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

AS-AATIC-131-2022
6 de julio 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 INFRAESTRUCTURA Y TECNOLOGÍA-1107

Licenciado
Jaime Barrantes Espinoza, gerente
GERENCIA DE PENSIONES-9108

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

Estimados(as) señores(as):

ASUNTO: **Oficio de Asesoría referente soluciones de autenticación en sistemas informáticos.**

Esta Auditoría en cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo para el período 2022, con fundamento en los artículos N.º 21 y 22 de la Ley General de Control Interno y siendo consecuentes a lo indicado en el oficio AI-874-2022 del 6 de junio del 2022, sobre el inicio de la evaluación referente al ataque cibernético sufrido en la CCSS y sus efectos, a partir de la desconexión de sistemas de información efectuada el 31 de mayo del 2022; procede a emitir la siguiente asesoría referente a soluciones de autenticación en sistemas informáticos.

A ese respecto, es conocido que la Caja Costarricense de Seguro Social (CCSS), recibió un ciberataque el pasado 31 de mayo del 2022, obligándole (de manera preventiva) a desactivar todos los sistemas informáticos de la Institución; es decir, han trascurrido más de 30 días desde la materialización de ese incidente tecnológico.

Aunado a lo anterior, recientemente se han restablecido algunos sistemas de información y la CCSS sigue bajo la necesidad de ejecutar el plan de gestión de crisis y/o recuperación, según corresponda; seguido de la puesta en marcha de una estrategia priorizada en ciberseguridad.

Bajo ese contexto, esta Auditoría estima pertinente recopilar la información contenida en el marco regulatorio, guías de mejores prácticas y acotaciones de profesionales que han enfatizado sobre la importancia del tema.

1- OBSERVACIONES

Es importante que la Administración analice como mínimo, las siguientes observaciones al definir o evaluar la implementación o mejora de mecanismos especializados en verificar la identidad de los usuarios que utilizan los sistemas informáticos de la CCSS, a saber:

1.1 Sobre el robo de credenciales

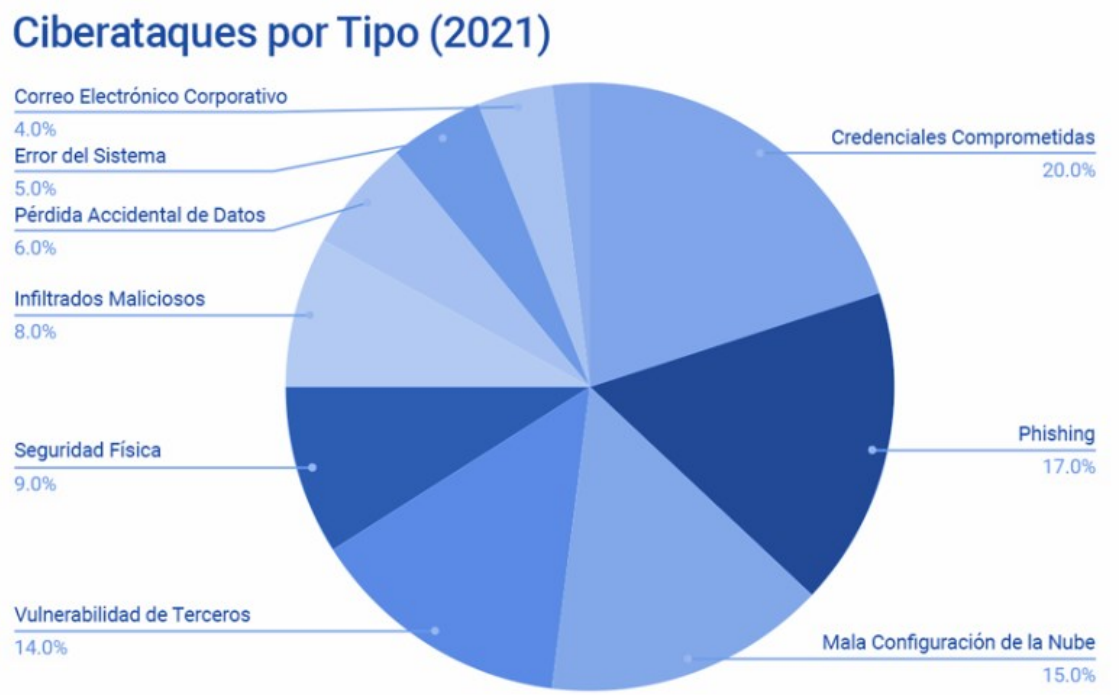
Las claves perdidas y robadas a menudo tienen relación con la apropiación de cuentas, filtraciones de datos y otros tipos de fraude. Tal y como se ejemplifica en la nota periodística “Cambia ya tus contraseñas, se han filtrado casi 9.000 millones en la Deep Web” del 8 de junio del 2022 publicado por el diario económico español “Cinco Días”, citando un caso donde se han comprometido credenciales:

