¿CÓMO PROTEGER TU VIDA DIGITAL HOY?

Una guía de Ciberseguridad

Comisión de Ciencia y Tecnología
Asociación del Personal Legislativo
Norberto Di Próspero | Secretario General

INTRODUCCIÓN

La Comisión de Ciencia y Tecnología de APL está conformada por compañero/as de los cinco sectores del Congreso de la Nación y de varios espacios institucionales del gremio. A través de distintas iniciativas bregamos para que las y los trabajadores puedan conocer los beneficios y riesgos que surgen en una era digital.

Por ello hemos recompilamos la siguiente guía a fin de contribuir al conocimiento en materia de seguridad de la informaación, ofreciendo consejos, herramientas, apoyo y una guia de buenas practicas para proteger la información de los agentes del Congreso de la Nación.

Nuestra premisa es trabajar sobre la información al respecto de la temática que esta en constante transformación, generando vínculos y uniendo lazos de manera interna.

Es fundamental que los avances tecnológicos y su aplicación sean interpelados por las organizaciones de todos los ordenes para que la innovación nunca sea en detrimento de la clase obrera y favorezca en generar más y mejor la tarea.

ÍNDICE

NOCIONES BÁSICAS

PROTECCIÓN DE DATOS

La protección de datos abarca las acciones preventivas y correctivas que las entidades implementan para salvaguardar la información, con el objetivo de garantizar su confidencialidad, disponibilidad, integrida y autenticidad.

DISPONIBILIDAD

La accesibilidad de la información se refiere a su capacidad para estar disponible para aquellos usuarios, procesos o aplicaciones autorizados en el momento en que lo necesiten.

AUTENTICACIÓN

La autenticación es la cualidad que permite reconocer de manera única al individuo o proceso responsable de crear o editar la información.

INTEGRIDAD

La integridad es el principio que persigue conservar la información sin alteraciones no autorizadas.

CONFIDENCIALIDAD

La confidencialidad se refiere a la característica que evita la revelación de información a personas, entidades o procesos no permitidos.

CIBERSEGURIDAD

La ciberseguridad representa un campo interdisciplinario dentro del ámbito informático, dedicado a examinar y evaluar una amplia gama de recursos y metodologías destinadas a resguardar los activos de información. Su misión abarca la identificación y gestión de amenazas que amenazan la integridad, confidencialidad y disponibilidad de los datos procesados, almacenados y trasladados a través de los sistemas de información interrelacionados. Este dominio de estudio se caracteriza por su enfoque integral en la detección y neutralización de riesgos que pueden impactar la seguridad de la información en un entorno digital cada vez más interconectado y dinámico. Además, busca implementar estrategias proactivas para anticipar y responder eficazmente a los desafíos emergentes en materia de ciberseguridad en el panorama tecnológico actual.

CIBERDEFENSA

La ciberdefensa engloba un conjunto de estrategias, tácticas y operaciones tanto proactivas como reactivas que se llevan a cabo en el entorno de las redes, sistemas, dispositivos, conexiones y personal de los recursos informáticos y de telecomunicaciones relacionados con la defensa. Su propósito es garantizar el adecuado funcionamiento y la integridad de las misiones o servicios para los cuales fueron concebidos estos recursos, al mismo tiempo que se previene y se contrarresta cualquier intento por parte de actores hostiles de utilizarlos con fines contrarios a los intereses de la defensa y la seguridad nacional. Este enfoque integral implica la implementación de medidas de protección activas y pasivas, así como la monitorización constante y la capacidad de respuesta ágil frente a posibles amenazas cibernéticas.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

ADMINISTRACIÓN DE CONTRASEÑAS - DOBLE FACTOR

PROBLEMA

Es desaconsejable emplear la misma contraseña para varios servicios en línea. Esto se debe a que si alguna vez se produce un incidente de seguridad o si por descuido se filtran nuestras credenciales de acceso junto con nuestra dirección de correo electrónico o nombre de usuario, todos nuestros servicios estarían en riesgo.

RECOMENDACIÓN

Se recomienda emplear un gestor de contraseñas para generar y almacenar varias contraseñas seguras, eliminando así la necesidad de recordarlas o apuntarlas. Además, es crucial activar la autenticación de dos factores en nuestros servicios más sensibles para reforzar su seguridad de manera efectiva.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

ESCRITORIOS LIMPIOS - REDES LIMPIAS

PROBLEMA

Es común dejar notas o archivos con datos confidenciales en nuestros lugares de trabajo, lo que los hace accesibles para cualquier individuo que tenga acceso físico a nuestros escritorios. Del mismo modo, al utilizar redes sociales o navegar en internet, la información que proporcionamos en formularios, servicios web o plataformas sociales puede ser delicada y ponernos en riesgo si es obtenida por un atacante.

