinde la indicación por parte de los equipos informáticos autorizados".*

> *"**Uso de equipo de cómputo en instalaciones de la CCSS** (27 de junio de 2022)*
>
> *La estación de trabajo (computadora) se debe mantener apagada y desconectada de la red institucional, hasta que personal de su Centro de Gestión Informática (CGI) realice el respectivo análisis y den el visto bueno para su uso"*
>
> *"**Uso de equipo de cómputo en instalaciones de la CCSS** (29 de junio de 2022)*
>
> *Es importante que respete las instrucciones del Centro de Gestión Informática (CGI) local y encienda su equipo hasta que haya sido revisado y verificado por un compañero de CGI o autorizado por el personal a cargo".*

En las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por el Ministerio de Ciencia, innovación, Tecnología y Telecomunicaciones (MICITT), 2021, descrito en el apartado la *"Gestión del 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."*

Ese mismo marco normativo, en el apartado "Administración Infraestructura Tecnológica", refiere:

> *"La institución debe implementar prácticas formales que permitan mantener identificados y actualizados los activos de TI, mediante inventarios de recursos tecnológicos instalados en la organización (hardware, software, aplicaciones, comunicaciones), clasificados según el nivel de criticidad, características, configuración, servicios y medidas de protección asociadas."*

## IV. CONSIDERACIONES

Un ciberataque está conformado por un conjunto de acciones cuyo principal objetivo es vulnerar o atacar diversas bases de datos o redes informáticas que contengan datos sensibles, con los cuáles se pueda afectar, dañar o destruir organizaciones, empresas o incluso poner en juicio la reputación de cualquier individuo.

La mayoría o casi todos los ciberataques son creados con la finalidad de obtener información de valor; estos ataques pueden provenir de acciones criminales, espionajes e incluso ciberterrorismo.

**La institución debe concientizar en los niveles centrales, regionales y locales, la necesidad e importancia de mantener el software y la infraestructura en TIC debidamente actualizados**, ya que dicho procedimiento es fundamental para poder garantizar la seguridad de los sistemas, equipos e información, ante los más novedosos tipos de ataque y, además, beneficiarse de todas las mejoras que se realicen para estos productos, por parte de los proveedores.

En relación con lo interior, está auditoría considera importante hacer mención de algunos puntos clave, establecidos por el Instituto Nacional de Ciberseguridad de España, en lo relativo a actualizaciones de software en una organización:

- **Determinar el software qué debe ser actualizado.** Se tendrá que realizar un inventario de todo el software y el firmware instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo, se debe instalar las correspondientes actualizaciones y parches de seguridad.

- **Determinar cuándo y qué actualizaciones instalar.** El equipo técnico determinará el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que tengamos software instalado que no disponga de estas opciones de actualización. En este caso se deben usar los canales de alerta y los procedimientos oportunos para detectar e instalar las actualizaciones correspondientes.

- **Probar las actualizaciones.** Siempre se deben de instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las actualizaciones, de este modo se podrá verificar que su funcionamiento es el esperado.

- **Deshacer los cambios.** Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado podremos volver a la situación anterior.

- **Herramientas de diagnóstico y actualización.** Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, se podrá proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que se quiere que el software instalado sea homogéneo y esté especialmente controlado.

- **Configuración de un sistema de alertas.** Conviene configurar un sistema de alertas para recopilar avisos y notificaciones sobre vulnerabilidades, actualizaciones y parches de seguridad del software utilizado.

- **Registro de actualizaciones.** Se debe de realizar un registro de las actualizaciones que se han instalado en los sistemas. De esta forma se podrá tener en todo momento un conocimiento exhaustivo del software operativo en los equipos.

Por otra parte, además de velar por la actualización del software, los diferentes actores involucrados de la institución deben contemplar el fortalecimiento de la gestión y control de la infraestructura de TI, la formación de colaboradores en materia de ciberseguridad y buenas prácticas en TIC, el reforzamiento de los equipos técnicos encargados del soporte y mantenimiento (preventivo y correctivo) del software, así como, la realización de auditorías y revisiones en materia de seguridad; lo anterior, con el fin de reaccionar ante las nuevas formas de amenaza y reforzar las medidas, herramientas y procesos actualmente establecidos en relación con las amenazas conocidas.

De conformidad con lo expuesto, y en apego al artículo 8 de la Ley General de Control Interno, referente al deber de garantizar la eficiencia y eficacia de las operaciones que se ejecuten, resulta fundamental que la administración activa se mantenga vigilante de que se adopten las acciones que sean pertinentes y se establezcan las medidas de control necesarias, a fin de garantizar razonablemente la recuperación y continuidad de los servicios en la gestión de Tecnologías de Información y Comunicaciones.

En virtud de lo mencionado, esta Auditoría hace de conocimiento de esa Administración los aspectos mencionados en el presente oficio, con el objetivo de incentivar la capacidad de la Institución para recuperar y restablecer el componente TI después de la interrupción en sus sistemas de información que aún afecta a la CCSS.

Atentamente,

**AUDITORÍA INTERNA**

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.05 13:17:44 -06'00'

Lic. Olger Sánchez Carrillo
**Auditor**

OSC/RJS/RAHM/AEBB/lbc

Anexo (1)

1. Productos emitidos por la Auditoría Interna sobre aspectos de contingencia de los servicios tecnológicos, vulnerabilidades y riesgos en TIC de la CCSS.

C Auditoría.

# ANEXO 1

**Cuadro 2**
**Productos emitidos por la Auditoría Interna sobre aspectos de contingencia de los servicios tecnológicos, vulnerabilidades y riesgos en TIC de la CCSS**

| |
|---|
| ATIC-106-2017 “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 AD–ATIC–8137–2018 “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 “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. |
| AD-ATIC-1512-2020 “Oficio de advertencia sobre la contingencia de la seguridad informática en el contexto de continuidad del negocio”. |
| AD-ATIC-038-2022 “Oficio de advertencia sobre la continuidad de servicios bajo el contexto del evento de interrupción de los servicios tecnológicos a nivel Institucional presentado el 7 de marzo de 2022”. |
| AD-ATIC-039-2022 “Oficio de advertencia sobre la exposición a ataques cibernéticos a la CCSS”. |
| AS-AATIC-072-2022 “Oficio de Asesoría sobre la gestión de crisis en materia de ciberseguridad como resultado del ataque cibernético ocurrido el 31 de mayo del 2022”. |
| AS-AATIC-088-2022 “Oficio de Asesoría sobre la continuidad del negocio ante amenazas o desastres de origen tecnológico”. |
| AS-AATIC-108-2022 “Oficio de asesoría sobre la estrategia de recuperación ante amenazas o desastres de origen tecnológico”. |