> *“Las contraseñas en Internet son básicas para poder navegar con un mínimo de seguridad y protección para nuestros datos. En el intercambio de datos continuo que supone navegar en Internet las contraseñas son los bienes más preciados por los hackers, pero se ha demostrado muchas veces que no es la solución más segura para garantizar que nuestros datos no serán robados. Pero poco se puede hacer cuando esas contraseñas directamente se sustraen de los servidores donde se alojan. Y eso es lo que ha pasado ahora con la que sin duda puede ser la mayor filtración de contraseñas de la historia, afectando a miles de millones de cuentas de todo el mundo.*
>
> ***Una filtración sin precedentes***
>
> *Una filtración que se ha volcado en un archivo de texto con un peso de 100GB, algo sencillamente brutal, y que cuenta con nada menos que 8.400 millones de contraseñas. Este archivo como suele ser habitual se ha filtrado en un foro que frecuentan hackers. Esta filtración masiva se conoce ya con el apodo de “RockYou2020” que viene rememorar a otra gran filtración conocida bajo este nombre en 2009. Parece ser que este archivo plagado de contraseñas no se surte solo de un mismo ataque, sino que parece una recopilación de contraseñas obtenidas en diferentes ataques a lo largo y ancho de la web en los últimos años.”*

En ese sentido, la situación expuesta se puede originar desde ambientes internos de la organización, particularmente ante la ausencia de una estrategia adecuada en ciberseguridad o por la exposición de factores externos donde cibercriminales exploran las posibilidades de obtener acceso a dispositivos o productos que son utilizados de manera habitual, siendo aprovechados como puertas traseras.

Lo anterior, al considerar que las credenciales comprometidas lideran los tipos de ciberataques en el 2021, según el estudio realizado por IBM[1] "Cost of a Data Breach Report 2021", resumido en la siguiente imagen:

Imagen No. 1
Los ciberataques más frecuentes en 2021



Fuente: Publicación del 25 de enero del 2022 de empresa TecnoSeguro[2], titulada "Las amenazas de Ciberseguridad de las que el Software "Nx" permanece seguro"

En cualquier caso, la recomendación de los expertos es fortalecer la ciberseguridad y no pasarle por alto, ya que los cibercrímenes crecen a un ritmo alarmante en todo el mundo.

1.2 Reutilización de contraseñas y su nivel de complejidad

El reutilizar contraseñas en múltiples sitios es una práctica habitual en los ecosistemas digitales, aunado a la falta de robustez en la definición de estas, lo cual conduce a grandes aumentos en el fraude.

A ese respecto, en el diario nacional "El Financiero" se publicó el 4 de diciembre del 2021, la nota "Estas son las contraseñas más usadas (y las más hackeadas)" donde expone una situación vinculada con la cultura de los usuarios al definir sus claves:

> *"La firma de seguridad informática ESET publicó un estudio de las 200 contraseñas más utilizadas en la web en 2021. No hay sorpresas.*

[1] International Business Machines (IBM) y es una de las corporaciones de tecnología e informática más famosas en el mundo.
[2] TECNOSeguro es la publicación on-line líder en audiencia para la industria de seguridad electrónica de habla hispana.