RECOMENDACIÓN

El phishing es una de las tácticas de ingeniería social más reconocidas y riesgosas, que puede llevarse a cabo mediante correo electrónico, mensajes de texto o llamadas telefónicas. La estrategia principal del phishing consiste en inducir a la víctima a hacer clic en un enlace hacia un sitio web fraudulento, simulando ser una entidad legítima y solicitando información confidencial bajo falsos pretextos, como haciéndose pasar por un técnico o utilizando réplicas de sitios web reales.

PHISHING - INGENIERÍA SOCIAL

PROBLEMA

La ingeniería social comprende diversas estrategias y técnicas utilizadas para obtener información sobre individuos o entidades.
Su finalidad es obtener la mayor cantidad de datos posibles con el objetivo de llevar a cabo ataques informáticos específicos o engañar y acceder a información confidencial.

Una de las técnicas de ingeniería social más conocida y peligrosa es el phishing. Se disparan por correo electrónico, mensaje de texto o a través de una llamada telefónica.
Los ataques de phishing se concretan cuando la víctima ingresa a un enlace de un sitio web malicioso; utilizando una copia de un sitio web real con el objetivo de que la víctima ingrese allí información sensible.

PHISHING - INGENIERÍA SOCIAL

RECOMENDACIÓN

Si se trata de una llamada telefónica es importante verificar con quién nos estamos comunicando antes de responder preguntas cuyas respuestas puedan contener información sensible personal o de alguna organización, al igual que al efectuar alguna operación riesgosa (ej. transacción de dinero). También se recomienda generar un segundo medio de contacto para asegurar la identidad.

Cuando el phishing se manifiesta a través de enlaces (links o direcciones URL) dentro de correos electrónicos o mensajes de texto es importante no acceder directamente a dichos enlaces; si no, escribirlos manualmente en un navegador para corroborar su legitimidad.

También es recomendable verificar el remitente del correo recibido.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

WIFI PÚBLICOS - HTTPS

PROBLEMA

Cuando nos conectamos a redes WiFi públicas o usamos contraseñas que se comparten, corremos el riesgo de comprometer nuestra seguridad y privacidad en línea. Si alguien malintencionado está en la misma red WiFi, podría espiar el tráfico y acceder a información confidencial, como contraseñas, correos electrónicos y otros datos sensibles. Esto es más probable si la conexión no está protegida mediante cifrado, como ocurre cuando no vemos el candado verde en la barra de direcciones del navegador.

RECOMENDACIÓN

Cuando estés en una red pública, evita enviar datos importantes y asegúrate de que los sitios web que visites tengan el candado verde en la dirección, eso significa que la información está protegida.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

DISPOSITIVOS EXTERNOS

PROBLEMA

Debemos ser precavidos al usar dispositivos desconocidos, como computadoras prestadas o dispositivos USB, ya que podrían estar infectados con software malicioso diseñado para robar nuestra información personal y dañar nuestros equipos.

RECOMENDACIÓN

Es importante evitar conectar dispositivos externos que no conocemos o que traemos de casa a las computadoras de la red de trabajo. Si necesitamos revisar su contenido, es mejor conectarlos a una computadora con un antivirus y que no esté conectada a la red.

Además, debemos tener precaución al usar computadoras de terceros, ya que podrían tener software que registra las teclas que presionamos, lo que podría resultar en la obtención de nuestras credenciales u otros datos sensibles.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

ACTUALIZACIONES - EN PC Y EN MÓVIL

PROBLEMA

La causa de la mayoría de las brechas de seguridad es el software desactualizado.
Cuando se encuentra una vulnerabilidad en un activo tecnológico, sea a través de software o hardware, se publica un parche de actualización, que debe ser instalado lo antes posible para remediar el problema de seguridad.

RECOMENDACIÓN

Asegurarse de tener todas las aplicaciones de todos los dispositivos en su última versión, desde el firmware, el sistema operativo y cada uno de los programas instalados. Asimismo, intentar no manipular información sensible en sistemas sin soporte oficial o desactualizados.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

ARCHIVOS SOSPECHOSOS

PROBLEMA

Solemos recibir archivos sospechosos de terceros o los descargamos de enlaces dudosos. Muchos tipos de malware están ocultos en archivos comunes, como programas ejecutables, documentos de texto, imágenes o videos, y a menudo no son detectados fácilmente por antivirus desactualizados.

RECOMENDACIÓN

Si existen dudas sobre algún programa o archivo, siempre es recomendable escanearlo con un antivirus que tenga sus bases de datos actualizadas. También puedes optar por utilizar un servicio de antivirus actualizado regularmente para realizar un análisis exhaustivo.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

BACKUPS - EN DISTINTOS LUGARES Y REGULARES

PROBLEMA

La información es el activo más importante de cualquier organización, por esta razón cada día son más frecuentes los ataques informáticos que se aprovechan de cualquier tipo de vulnerabili- dad e intentan secuestrar la información; ya sea mediante su cifrado, para luego pedir remune- ración económica para su restauración, filtrando dicha información por un precio o utilizándose para otro tipo de estafa o fraude.

