ASEGURANDO NUESTRA IDENTIDAD DIGITAL

CONTENIDO

LAS 5 FUNCIONES DE LA CIBERSEGURIDAD

Tu estrategia de seguridad debe considerar cada una de ellas.

IDENTIFICAR
Gestionar los riesgos de la ciberseguridad que aplican a la organización y la continuidad del negocio incluyendo los sistemas, los procesos, las personas, los activos y la información.

PROTEGER
Asegurar y garantizar la prestación de los servicios de la infraestructura crítica de la organización, considerando limitar o contener el impacto de un posible evento de ciberseguridad.

DETECTAR
Identificar la ocurrencia de un evento de ciberseguridad, permitiendo su descubrimiento de manera oportuna.

RESPONDER
Tomar las medidas adecuadas con relación a un incidente de ciberseguridad detectado, incluyendo la capacidad de contener su posible impacto.

RECUPERAR
Mantener los planes de resiliencia, contingencia y restauración de capacidades o de servicios que se vieron afectados debido a un incidente de ciberseguridad, la recuperación es el fin para volver a las operaciones normales de la organización.

TOMEMOS CONCIENCIA

Pequeños actos de consciencia generan un gran efecto en la seguridad para todos.

PUESTO DE TRABAJO
Mantener el escritorio limpio de papeles que contengan información sensible. Bloquear la estación de trabajo al levantarse.

MEDIOS DE ALMACENAMIENTO EXTERNO
No conectar USB no confiables. Encriptar la información sensible transportada en dispositivos extraíbles.

FUGA DE INFORMACIÓN
Destruir en las trituradoras, toda la información sensible en formato papel. No facilitar información sensible, si no se conoce al receptor.

PROTECCIÓN DE INFORMACIÓN
Realizar copias de seguridad (backup) de toda la información sensible que esté guardada solamente en los dispositivos personales.

USOS DE EQUIPOS PERSONALES Y/O PÚBLICOS
No manejar información corporativa en equipos públicos. No descargar archivos en los equipos no corporativos enviados desde correos laborales.

CONTRASEÑAS
No compartir ni revelar las contraseñas. Usar contraseñas difíciles de adivinar, mezclando caracteres numéricos, alfanuméricos y caracteres especiales.

CORREO ELECTRÓNICO
Nunca envíe datos personales, claves o información confidencial por email. Utilizar la dirección de mail corporativo para enviar o recibir información interna.

NAVEGACIÓN
No acceder a sitios webs no confiables. No hacer clicks en links sospechosos, escribir la dirección en la barra del navegador.

"La digitalización de los procesos trae un sinfín de ventajas en el ecosistema de negocios: rapidez, eficiencia, menores costos, pero también nos colocan en el radar de ciberdelincuentes que evolucionan y perfeccionan sus métodos de acción."

FABIÁN DESCALZO
Socio de Gobierno Tecnológico y Ciberseguridad

CUIDADOS EN EL ÁMBITO FAMILIAR

La ciberseguridad no son actos dentro del ámbito laboral únicamente. Nuestra vida alterna entre actividades sociales, familiares y laborales. Aquí algunas recomendaciones a tener presente en el ámbito familiar.

- Tenga cuidado al recibir un correo electrónico con un asunto, archivo adjunto o hipervínculo relacionado con COVID 19.
- No comparta ninguna información personal a través de correo electrónico, redes sociales o mensajes de texto a personas fuera de su círculo familiar /amigos cercanos.
- Compruebe la validez de las redes sociales y los mensajes de texto SMS relacionados con COVID 19.
- No responda a ninguna solicitud para compartir información personal.
- Tenga cuidado de no hacer clic en presuntos enlaces maliciosos o archivos adjuntos Hay una gran cantidad de 'noticias falsas' circulando sobre el virus COVID 19.
- Revisar y configurar las opciones de privacidad disponibles en cada una de las redes sociales que se utilizan.
- Busque información actualizada de fuentes legítimas, como sitios web gubernamentales Tenga cuidado al instalar aplicaciones móviles con respecto a COVID 19.
- Siempre que sea posible, se recomienda limitar al máximo el acceso de personas que pueden ver lo que se está haciendo.
- Tenga cuidado con aplicaciones maliciosas, como por ejemplo ' coronatracker ', que pueden bloquear su dispositivo móvil.
- Analizar la información que se decide publicar, ya que apenas se publica algo se pierde el control sobre lo que otros hacen con ese material.
- Utilice su dispositivo de empresa cuando trabaje desde casa.

CUIDADOS EN EL TRABAJO REMOTO

La transformación del futuro del trabajo hoy día es híbrido, entre el presencial y el remoto. Aquí algunas consideraciones de seguridad al respecto del teletrabajo.

