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

AS-AATIC-186-2022
6 de septiembre de 2022

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

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

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

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

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

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

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

Estimados(as) señores(as):

ASUNTO: Oficio de Asesoría Referente a Aplicaciones que Originan Descargas de Malware.

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, específicamente en su rol de asesor, esta Auditoría informa sobre las amenazas generadas por aplicaciones que originan descargas de malware y de un posible resurgimiento del malware de Microsoft office que afecta el manejo de los datos en términos de robo, cifrado o borrado de estos, además de un alto riesgo de alterar o secuestrar funciones básicas del computador, así como el espionaje de la actividad sin conocimiento o permiso de acceso. Todo esto con el fin de que se implementen acciones preventivas, y evitar la materialización de riesgos en materia de Ciberseguridad y que se vuelvan a presentar eventos como el del pasado 31 de mayo.

ANTECEDENTES

Como es del conocimiento, el 31 de mayo 2022, se registró en horas de la madrugada un ciberataque en contra de los servidores e infraestructura de telecomunicaciones de la CCSS, el cual obligó a la institución a desconectar todos los sistemas informáticos, a fin de determinar el nivel de afectación.

De esa forma, el diario La República publicó el 31 de mayo 2022, "Hackers tenían como objetivo el robo de información y las bases de datos de la Caja", detallando:

> *"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.*
>
> ***La modalidad de vulneración de los sistemas informáticos utilizado por los delincuentes fue por medio de "ransomware**", el cual, consiste en el robo de información y bases de datos, sin que se conozca el responsable del daño". (La negrita no es del original)*

ASPECTOS GENERALES SOBRE MALWARE

Como es conocido, el malware hostil, intrusivo e intencionadamente dañino, intenta invadir, dañar o deshabilitar computadoras, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Aunque el malware es muy difícil que pueda dañar el hardware de los sistemas o el equipo de red, sí puede robar, cifrar o borrar los datos, alterar o secuestrar funciones básicas y espiar la actividad sin su conocimiento o permiso.

El malware puede penetrar cuando se navega por sitios web no autorizados, se da clic en demostraciones de juegos, descarga de archivos de música infectados, se instala nuevas barras de herramientas de un proveedor desconocido, se instala software de una fuente dudosa, se abre un adjunto de correo electrónico malicioso o descarga de prácticamente cualquier cosa de la web en un dispositivo que carece de una aplicación de seguridad antimalware de calidad.

Las aplicaciones maliciosas pueden ocultarse en otras aparentemente legítimas, especialmente cuando se descargan a través de sitios web o mensajes y no desde una App Store segura. Es importante, por tanto, prestar atención a los mensajes de advertencia de los mecanismos de seguridad que tiene implementado la institución al instalar las aplicaciones, sobre todo si solicitan permiso para acceder a su correo electrónico u otro tipo de información personal.

- **Tipos de Malware**

Dentro de la galería de malware se pueden mencionar a continuación los más comunes:

- ✓ **El adware**: es un software no deseado diseñado para mostrar anuncios en la pantalla, normalmente en un explorador. Suele recurrir a un método subrepticio: bien se hace pasar por legítimo, o bien se adosa a otro programa para engañar al usuario e instalarse en su computador, tableta o dispositivo móvil.

- ✓ **El spyware**: es malware que observa las actividades del usuario en el computador en secreto y sin permiso, y se las comunica al autor del software.

- ✓ **Un virus** es malware que se adjunta a otro programa y, cuando se ejecuta —normalmente sin que lo advierta el usuario—, se replica modificando otros programas e infectándolos con sus propios bits de código.

- ✓ **Los gusanos**: son un tipo de malware similar a los virus, que se replica por sí solo con el fin de diseminarse por otros computadores en una red, normalmente provocando daños y destruyendo datos y archivos.

- ✓ **Un troyano, o caballo de Troya**: es uno de los tipos de malware más peligrosos. Normalmente se presenta como algo útil para engañar al usuario. Una vez que está en el sistema, los atacantes que se ocultan tras el troyano obtienen acceso no autorizado al computador infectado. Desde allí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware.