En el informe quedó demostrado que las combinaciones numéricas, fáciles de adivinar para los ciberdelincuentes, siguen siendo muy populares entre los usuarios.

Ocho de las diez contraseñas más utilizadas están compuestas por varias combinaciones numéricas, particularmente 123456, 123456789 y 12345 ocupan el primer, segundo y tercer lugar de la lista este año.

Junto con la preferencia por las diferentes combinaciones numéricas, se advirtió lo repetitivas que son las variaciones.

El reporte mostró más comportamientos nada sorprendentes:

—Uso de nombres: a una cantidad asombrosa de personas les encanta usar su propio nombre como contraseña, dice ESET.

—Música: Onedirection regresa a la lista de las contraseñas más comunes en varios países después de desaparecer misteriosamente de la lista de 2020.

—Fútbol: el Liverpool podría ser el equipo más popular del mundo, a juzgar por la cantidad de veces que se ha utilizado como contraseña.

—Automóviles: las marcas Ferrari y Porsche son las más populares cuando se trata de contraseñas incorrectas.

—Malas palabras: las malas palabras se utilizan con bastante frecuencia como contraseñas. Las investigaciones muestran que los hombres usan malas palabras como contraseñas con más frecuencia que sus contrapartes femeninas.

—Animales: delfín o dolphin ocupó el primer lugar entre las contraseñas relacionadas con animales en muchos países.

Si se repasan los resultados de los informes de contraseñas hackeadas de 2017, 2018, 2019 y 2020, las que más veces registraron filtraciones son precisamente las que combinan los mismos números.

Por ejemplo, 123456 se mantiene entre la primera y la segunda posición desde 2017 a 2021. También se repiten año tras año dentro de las primeras cinco posiciones, aunque en distinto orden, otras variantes como 123456789, 12345678 o password (esta no se me había ocurrido a la fecha).

ESET recalca que queda en evidencia lo populares que siguen siendo contraseñas extremadamente débiles. Además, si se toma como referencia solamente las 20 contraseñas más recurrentes, el tiempo para descifrarlas a través ataques de fuerza bruta y con sistemas informáticos en la mayoría de los casos es menor a un segundo."

Es decir, no solo hay riesgo por el ciberataque, sino por usuarios que propician oportunidades a los ciberdelincuentes, en este caso, usando contraseñas muy sencillas y fáciles de hackear. A ese respecto, en el Anexo 1 podrá visualizar la lista de claves más usadas durante 2020 según un estudio realizado por NordPass[3].

Además, se comparte en el Anexo 2 el artículo "Generadores de contraseñas seguras: una herramienta útil y de fácil acceso", publicado por ESET[4] el 05 de mayo del 2022, mencionado las recomendaciones para crear combinaciones, aplicativos para evaluar la seguridad de las claves, utilitarios para el almacenamiento de credenciales, entre otras herramientas, tiempo que le lleva a un cibercriminal descifrar una contraseña y demás tópicos de valor agregado para el nivel táctico y operativo.

Bajo ese contexto, expertos en seguridad comparten a diario consejos para fortalecer la cultura en los usuarios, por ejemplo, al recordarles la importancia de mantener en secreto las contraseñas, enseñarles a elegir una combinación robusta de caracteres, evitar la simplicidad, no repetir claves, utilizar gestores de credenciales, entre otras buenas prácticas.

En ese orden de ideas, valorando la necesidad de implementar soluciones tecnológicas modernas, orientadas a garantizar la verificación inequívoca de usuarios, la supervisión de comportamientos, la alerta temprana de amenazas y, por ende, evitando razonablemente el robo de datos confidenciales que puedan comprometer a la organización.