- De ser posible, utiliza los equipos de la empresa. Evitar el uso de dispositivos personales.
- Conectarse a través de la red privada virtual (VPN). Evitar el uso de redes wifi públicas o de terceros.
- Extremar aún más la precaución frente al phishing. No pinchar en enlaces que aparecen en correos de dudosa procedencia ni descargar el contenido adjunto que llega en dichos emails.
- Acceder únicamente a sitios web que u tilizan HTTPS. Son páginas que ofrecen una conexión segura.
- Asegurar que las contraseñas que protegen el acceso a tus cuentas sean robustas, individuales y conocidas únicamente por ti.
- Dejar recipientes con líquidos alejados de los dispositivos que utilicen.
- Evitar el almacenar los datos de la empresa en´dispositivos que no sean de negocio cuando trabaje desde casa.
- Utilice su dispositivo de empresa cuando trabaje desde casa.
- Mantenga las pantallas limpias de post it o papeles con información comercial.
- No usar mail personal para enviar información del trabajo.
- No usar programas no autorizados para intercambio de información corporativa.
- No facilitarla notebook o celulares que utilizan para trabajar a sus hijos, para evitar eliminación de o borrar información.
- Apagar su notebook cuando no la utilice.
- No conectar periféricos de dudosa calidad.
- Alejar la notebook de lugares calientes y de las ventanas.
- Enchufar el cargador en tomas seguros, sin adaptadores o falsos contactos.

SISTEMA DE CONTROL DE CIBERSEGURIDAD

Pasos rápidos que puede seguir ahora para proteger su sistema de control de ciberseguridad.

PONGA A ALGUIEN A CARGO

Designe a una o más personas para que lideren los esfuerzos de ciberseguridad de su sistema de control.

CONOZCA LO QUE TIENE

Documente qué tipos de activos informáticos y del sistema de control tiene, cómo se utiliza cada activo y determine los activos más críticos. Verifique y elimine activos no autorizados.

ESTABLECER RELACIONES DE CIBERSEGURIDAD

Únase a las comunidades de ciberseguridad específicas de su sector y establezca relaciones con proveedores e integradores que pueden ayudarlo con las prácticas de ciberseguridad recomendadas.

CAMBIAR CONTRASEÑAS PREDETERMINADAS

Verifique sus activos en busca de contraseñas predeterminadas y cambie las que encuentre por contraseñas nuevas y difíciles de adivinar. No deje las contraseñas a la vista.

PROTEGER LOS ACTIVOS CONTRA EL MANEJO

Mantenga los activos críticos físicamente asegurados y mantenga las claves de los activos del sistema de control, como los controladores lógicos programables (PLC) y los sistemas de seguridad en la posición “Ejecutar” en todo momento, a menos que se estén programando activamente.

CONCIENTIZACIÓN Y CAPACITACIÓN

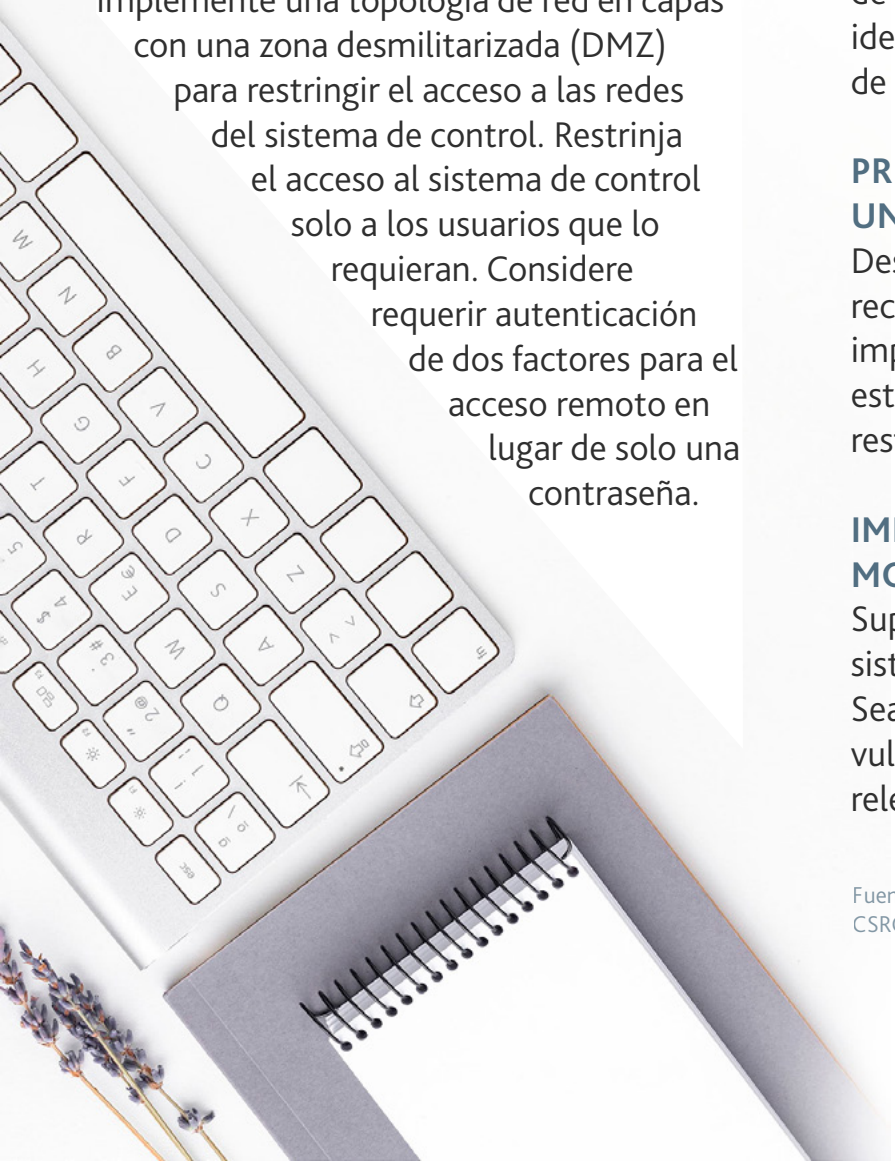
Capacite a los usuarios del sistema de control sobre sus responsabilidades de ciberseguridad y busque cosas fuera de lo común, que pueden ser evidencia de un incidente de ciberseguridad.