- ✓ **El ransomware**: es un tipo de malware que bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos. El ransomware se ha reconocido como el arma preferida de los delincuentes informáticos porque exige un pago rápido y provechoso en criptomoneda de difícil seguimiento. El código que subyace en el ransomware es fácil de obtener a través de mercados ilegales en línea y defenderse contra él es muy difícil.

- ✓ **El rootkit**: es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado. Normalmente, también se diseña de modo que permanezca oculto del usuario, de otro software del sistema y del propio sistema operativo.

- ✓ **Un registrador de pulsaciones de teclas:** es malware que graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito.

- ✓ **La minería de criptomonedas maliciosa, denominada también minería fortuita o cryptojacking**: es un malware cada vez más prevalente instalado por un troyano. Permite que otras personas utilicen su computador para hacer minería de criptomonedas como bitcoin o monero. Los programas maliciosos de minería de criptomonedas utilizan los recursos de su computadora, pero envían los coins obtenidos a sus propias cuentas, no a las del propietario del equipo. En pocas palabras, un programa de minería de criptomonedas malicioso, le roba recursos para hacer dinero.

- ✓ **Los exploits**: son un tipo de malware que aprovecha los errores y vulnerabilidades de un sistema para que el creador del exploit pueda asumir el control. Los exploits están vinculados, entre otras amenazas, a la publicidad maliciosa, que ataca a través de un sitio legítimo que descarga contenido malicioso inadvertidamente desde un sitio peligroso. A continuación, el contenido dañino intenta instalarse en el ordenador tras una descarga involuntaria. Ni siquiera es necesario hacer clic. Todo lo que tiene que hacer es visitar un sitio bueno el día equivocado.

- ➢ **Proceso de Infección**

Según la plataforma de información electrónica SpringerLink (2019), por ejemplo, para que un Ransomware se propague en una organización y provoque una afectación importante, se debe seguir una serie de pasos explicados por el modelo Cyber Kill Chain (CKC), presentado en la imagen:

Figura 1
Diagrama Proceso de Infección

Fuente: SpringerLink, 2019.

Es importante hacer hincapié que los grupos criminales utilizan técnicas de ingeniería Industrial o de **reconocimiento**, esta es la puerta de entrada y utilizan diversas técnicas entre ellas el pretexto llamativo para una persona o inclusive la organización, un tema que haga sentido e interese para luego dar paso al ya conocido phishing o "pesca", logrando obtener de manera voluntaria información relevante.

Sin embargo, no es la única técnica para obtener datos relevantes, también el Vishing, que es similar al phishing pero en la que se utilizan llamadas telefónicas, muy conocidas en nuestro contexto; el Baiting gancho o cebo que consiste en dejar supuestamente olvidados en lugares públicos dispositivos de almacenamiento secundario como llaves "maya" o USB discos externos para que los transeúntes los recojan, los utilicen en sus dispositivos y comprometan sus equipos; y por último, menos conocido pero psicológicamente muy efectivo es el "Quid pro quo" del latín una "cosa por otra", que se refiere por ejemplo a una llamada de personal de soporte técnico que indica que se debe atender su equipo de manera remota, pero para esto necesita el usuario y contraseña de su equipo.