1.3 Autenticación multifactorial

El negocio del cibercrimen y la sofisticación técnica del fraude para conseguir las contraseñas de los usuarios, han generado advertencias sobre la obligación de los sistemas de información por aumentar el nivel de precisión correspondiente a confirmar la identidad de las personas que acceden a los recursos organizacionales.

Sobre el particular, en la nota periodística "Así funciona el mercado negro de contraseñas, un suculento 'negocio' para el cibercrimen", publicada por el diario español "El Heraldo" el 7 de mayo del 2022, se menciona la exigencia de aumentar el nivel de control ante las amenazas tecnológicas, a saber:

> *"Unos 12.000 ataques a sistemas informáticos de organismos públicos fueron gestionados el pasado año por el Centro Criptológico Nacional, el organismo dependiente del CNI encargado de la defensa de nuestras redes. Los ciberdelincuentes que atacaron esos ordenadores lo hicieron sin levantar sospecha con claves que habían adquirido en el mercado negro.*
>
> *Y es que la compraventa de todo tipo de datos se ha convertido en el suculento "negocio" del cibercrimen. En el infinito escaparate de la internet profunda crecen los piratas informáticos que con programas sofisticados roban paquetes de datos que venden a otros delincuentes que cometen más ataques, de forma que todos ganan dinero.*

[3] NordPass ha sido desarrollado por Nord Security, líder mundial en la industria dedicada a la ciberseguridad.
[4] Compañía de software especializada en ciberseguridad, fundada en 1987 y opera en más de 200 países.

(…) Con la pandemia y el aumento del teletrabajo que conlleva acceder de forma masiva con credenciales en accesos remotos más vulnerables, los programas de secuestro de datos o de chantaje, el "ransonware", han crecido hasta un 600 por ciento. En la mayoría de los casos nadie detecta este robo hasta el siguiente ataque en el que se emplean esas contraseñas para acceder de nuevo a los sistemas y provocar otros daños.

En la jornada celebrada en el Senado el subdirector del Centro Criptológico fue claro al explicar el modus operandi: "No hay manipulación ni hackeo del sistema, sino una entrada con una credencial válida que ha sido comprada en el mercado negro (...) Una vez dentro y sin levantar sospechas, se hacen con el control".

De estas vulnerabilidades alertaba también el Ministerio del Interior en su último informe sobre cibercriminalidad de 2020, donde apuntaba que los ataques a trabajadores a través de sus redes domésticas y dispositivos personales iban a incrementarse "con el objetivo de acceder a la infraestructura de la organización del empleado para conseguir otros fines, entre ellos el ciberespionaje".

Para hacer frente a este creciente fenómeno que pone en peligro la ciberseguridad pública y también la privada -hay más de tres millones de empresas-, desde el CNI y el Incibe insisten a la administración pública y aconsejan al sector privado que inviertan más en tecnología y que doten a sus sistemas de doble autentificación para sus usuarios, de forma que al delincuente le sea más difícil robar sus datos."

Bajo ese contexto, la autenticación de múltiples componentes utiliza distintos tipos de tecnología, combinando al menos dos factores de verificación. En ese sentido, las técnicas utilizadas hacen referencia a "algo de conocimiento del usuario", cierto "elemento de posesión" o a un "factor de injerencia", tal y como se señala en el siguiente cuadro:

Cuadro No. 1
Tipos de factores y tecnologías de autenticación

Factor de Autenticación	Tipo de solución	Ejemplo
Factor de conocimiento	- Contraseña, tal y como la digitada en nuestros computadores.	Digitada al ingreso del computador o correo electrónico
	- PIN.	Digitado al utilizar un cajero automático de un banco.
Factor de posesión	- Plástico de identificación.	Tarjeta de crédito o debido.
	- Token o aplicación de autenticación	Dispositivo o aplicativo que genera un código.
Algo que usted es (factor de inherencia	- Huellas dactilares.	Reloj marcador.
	- Reconocimiento facial.	Funcionalidad de dispositivos celulares, entre otros.