ADMINISTRAR LOS ACCESOS Y CREDENCIALES DE LOS USUARIOS

Verifique quién tiene acceso en el sitio o remoto a sus sistemas y revoque el acceso que no es necesario. Inmediatamente deshabilite las cuentas y revoque las identificaciones cuando alguien deje la organización.

RESTRINGIR EL ACCESO AL SISTEMA DE CONTROL RED Y ACTIVIDAD DE RED

Implemente una topología de red en capas con una zona desmilitarizada (DMZ) para restringir el acceso a las redes del sistema de control. Restrinja el acceso al sistema de control solo a los usuarios que lo requieran. Considere requerir autenticación de dos factores para el acceso remoto en lugar de solo una contraseña.



GESTIONAR LA VULNERABILIDAD DE LA CIBERSEGURIDAD

Mantenga sus activos actualizados y completamente parcheados. Priorizar la aplicación de parches a las máquinas "PC" utilizadas en interfaces hombre-máquina (HMI), servidores de bases de datos y estaciones de trabajo de ingeniería. Deshabilite los puertos y servicios no utilizados. Implemente tecnologías antivirus / antimalware / antiphishing cuando sea posible para prevenir, detectar y mitigar el malware, incluido el ransomware.

IMPLEMENTAR CONTROL DE APLICACIONES

La naturaleza estática de algunos activos del sistema de control, como servidores de bases de datos, HMI y estaciones de trabajo de ingeniería, los convierte en candidatos ideales para ejecutar soluciones de control de aplicaciones.

PREPÁRESE PARA RECUPERARSE DE UN INCIDENTE DE CIBERSEGURIDAD

Desarrollar e implementar un plan de recuperación de incidentes. Planifique, implemente y pruebe un sistema y una estrategia de copia de seguridad y restauración de datos.

IMPLEMENTAR Y REALIZAR UN MONITOREO CONTINUO

Supervise continuamente los límites del sistema y el tráfico de entrada y salida. Sea consciente de las amenazas y vulnerabilidades de ciberseguridad relevantes.

Fuente:
CSRC.NIST.GOV

RECOMENDACIONES PARA LA COMPAÑÍA

La seguridad de la información se construye todos los días, con pequeñas medidas aplicadas por todos.

GESTIÓN DE ROLES

Mantener y controlar que la información solo sea accesible para los perfiles de usuario que realmente necesitan visualizarla y modificarla. Para el resto, debería estar restringida.

CONTROL DE DISPOSITIVOS

Teniendo en cuenta la amplia variedad de dispositivos en el mercado, restringir el acceso solamente a aquellos en los cuales se aplican las herramientas de seguridad adecuadas.

PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Para garantizar que los datos no sean afectados por códigos maliciosos, todos los dispositivos deben contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.

MONITOREO DEL TRÁFICO DE RED

Dado que hay dispositivos que están ingresando a la red por fuera del perímetro físico de la oficina, es necesario hacer un seguimiento de qué tipo de tráfico generan.

CONEXIONES SEGURAS

Para teletrabajo, la implementación de conexiones VPN basadas en el cliente es lo más conveniente, donde el usuario ejecuta la aplicación autenticándose con un nombre de usuario y contraseña, e incluso agregar un segundo factor de autenticación, creando el canal cifrado entre el equipo y la red remota, para un intercambio seguro de datos.