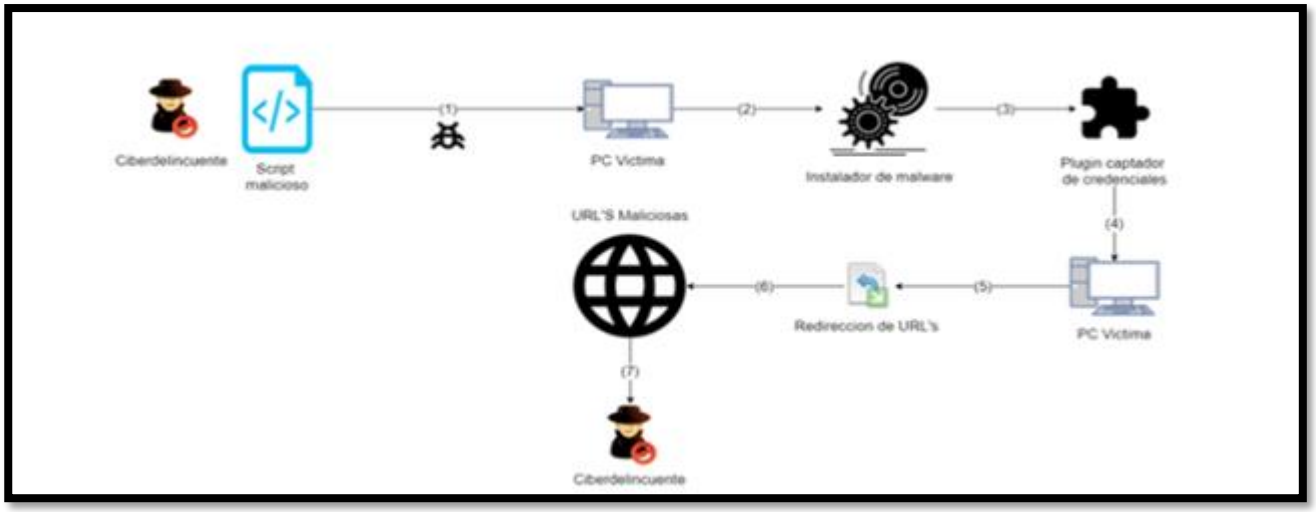
El siguiente paso es la ***intrusión***, que en la mayoría de los casos se da por correos electrónicos con adjuntos comprometidos; de allí la importancia de identificar cuando un correo electrónico es malicioso, sobre todo si es un subtipo de phishing de mayor impacto conocido como "whaling" o ballenera, que se refiere a pesca masiva, en este caso los correos suplantan a un superior jerárquico reconocido de la organización. El tercer paso es la ***explotación*** de los sistemas computacionales desde lo interno, para dar paso a la ***elevación de privilegios*** o toma de control. Este punto es especialmente importante puesto que además de controlar el dispositivo, el malware puede iniciar el ***desplazamiento lateral*** o explotación de otros equipos en la misma red aprovechando vulnerabilidades similares, pero esta vez con los permisos y autorizaciones del equipo afectado.

En este punto inicia la afectación exponencial y posterior ***ofuscación*** o encubrimiento de comunicaciones con los servidores de mando, así como el control del grupo criminal en espera de la señal del ataque, mejor conocida como ***denegación de servicio*** y posterior ***filtración*** de datos.

- **Troyano basado en una Extensión de Chrome**

Para brindar una perspectiva más real a continuación se expone un ejemplo de un análisis inicial presentado por la compañía CSIRT, de Colombia relacionado a un "Troyano" bancario basado en una extensión de Chrome.

Figura 2
Diagrama Troyano basado en extensión de Chrome



Fuente: www.csirtasobancaria.com

En el análisis inicial por parte del CSIRT se encuentra que la infección preliminar en el equipo víctima se realiza mediante la ejecución de un script con código malicioso, que permite la descarga del malware más los complementos necesarios para el ataque, entre ellos un instalador legítimo de Google Chrome Canary y la extensión maliciosa. Seguidamente se realiza el proceso de instalación del malware, con un nuevo explorador configurado dentro de la maquina afectada, se inicia el proceso de configuración del plugin. Después, dentro de la maquina víctima se inicia el nuevo explorador con la configuración del plugin para captar las credenciales, se realiza el redireccionamiento de los dominios legítimos, se ingresa a los dominios maliciosos y el ciberdelincuente captura la información de las páginas phishing.

En síntesis, se encarga de modificar el registro de Windows para utilizar un servidor proxy malicioso, que será el encargado de resolver las peticiones hechas a las URL's legítimas y redireccionarlas a las páginas web que contienen el Phishing.