Fuente: Elaboración propia.

En otras palabras, si un factor se ve comprometido, un atacante todavía no accede, porque tendría que romper al menos una barrera más, antes de poder acceder a la cuenta del objetivo. Para tales efectos, entre los mecanismos de autenticación, valorados al momento de incrementar la combinación de controles, se destacan:

- **Pin o contraseña**: considerado como un factor de conocimiento para el usuario final, donde debe introducir correctamente la información que coincida con los detalles qué se almacenaron previamente en la base de datos.

- **Claves de seguridad**: este método consiste en la generación de una clave aleatoria e irremplazable, puede realizarse a través de tarjetas inteligentes, tokens (hardware y/o software), aplicativos informáticos móviles, entre otras herramientas dinámicas.

- **Datos biométricos**: identificación de forma precisa, mediante huellas dactilares; escaneo de retina; reconocimiento facial, voz e inclusive de comportamientos tales como la intensidad o la rapidez con que una persona teclea.

- **Mensaje de texto o voz**: Los códigos de acceso de un solo uso, se envían al correo electrónico, al dispositivo móvil o llamada, en cual notifica al usuario la clave a utilizar.

Aunado a lo anterior, en el Anexo 3 de esta misiva contiene la publicación "Este Día Mundial de la Contraseña consideren deshacerse de las contraseñas por completo" efectuada por Microsoft[5] el 5 de mayo del 2022, ampliando como reforzar o potencializar el uso de este tipo de mecanismos.

En ese sentido, la premisa de disponer de reconocimiento multifactorial puede prevenir incluso los ataques más sofisticados. Por ello, recomiendan utilizar al menos dos tecnologías diferentes para el proceso de autenticación, así evitando la probabilidad para descifrar la contraseña de un usuario en la organización.

1.4 Soluciones de autenticación sin contraseña

Estas iniciativas surgen como respuesta a los problemas reiterativos con el manejo habitual de las contraseñas; exponiendo a las organizaciones a niveles de fraude descontrolados, malas experiencias con los usuarios y altos costos operativos.

En ese sentido, tal y como se detalla en el artículo "Contraseñas en camino a la extinción, pero eso no es malo" publicado en la revista ITNow el 17 de enero del 2022, a saber:

> *"El exceso de contraseñas es una molestia, por no hablar de la creación y el recuerdo de contraseñas seguras que cumplan requisitos específicos. Según el Biometric Usage Study de Dell Technologies, crear, recordar y cambiar regularmente las contraseñas es considerado "una molestia" para el 62% de los trabajadores en Estados Unidos.*
>
> *Otro estudio de Dell, Brain on Tech, descubrió que cuando a los usuarios de todo el mundo se les presentaba una contraseña larga y difícil para acceder bajo presión de tiempo a un computador, su estrés aumentaba un 31% en cinco segundos… Y seguía aumentando incluso después de que los usuarios iniciaran la sesión con éxito."*
>
> *Estos resultados refuerzan que, para la mayoría de nosotros, una buena higiene de las contraseñas no es una prioridad: es, en cambio, una molestia. Tanto si se reutiliza la misma contraseña repetidamente, como si se utilizan contraseñas débiles o se escriben en una nota adhesiva, muchos de nosotros hacemos exactamente lo que nos han dicho que no hagamos."*

[5] Microsoft es una compañía multinacional, que diseña y comercializa programas informáticos y dispositivos electrónicos. Los inicios de esta fueron en la década de los 70.