RECOMENDACIÓN

Además de contar con la mayor cantidad de me- dios de seguridad posibles es muy importante contar con copias de seguridad de los activos de información críticos (sensibles) almacenados con técnicas de cifrado () avanzadas y resguardados en distin- tos medios y lugares físicos.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

CONTRASEÑAS POR DEFECTO

PROBLEMA

Los problemas de seguridad suelen originarse por configuraciones deficientes en los dispositivos conectados a la red. Muchos dispositivos, como routers, repetidores y dispositivos como cámaras web o asistentes de hogar, vienen con contraseñas predeterminadas que son ampliamente conocidas. Esto les brinda a los atacantes la oportunidad de explotar esa información para su beneficio.

RECOMENDACIÓN

Es fundamental reemplazar las contraseñas predeterminadas en dispositivos y servicios por otras personalizadas.

Además, es importante establecer una política para cambiar estas contraseñas periódicamente, ajustando la frecuencia según la cantidad de personas que tengan acceso a ellas durante un período de tiempo determinado. Esto aplica no solo a entornos empresariales, sino también en el hogar.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

SEGURIDAD Y PRIVACIDAD EN LA COMUNICACIÓN

PROBLEMA

En la actualidad, muchas de las estafas y los fraudes se producen a través de la suplantación de identidad de intermediarios o ataques avanzados de ingeniería social. Una vez que el medio de comunicación con un agente confiable es intercedido, comienza la obtención de la información sensible o el fraude.

RECOMENDACIÓN

Es importante utilizar un medio de comunicación confiable y seguro para evitar tanto los riesgos en la comunicación como el envío de información sensible.

Unos de los mecanismos de cifrado de datos más seguro, útil para enviar por correo o por cualquier medio, es PGP. Al utilizar PGP, garantizamos que ningún intermediario pueda descifrar y obtener la información que viaja por el medio que fuere; y, a la vez, nos permite corroborar su identidad unívoca.

CONSEJOS Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD

CONEXIONES SEGURAS PRIVADAS

PROBLEMA

Permitir sesiones remotas a equipos o redes internas de una organización conlleva riesgos significativos. Los firewalls deben estar configurados con restricciones estrictas para prevenir posibles ataques e intrusiones, por lo que abrir puertos adicionales representa un peligro. Además, al conectarse remotamente, los clientes están expuestos a posibles ataques de suplantación de identidad y monitoreo de tráfico, lo que podría resultar en la obtención de credenciales de acceso u otra información sensible

RECOMENDACIÓN

Para abordar estos problemas, se recurre a las Redes Virtuales Privadas o VPN (por sus siglas en inglés). Al emplear una VPN, los usuarios pueden garantizar la seguridad de sus conexiones a las redes internas de la organización mediante un túnel cifrado punto a punto, lo que les permite operar como si estuvieran físicamente conectados a la red. Es aconsejable implementar autenticación de doble factor para los usuarios de VPN y utilizar contraseñas robustas.

RECOMENDACIONES

RECOMENDACIONES

Puesto de trabajo

- Mantené la mesa limpia de papeles que contengan información sensible.
- Bloqueá la sesión de tu equipo cuando abandones tu puesto.

Dispositivos

- No modifiques la configuración de tus dispositivos.
- No instales aplicaciones no autorizadas.
- No conectes dispositivos USB no confiables.
- Establecé una clave de acceso y la opción de bloqueo automáti- co en tus dispositivos móviles.

Uso de equipos no oficiales

- No manejes información sensible o confidencial en equipos públicos Si accedés al correo oficial desde tu equipo personal, no descar- gues ficheros con información sensible o confidencial.

RECOMENDACIONES

Figuras de información

- No facilites información sensible si no estás seguro de quién es el receptor de la misma.
- Destruye la información sensible en formato papel. No la tires a la papelera.
- No mantengas conversaciones confidenciales en lugares donde puedan ser oídas por terceros.

Gestión de credenciales

- No compartas tus credenciales de acceso (usuario y contraseña) No utilices tus credenciales de acceso corporativas en aplicacio- nes de uso personal.
- No anotes tus credenciales en lugares visibles.

Gestión de credenciales

- Evitá acceder a páginas web no confiables.
- No acceder (hacer click) en enlaces (links) sospechosos. Procurá escribir la dirección en la barra del navegador.

RECOMENDACIONES

Correo electrónico

- Eliminá todo correo sospechoso que recibas.
- Evitá los correos en cadena (reenvío de correos que van dirigi- dos a un gran número de personas).

Protección de la información

- Realizá copias de seguridad de aquella información sensible que solo esté alojada en tus dispositivos.

LA TECNOLOGÍA AL SERVICIO DE LOS TRABAJADORES

Comisión de Ciencia y Tecnología

Asociación del Personal Legislativo

Norberto Di Próspero - Secretario General