SOBRE LAS APLICACIONES QUE ORIGINAN DESCARGAS DE MALWARE

Según la empresa de software estadounidense Netskope, dedicada a proporcionar una plataforma de seguridad informática en datos, defensa contra amenazas en las aplicaciones de la nube, la infraestructura de la nube y web. Menciona más de 100 aplicaciones diferentes que originan descargas de malware, también alerta de un resurgimiento del malware de VBA (Visual Basic para aplicaciones).

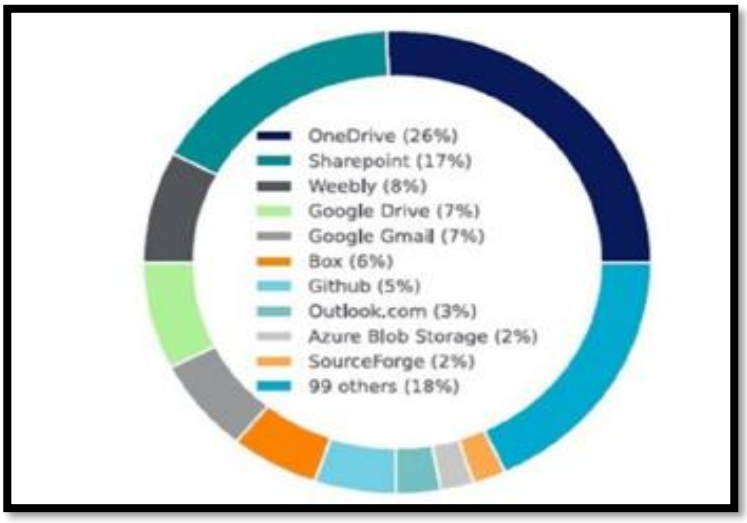
Se dio a conocer la identificación de 105 aplicaciones que originan descargas de malware, según revela el informe más reciente de Netskope Threat labs, correspondiente a junio de 2022.

Es importante mencionar y tener en cuenta que las aplicaciones de "OneDrive", "Sharepoint" y "Weebly" ocupan los primeros puestos dentro de la lista de aplicaciones, siendo las tres que más originan descargas de malware. A este respecto, llama la atención que Weebly sigue atrayendo la atención de los expertos en amenazas debido al patrón de entrega, a través de **archivos PDF** maliciosos que redirigen a las víctimas a sitios web de phishing, spam, fraude y distribución de malware. La misma estrategia se está utilizando en Squarespace, Wordpress, así como en otras plataformas.

- ✓ **Principales aplicaciones que originan descargas de malware junio 2022**

En la siguiente imagen se muestra la lista con las principales apps de descarga de malware.

Figura 3
Principales Apps para descargas de malware junio 2022



Fuente: Netskope Threat Labs

El informe menciona que a raíz de campañas en las que se utilizó como medio el correo electrónico durante el mes de junio de 2022, dio como resultado un aumento en la propagación de malware, lo que propició la subida en la clasificación de las apps Baidu Object Storage, Google Gmail y Outlook.com. Por su parte para nuestro principal interés véase que la app de Google Gmail que es de descarga masiva en nuestros dispositivos de sistema operativo Android y que corresponde al complemento de las cuentas de Google necesarias para poder acceder a la gama de apps de la tienda virtual “Play Store”, aparece en la lista con un aumento considerable.

De igual forma la App de Outlook.com la cual actualmente es de uso de la institución de manera masiva y que ha venido a ocupar un nivel importante de uso en la gestión de la Caja Costarricense de Seguro Social; podría elevar el riesgo de contaminación por malware, razón por la cual es importante tomar las medidas necesarias para proteger nuestros sistemas y equipos.