REDACCIÓN DE UNA POLÍTICA DE SEGURIDAD

Determinar las obligaciones y responsabilidades de los usuarios respecto al uso de las tecnologías que tienen a su disposición. Definir el tipo de acciones que se pueden hacer y quién está habilitado a ejecutarlas

CONCIENTIZACIÓN DE LOS EMPLEADOS

La educación debe ser un pilar importante para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener al ingresar dispositivos ajenos a la compañía.

CONTRASEÑAS SEGURAS

Los atacantes utilizan una variedad de técnicas para descubrir contraseñas, incluido el uso de herramientas poderosas disponible gratis en Internet. El siguiente consejo facilita la seguridad de la contraseña para su usuarios, mejorando la seguridad de su sistema como resultado (Fuente: National Cyber Security Center).

CÓMO SE DESCIFRAN LAS CONTRASEÑAS...

Intercepción: las contraseñas se pueden interceptar a medida que se ransmiten a través de una red.

Fuerza bruta: Adivinación automatizada de miles de millones de contraseñas hasta que se encuentra la correcta.

Búsqueda: se puede buscar en la nube digital información que sirva para descubrir su contraseña.

Robo de contraseñas: las contraseñas almacenadas de forma insegura pueden ser robadas; esto incluye contraseñas escritas a mano escondidas cerca de un dispositivo.

Adivinar manualmente: la información personal, como el nombre y la fecha de nacimiento, se puede utilizar para adivinar contraseñas comunes.

Espiando por arriba del hombro: Observar a alguien escribiendo su contraseña.

Ingeniería social: los atacantes utilizan técnicas de ingeniería social para engañar a las personas para que revelen contraseñas.

Registro de claves: un registrador de teclas instalado intercepta las contraseñas a medida que se escriben.

...Y COMO MEJORAR LA SEGURIDAD DE ELLAS!

Ayude a los usuarios a afrontar la "sobrecarga de contraseñas"

- Utilice las contraseñas únicamente cuando sean realmente necesarias.
- Utilice soluciones técnicas para reducir la carga para los usuarios.
- Permitir que los usuarios registren y almacenen de forma segura sus contraseñas.
- Pida a los usuarios que cambien sus contraseñas solo si hay sospechas de compromiso.
- Permitir a los usuarios restablecer la contraseña de forma fácil, rápida y económica.

Ayude a los usuarios a generar contraseñas adecuadas.

- Ponga defensas técnicas en su lugar para que se puedan utilizar contraseñas más simples.
- Aleje a los usuarios de contraseñas predecibles y prohíba las más comunes.
- Anime a los usuarios a que nunca reutilicen las contraseñas entre el trabajo y el hogar.
- Capacite al personal para ayudarlos a evitar la creación de contraseñas que sean fáciles de adivinar.
- Tenga en cuenta las limitaciones de los medidores de seguridad de las contraseñas.

Incluya en la lista negra las opciones de contraseña más comunes.

Supervise los intentos fallidos de inicio de sesión, capacite a los usuarios para que informen de actividades sospechosas.

No almacene las contraseñas en formato de texto sin formato.

LA PRIMERA LINEA DE DEFENSA: CONTRASEÑAS

Si en nuestra casa poseemos una caja fuerte es porque tenemos información importante que resguardar dentro de ella. Nunca se nos ocurriría pegar un papel en la puerta con la combinación correcta para abrirla.

Pegar una nota adhesiva en el monitor de nuestro equipo con la contraseña de acceso le permitirá a cualquier persona acceder, manipular y hasta incluso robar información privada y confidencial personal y de nuestra organización.

En la actualidad, prácticamente todos utilizamos un nombre de usuario y contraseña para poder ingresar a sitios, servicios, equipos o dispositivos. La contraseña funciona como una llave digital que nos permite acceder a toda nuestra información.

Utilizar una contraseña segura nos ayudará a mantener a salvo nuestra información y evitar ser víctimas de un ciberdelito.

Utilicemos contraseñas diferentes entre si. Si siempre elegimos la misma, y alguien se hace con ella, tendrá acceso a todas nuestras cuentas.

Utilicemos cerraduras fuertes creando contraseñas de al menos 10 caracteres de longitud que contengan letras minúsculas, letras mayúsculas, números y símbolos especiales.

No publiquemos, compartamos, ni dejemos escritas nuestras contraseñas en lugares que puedan ser vistas por otras personas.

¡Nunca dejemos nuestras contraseñas al alcance de cualquiera!

Aplicar buenas prácticas para gestionar nuestras contraseñas es la primera línea de defensa para nuestra información.