No obstante, las soluciones sin contraseña han resonado desde hace algunos años, en su intento por prevenir el fraude, ya que los piratas informáticos simplemente no tienen nada por descifrar o robar a través de programa malignos, ataques cibernéticos o de ingeniería social, tal y como explica el Instituto Nacional de Ciberseguridad (INCIBE) de España en la publicación "Passwordless, el comienzo del fin de las contraseñas" del 7 de noviembre del 2019, al indicar:

> *"La contraseña es el método habitual utilizado por los usuarios para autenticarse en prácticamente todos los servicios, ya sean propios de la empresa o externos. Desde el acceso al correo corporativo, pasando por las redes sociales hasta llegar a la mayoría de los comercios online, las contraseñas son, en muchos casos, la única medida de seguridad que protege la cuenta frente a ciberdelincuentes. Pero el uso de contraseñas, como hoy lo conocemos, puede cambiar. Grandes organizaciones como Google, Mozilla o Microsoft están llevando el control de accesos a un nuevo paradigma denominado passwordless.*
>
> *(…) Los beneficios que aportará este método de autenticación son varios:*
>
> *-Las contraseñas dejarán de ser la única vía de acceso a los sistemas, utilizando una opción más segura como es el sistema de clave pública y privada.*
> *-Los principales métodos utilizados por los ciberdelincuentes, como son el phishing, ataques de fuerza bruta o contra contraseñas débiles, dejarán de funcionar.*
> *-Para acceder de forma fraudulenta a un sistema, los ciberdelincuentes tienen que estar en posesión del dispositivo, ya que en él se encuentra la clave privada, y del método elegido para su desbloqueo. Esto hace que resulte extremadamente complicado un acceso fraudulento al sistema.*
> *-Los usuarios no tendrán que recordar complejas contraseñas ya que utilizando métodos biométricos podrán acceder a su clave privada y por lo tanto a su cuenta.*
> *-El flujo de trabajo será mucho más ágil, ya que en muchas ocasiones los usuarios no tendrán que introducir ningún dato. Solamente con algo que poseen, como su huella dactilar, podrán acceder al sistema.*
> *-Aunque su uso pueda resultar similar en términos de seguridad que el ya conocido doble factor de autenticación, passwordless permitirá un manejo más simple, eficiente y seguro de los sistemas que lo implementen.*
>
> *El adiós a las contraseñas no es algo nuevo y muchos usuarios ya se están familiarizando con este paradigma. Actualmente la mayoría de los dispositivos móviles cuentan con componentes que permiten su desbloqueo por medio de biometría como la huella dactilar o reconocimiento facial, ofreciendo una experiencia de usuario más fluida. Además, la existencia de nuevos estándares, como FIDO2, está permitiendo integrar el passwordless en múltiples entornos y dispositivos como ya ha hecho Google con Android o Microsoft con Windows 10."*

Por ello, es relevante analizar minuciosamente estas posibilidades en el mercado de las TIC[6] y sus beneficios, claro está evaluando la capacidad de combinar e implementar métodos de autenticación vía software y hardware que mitiguen los riesgos asociados.

[6] Tecnologías de la información y las comunicaciones (TIC).

1.5 Módulos integrados de seguridad

Ante los requerimientos a nivel organizacional para garantizar el uso de contraseñas bajo determinados parámetros (robustez de la combinación, impedir repetición, periodicidad en el cambio, entre otros), evitar la creación de múltiples mecanismos de autenticación e inclusive mitigar el riesgo asociado con la administración de la cantidad de claves posibles para una persona; los especialistas han insistido durante años sobre la necesidad de implementar plataformas centralizadas que garanticen el adecuado manejo de la seguridad.

Entre las funciones o beneficios que se pueden obtener a través de estas soluciones, se tiene:

- Crea usuarios de manera estandarizada.
- Parametriza variables.
- Define niveles de acceso.
- Establece un único mecanismo de autenticación.
- Simplifica las labores de mantenimiento.
- Flexible ante cambios a nivel técnico o de negocio.
- Posibilita el seguimiento integrado de acciones, a través de bitácoras.
- Otorga viabilidad para generar reportes especializados.