En este contexto, el informe también destaca que los cinco primeros dominios de phishing del mes estaban alojados en dos plataformas del ranking: Weebly y Blogger, seguidamente los investigadores de Netskope observaron un aumento del tráfico hacia los sitios web de phishing alojados en plataformas como Azure Blob (es la solución de almacenamiento de objetos de Microsoft para la nube). Blob Storage está optimizado para el almacenamiento de cantidades masivas de datos no estructurados, como texto o datos binarios.
Las cinco primeras familias de malware en junio de 2022 fueron:

1. PhishingX, utilizado en PDF para el phishing.
2. AgentTesla, troyano de acceso remoto o RAT, por sus siglas en inglés, en uso desde 2014.
3. Zmutzy, escrito en .NET para robar credenciales y carteras de criptomonedas.
4. Abracadabra, en macros de hojas de cálculo de Excel.
5. Razy, utilizado para el robo de datos y anuncios maliciosos.

Figura 4
Gráfico de cinco primeras familias de malware en junio 2022

Fuente: Netskope Threat Labs

- **Resurgimiento del Malware de Office**

Por otra parte, como resultado de la decisión de Microsoft de habilitar de nuevo los macros de (Visual Basic para Aplicaciones, lenguaje de programación de Microsoft) para los archivos descargados de internet, Netskope Threat Labs alertó de las consecuencias que esta medida podría tener para los usuarios.

> *"Tras la resolución tomada por Microsoft a principios de año de restringir las macros de Excel 4.0 y, posteriormente, las de VBA para los archivos descargados de internet, los documentos maliciosos de Office disminuyeron", afirma Ray Canzanese, director del Laboratorio de Amenazas de Netskope.*
>
> *"Sin embargo, el 7 de julio de 2022, Microsoft revirtió silenciosamente el curso y volvió a habilitar las macros de VBA para los archivos descargados de internet. Esperamos que los atacantes continúen justo donde lo dejaron, y pronto veremos un aumento en los documentos maliciosos de Office".*

En relación con lo anterior, según datos de la plataforma Netskope Security Cloud, el porcentaje de malware de Office detectado disminuyó progresivamente tras la decisión de Microsoft. Así, a partir de febrero, los documentos de Office representaron menos del 15 % de todo el malware, mientras que la mayor parte de los últimos cinco meses estuvieron por debajo del 10 %. Estos resultados contrastan con los del año anterior, cuando los documentos de Office supusieron el 35 % de todo el malware desde febrero y más del 25 % del malware durante la mayor parte de la segunda mitad de 2021.

A raíz de lo anteriormente mencionado, en vista de la utilización en la institución de la herramienta de Excel es recomendable la anulación de los valores predeterminados y la deshabilitación de los macros de VBA, esto para poder proteger contra macros maliciosos y los demás riesgos asociados.

OBSERVACIONES EFECTUADAS POR LOS EXPERTOS.

Por lo anterior, los expertos en esta temática han emitido recomendaciones generales para contrarrestar las posibilidades de que se materialicen vulnerabilidades mediante estos mecanismos, entre ellas:

- ✓ Limitarse a utilizar fuentes de confianza para las aplicaciones móviles y de escritorio e instalar únicamente aplicaciones de buena reputación, descargadas directamente del sitio del proveedor, jamás de ningún otro sitio, esto de acuerdo con las políticas y normas de seguridad institucionales.

- ✓ Estar atentos y saber detectar los ataques escondidos en cebos contaminados, por ejemplo; junto con una oferta de acelerador de Internet, un nuevo gestor de descargas, un limpiador de disco duro o un servicio de búsqueda web alternativo.

- ✓ Los ataques de malware no funcionarían sin el componente más importante que es el factor humano. Es decir, una versión crédula de la persona que abre sin pensar un adjunto de correo electrónico que no reconoce o hace clic en algo procedente de una fuente no fidedigna y lo instala.

- ✓ Aunque se instale algo de una fuente fidedigna, si no se presta atención a la petición de permiso para instalar al mismo tiempo otro software empaquetado, podría instalarse software que no quiere. Este software adicional se presenta a menudo como un componente necesario, pero no suele serlo.

- ✓ También debemos incluir una situación de infección con malware de la que el usuario no tiene culpa alguna, porque es posible incluso que el hecho de visitar un sitio web malicioso y ver una página o un rótulo publicitario tenga como resultado una descarga involuntaria de malware.