PHISHING

El phishing es una técnica utilizada por delincuentes para robar nuestra información confidencial como nombres de usuario, contraseñas, datos de tarjetas de crédito, entre otros.

Los delincuentes intentan engañarnos haciéndose pasar por otra persona y organización, generalmente a través de un correo electrónico.

Sus mensajes suelen poseer carácter de urgencia, de manera que el destinatario no piense ni analice demasiado la situación y haga lo que el delincuente desea: abrir un archivo adjunto, hacer clic en un enlace o responder el mensaje.

Los delincuentes buscan obtener los nombres de usuario y contraseñas de los servicios que utilizamos y nuestra información personal y financiera.

Con esta información, pueden realizar compras en nuestro nombre, transferir nuestro dinero a sus cuentas y hacerse pasar por nosotros para cometer delitos, entre otras cosas.

¿CÓMO PODEMOS DETECTAR CORREOS DE PHISHING?

- El nombre y correo del remitente es desconocido o intenta parecerse a uno conocido, por ejemplo “Fecebook“ y “Facebook”.
- El remitente es conocido, pero escribe un un horario fuera de lo común o envía algo que no hemos solicitado.
- El remitente intenta que hagamos algo con urgencia o dentro de un plazo límite, para que pensemos lo menos posible.
- El remitente solicita que hagamos clic en un enlace para obtener algo de nuestro interés o para evitar alguna sanción o situación desagradable.
- El mensaje posee archivos adjuntos inesperados, como por ejemplo una factura a nuestro nombre.
- El remitente requiere una respuesta que contiene datos confidenciales como por ejemplo una contraseña o número de tarjeta de crédito.

Eventualmente, recibiremos algún correo de phishing en nuestra bandeja de entrada. Es por eso que debemos estar atentos y pensar dos veces antes de:

- Hacer clic en enlaces no solicitados.
- Descargar archivos adjuntos inesperados.
- Responder un correo con nuestra información confindencial.compras en nuestro nombre, transferir nuestro dinero a sus cuentas y hacerse pasar por nosotros para cometer delitos, entre otras cosas.

CORREO ELECTRÓNICO

Cuando utilizamos nuestro correo electrónico nos estamos exponiendo a una gran cantidad de amenazas, como SPAM y phishing, entre otras.

Los correos electrónicos no solicitados que se envían a un gran número de destinatarios con fines publicitarios o comerciales, se los llama SPAM.
No sólo puede ser molestos, sino también, representan un peligro.

Los ciberdelincuentes pueden hacerse pasar por personas u organizaciones conocidas y engañaros para robar dinero e información privada.
Los correos electrónicos en los que intentan engañarnos para robar nuestra información privada reciben el nombre de phishing, y son una amenaza muy común en estos días.

Un correo de un ciberdelincuente puede verse idéntico a uno legítimo, y puede también llevarnos a sitios idénticos a los sitios legítimos por medio de enlaces.
Para prevenir ser víctimas de phishing, sencillamente no brindemos nunca nuestra información privada por correo, ni a través de ningún sitio web al que lleguemos haciendo clic en un enlace.
Para proteger un correo corporativo, es importante que se evite publicar direcciones asociadas a la empresa en cualquier sitio web, sin antes verificar la reputación y seriedad de este.

Algunas consecuencias de ser víctimas de phishing:
- Realización de compras en nuestro nombre.
- Utilización de nuestra identidad para actividades ilegales.
- Más correos de phishing en nuestra bandeja de entrada.

Frente a un correo de SPAM o phishing:
- No respondas ni reenvíes el correo.
- Evita hacer clic en los enlaces y descargar archivos adjuntos.
- Marcar el correo como SPAM o suplantación de identidad.
- Eliminar el correo.

Es importante que estemos atentos, tengamos precaución, y nos capacitemos día a día para prevenir todas las amenazas que enfrentamos al hacer uso de nuestro correo electrónico.

NAVEGACIÓN SEGURA

Actualmente pasamos gran parte del día conectados a Internet, pero no siempre actuamos con seguridad.

Utilizamos redes sociales, revisamos el correo electrónico, operamos con nuestras cuentas bancarias, realizamos compras y mucho más.
… pero también puede convertirse en una trampa.
Lamentablemente, existen ciberdelincuentes que utilizan Internet para cometer delitos.

¿QUÉ PUEDE HACER UN CIBERDELINCUENTE SI CAEMOS EN SU TRAMPA?

- Robar información de nuestro dispositivo, como ser credenciales de acceso, datos bancarios o material privado, entre otros.
- Realizar compras en nuestro nombre o transferencias de nuestro dinero.
- Secuestrar nuestra información y luego pedir un rescate por ella.
- Cometer delitos en nuestro nombre, como por ejemplo la difusión de pornografía infantil.