De esa manera, ese tipo de sistemas son oportunos al integrar a todo el conjunto de aplicaciones informáticas, disminuyendo considerablemente los riesgos asociados a múltiples mecanismos de autenticación; desarticulación en la definición de privilegios; ausencia de mantenimiento y supervisión en los perfiles de acceso; entre otras situaciones que denotan posibles tecnologías sin la capacidad de detectar y prevenir el fraude.

2- CONSIDERACIONES FINALES

En virtud de la evolución constante de las TIC y los riesgos a los cuales se ha visto expuesta la ciudadanía, ante el efecto natural del uso y aprovechamiento de las soluciones tecnológicas, se debe prestar mayor atención a la ciberseguridad.

Tal y como cita la nota periodística del 27 de junio del 2022 en el diario nacional “El observador”, en el titular “Estudio del Gobierno detecta serias debilidades en seguridad informática del Estado”, al exponer los resultados de vulnerabilidades detectadas en Costa Rica, entre ellas algunas asociadas con la gestión de contraseñas, a saber:

> *“Un análisis realizado por el actual Gobierno de Rodrigo Chaves detectó una serie de debilidades en los sistemas informáticos de las distintas instituciones públicas.*
>
> *El reporte recoge datos de 226 instituciones, visitadas por personal del Instituto Costarricense de Electricidad (ICE), que recopiló la información.*
>
> *Algunos de los principales hallazgos son que, de las 226 entidades analizadas, 188 de ellas no cuentan con personal especializado en ciberseguridad. Además, 41 instituciones no realizan copias de seguridad en sus sistemas.*

Un 46% de ellas no poseen plataformas de seguridad informática y 99 de las 226 no han completado el doble factor de autenticación, con lo que se podrían evitar gran cantidad de intrusiones, según dijo el ministro de Ciencia, Tecnología y Telecomunicaciones (MICITT), Carlos Enrique Alvarado."

Así las cosas, es menester de esta Auditoría hacer énfasis sobre el tema desarrollado en este oficio, con el objetivo de proporcionar insumos que incentiven en el corto y mediano plazo, el mejoramiento priorizado, secuencial y continuo de la seguridad, particularmente con lo referente a soluciones de autenticación en sistemas informáticos.

Entre los aspectos a resaltar, poniendo en marcha una estrategia en ciberseguridad que atienda de forma oportuna los temas de verificación de identidad; cumplimiento de normas; estandarización de mecanismos; mejora continua de los factores de autenticación; monitoreo de vulnerabilidades; y la implementación e innovación de herramientas especializadas.

Además, reconociendo que la cultura informática debe ser más fuerte y/o segura, incluyendo la responsabilidad de todos para estar preparados ante el crecimiento de amenazas cibernéticas y el nivel de respuesta a ese hecho.

Lo anterior, siendo consecuente con lo indicado en "Las Normas técnicas para la gestión y el control de las Tecnologías de Información" emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), al señalar en el Apartado XI, Seguridad y Ciberseguridad, lo siguiente:

"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."

Además, con fundamento a lo indicado en las políticas, normas y guías de seguridad informática institucional, referentes a la temática citada en el epígrafe; recomendaciones emitidas por la Auditoría o consultorías en TIC; así como los marcos referenciales de mejores prácticas; todos vigentes al contexto actual de la Institución.

En virtud de lo expuesto, este Órgano Fiscalizador brinda la presente asesoría, con el propósito de fortalecer los mecanismos de seguridad en los sistemas de la Institución, así como enfrentar con éxito los eventos adversos que puedan presentarse, garantizando un marco adecuado para el resguardo de la información institucional y de la ciberseguridad.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.07.13 11:44:43 -06'00'

Lic. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

Anexos (1)

1- Contraseñas más usadas durante 2020 según estudio realizado por NordPass, 2021.
2- Artículo "Generadores de contraseñas seguras una herramienta útil y de fácil acceso", ESET, 2022.
3- Publicación "Este Día Mundial de la Contraseña consideren deshacerse de las contraseñas por completo" efectuada por Microsoft el 5 de mayo del 2022.

C. Auditoría