- ✓ Por otra parte, si no se ejecuta un programa de seguridad adecuado, se sigue teniendo la responsabilidad de la infección de malware y sus consecuencias.

- ✓ Es importante monitorear si se observa un nombre de dominio que termine con un conjunto de letras extraño, es decir, algo distinto de “com, org, edu o biz”, por mencionar algunos ejemplos, ya que esto puede indicar que se trata de un sitio web peligroso.

- ✓ Se debe de evitar hacer clic en anuncios emergentes mientras se navega por Internet. No es recomendable abrir los adjuntos de correo electrónico no solicitados ni abrir software de sitios web poco fidedignos o de redes de transferencia de archivos punto a punto.

- ✓ Es importante asegurarse de que el sistema operativo, navegadores y complementos están siempre actualizados, porque mantener el software con parches puede bloquear a los delincuentes de Internet.

- ✓ En el caso de los usuarios móviles, se debe de descargar las aplicaciones sólo de las tiendas autorizadas. Cada vez que se descargue una aplicación, se debe de comprobar básicamente antes las calificaciones y los comentarios. Si una aplicación tiene una calificación baja y pocas descargas, es mejor evitarla.

- ✓ No se debe descargar aplicaciones de fuentes de terceros. La mejor manera de asegurarse de cumplir esto es desactivar esta función en los dispositivos.

- ✓ No dar clic en enlaces extraños no verificados de correos electrónicos, mensajes de texto y mensajes de WhatsApp de origen desconocido, por ejemplo. Los enlaces extraños de amigos y contactos deben evitarse también, a menos que haya verificado que son seguros.

La organización puede evitar que sus redes se vean amenazadas por aplicaciones maliciosas si crean políticas robustas de seguridad móvil y despliegan una solución de seguridad móvil que pueda exigir el cumplimiento de esas políticas. Esto es vital en el entorno empresarial de hoy en día, en el que múltiples sistemas operativos están en funcionamiento en diversos lugares y dispositivos, en este caso con la apertura del teletrabajo el riesgo se eleva, mismo que debe de ser instruido y capacitado para salvaguardar la red de sistemas.

Por último, es importante que la Institución disponga de un buen programa antimalware, así como incluir protección por capas (la capacidad de analizar y detectar malware como adware y spyware, a la vez que mantiene una defensa proactiva en tiempo real que puede bloquear amenazas como el ransomware). El programa de seguridad debe proporcionar también desinfección para corregir cualquier cambio del sistema realizado por el malware limpiado para que todo vuelva a la normalidad.

CONSIDERACIONES FINALES.

En este sentido, esta Auditoría informa sobre lo descrito con el objetivo de que se analice la información expuesta y se refuercen los mecanismos de ciberseguridad de considerarse la posible materialización de riesgos, una vez que se hayan reestablecido los servicios tecnológicos institucionales.

Lo anterior, en apego a lo indicado en 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 “Seguridad y Ciberseguridad”, a saber:

> *“XI. SEGURIDAD Y CIBERSEGURIDAD*
>
> *La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.*
>
> *La Unidad de TI, basado en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información (…).*
>
> *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 (…)”.*

En virtud de lo expuesto, se da conocer la información descrita, con el propósito de que sea sometida a valoración y revisión por parte de la Administración, con base a los resultados de las aplicaciones que descargan malware y a las recomendaciones emanadas, de manera que se puedan definir o implementar estrategias y acciones específicas, dentro de las cuales se pueden considerar informar y capacitar al personal en esta materia, acorde a las políticas y normas de seguridad informática de la institución, así como las observaciones dadas por los expertos. Lo anterior para coadyuvar al cumplimiento de los objetivos institucionales, garantizando un marco adecuado para el resguardo de la información institucional y de la seguridad informática, así como de la continuidad en la prestación de los servicios.

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2022.09.06 16:21:34 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/EGC/lbc

C. Doctor Roberto Cervantes Barrantes, gerente, Gerencia General -1100
Auditoría