SIGUIENDO UNAS POCAS RECOMENDACIONES PODREMOS NAVEGAR TRANQUILOS POR INTERNET

- Mantegamos nuestro navegador, sistema operativo y antivirus actualizado.
- Naveguemos por sitios de confianza, con buena reputación y ampliamente recomendados.
- Prestar atención al candadito al lado de la dirección web en los sitios seguros, en caso de no estar presente, no se debe ingresar usuarios ni contraseñas.
- Evitemos utilizar conexiones a Internet públicas si vamos a ingresar información confidencial como los datos de nuestra tarjeta de crédito o nuestro usuario y contraseña de homebanking.
- Evitemos hacer clic en publicidades o ventanas emergentes. Utilicemos un bloqueador de publicidades para prevenir su aparición.
- Evitemos instalar complementos desconocidos en nuestro navegador.
- Evitemos descargar programas, películas o música desde sitios no oficiales.

LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La información es el activo que nos permite tomar decisiones tanto en lo personal y lo laboral, por eso debemos protegerla.

La información es un recurso esencial y vital para nuestra organización.

- Los datos que generamos y/o utilizamos en nuestro trabajo diario.
- Los sistemas en los cuales operamos.
- Los informes que leemos.
- El conocimiento que poseemos de la empresa.
- Toda forma parte de la INFORMACIÓN de la organización y debe ser protegida.

¿QUÉ INFORMACIÓN DEBE SER CONSIDERADA CONFIDENCIAL?

- Datos personales de clientes y colaboradores en general.
- Información financiera.
- Proyectos de desarrollo de productos o servicios.
- Información comprometida con un tercero a mantener confidencial. Cliente, socio, proveedor, etc.

Diariamente manejamos todo tipo de información en nuestra vida laboral y personal.

Si miramos con atención, podremos ver que es muy valiosa. No solo para nosotros, sino también para personas malintencionadas que cometen ciberdelitos a través del uso de tecnología e Internet.

Para mantener a salvo nuestros datos privados de estas amenazas que cada vez son más comunes, el ámbito de la Seguridad de la Información nos enseña buenos hábitos a tener en cuenta en nuestra vida personal, familiar y laboral. Sin un comportamiento seguro, los ciberdelincuentes se aprovecharán de nosotros, y además de pérdidas económicas, expondremos la imagen de nuestra organización y la de sus clientes.

¿PARA QUÉ PUEDEN UTILIZAR LOS CIBERDELINCUENTES ESTE TIPO DE INFORMACIÓN?

- Obtener grandes sumas de dinero al venderla en el mercado negro.
- Suplantar la identidad de algún directivo.
- Dañar la imagen o credibilidad de nuestra organización.
- Extorsionar a miembros de nuestra organización.

> No necesitamos ser expertos en seguridad, pero sí ser conscientes de las amenazas a las cuales estamos expuestos y evitar caer en los engaños de los ciberdelincuentes aprendiendo unos pocos hábitos seguros.

RANSOMWARE TIPS

Pasos rápidos que puede tomar ahora para **protegerse** de la amenaza del ransomware:

- **USE SOFTWARE ANTIVIRUS TODO EL TIEMPO:** Configure su computadora para que escanee automáticamente sus correos y dispositivos almacenamiento externos.
- **MANTENGA SU COMPUTADORA ACTUALIZADA:** Ejecute periódicamente chequeos para mantener su computadora actualizada y "parcheada".
- **BLOQUEE EL ACCESO A SITIOS DE RANSOMARE:** Use productos o servicios de seguridad que bloquean el acceso a sitios conocidos de ransomware.
- **PERMITA EL USO DE APLICACIONES AUTORIZADAS:** Configure el sistema operativo o software de terceros para permitir solo las aplicaciones autorizadas en su computadora.
- **RESTRINJA EL ACCESO DE DISPOSITIVOS PERSONALES:** Las organizaciones deben restringir o prohibir el acceso de dispositivos personales a las redes oficiales.
- **USE CUENTAS DE USUARIO ESTÁNDAR:** Use cuentas estándares de usuario en lugar de cuentas de administración privilegiadas cuando fuera posible.
- **ANULE EL USO DE APLICACIONES PERSONALES:** Anule el uso de aplicaciones personales y sitios, tales como email, chat y redes sociales, desde las terminales de la empresa.
- **TENGA CUIDADO CON LAS FUENTES DESCONOCIDAS:** No abra archivos ni haga clic en enlaces de fuentes desconocidas a menos que primero ejecute un análisis antivirus o mire los enlaces con atención.

Pasos que puede tomar ahora para ayudarlo a **recuperarse** de un futuro ataque de ransomware:

- **BACKUP & RESTORE:** Planifique, implemente y pruebe cuidadosamente una estrategia de copia de seguridad y restauración de datos, y proteja y aísle las copias de seguridad de los datos importantes.
- **MANTENGA SUS CONTACTOS ACTUALIZADOS:** Mantenga una lista actualizada de contactos internos y externos para casos ataques de ransomware, incluida la aplicación de la ley.
- **PREPARA UN PLAN DE RECUPERO FRENTE A INCIDENTES:** Desarrolle e implemente un plan de recuperación de incidentes con roles y estrategias definidos para la toma de decisiones.dispositivos almacenamiento externos.

Fuente:
CSRC.NIST.GOV

En **BDO** hacemos lo que hacemos de manera excepcional y lideramos en cada lugar donde estamos presentes: hemos sido la organización global con mayor crecimiento en nuestro rubro durante los últimos 10 años, y atendemos a mas de **775.000 clientes** a nivel global.

CHARLAS A USUARIOS FINALES

Concientizar, Capacitar y Entrenar de manera conitnua a toda la población organizacional.

- **PREVENCIÓN**
  Cuentas y contraseñas, virus, gusanos, bots y botnets , caballos de troya , backdoors , keyloggers, spywares y phishing entre muchos otros.

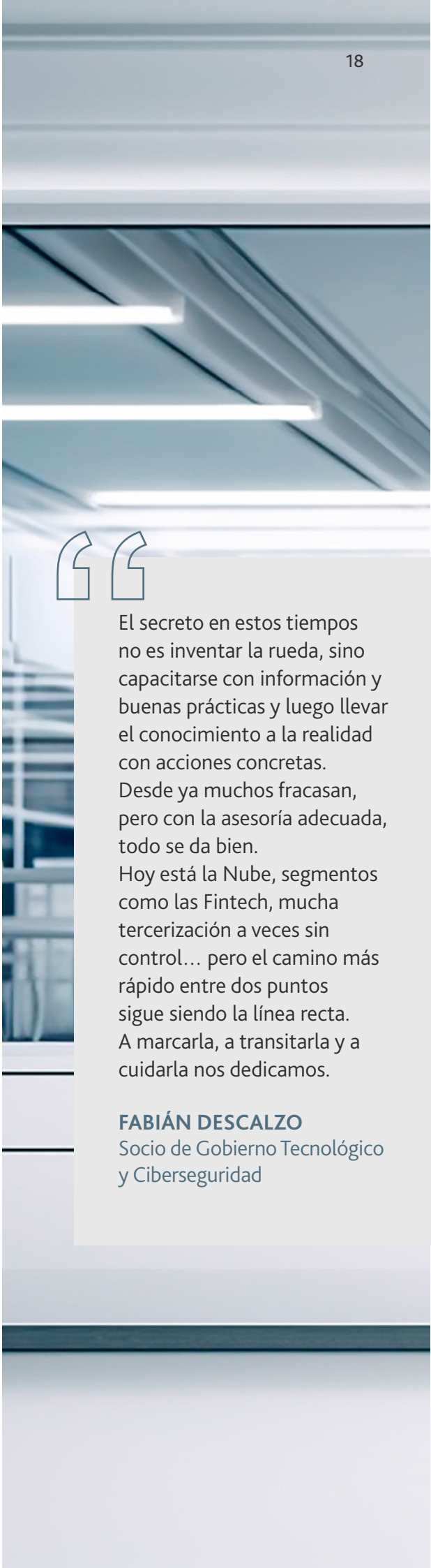
- **CUIDADOS EN EL USO DE INTERNET**
  Programas de correo, navegadores, mensajería instantánea, spam, programas para compartir archivos, compartir recursos, copias de seguridad. Introducción a la privacidad y protección de datos. Privacidad y seguridad en la Web. Robo de Identidad y respuesta a incidentes.

- **FRAUDE**
  Ingeniería social, cuidados al realizar transacciones bancarias o comerciales, cadenas.

- **PROTECCIÓN DE INFORMACIÓN**
  Realizar copias de seguridad (backup) de toda la información sensible que esté guardada solamente en los dispositivos personales.

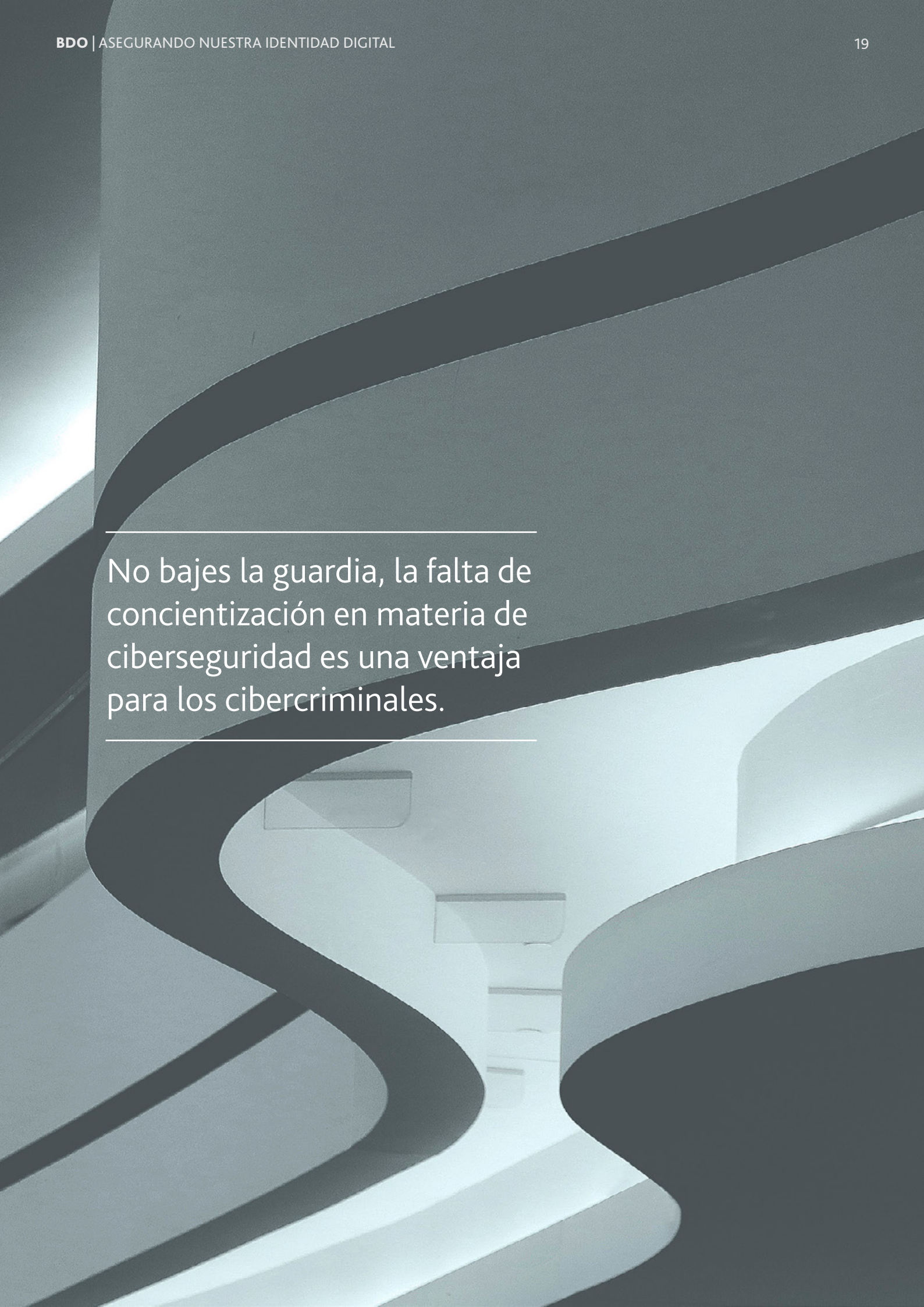
- **PRIVACIDAD**
  Emails, cookies, cuidados con datos personales en páginas web, blogs y sitios web de redes de relaciones personales, cuidados con los datos almacenados en el disco rígido, cuidados con smartphones y IoT / IoP.

- **BANDA ANCHA Y REDES INALÁMBRICAS**
  Protección de una computadora utilizando banda ancha, protección de una red utilizando banda ancha, cuidados para un cliente de red inalámbrica.



"El secreto en estos tiempos no es inventar la rueda, sino capacitarse con información y buenas prácticas y luego llevar el conocimiento a la realidad con acciones concretas.
Desde ya muchos fracasan, pero con la asesoría adecuada, todo se da bien.
Hoy está la Nube, segmentos como las Fintech, mucha tercerización a veces sin control… pero el camino más rápido entre dos puntos sigue siendo la línea recta.
A marcarla, a transitarla y a cuidarla nos dedicamos.

FABIÁN DESCALZO
Socio de Gobierno Tecnológico y Ciberseguridad



No bajes la guardia, la falta de concientización en materia de ciberseguridad es una ventaja para los cibercriminales.

LIMITACIONES DE LA IA

Explora las limitaciones de la IA, desde sesgos y falta de transparencia, sus desafíos clave.

1. **Sesgo:** Los algoritmos de IA pueden reflejar sesgos debido a datos de entrenamiento incompletos o prejuiciosos, generando resultados injustos o discriminatorios al tomar decisiones.

2. **Falta de transparencia:** La toma de decisiones opaca por parte de los algoritmos de IA dificulta la identificación de errores y sesgos en los resultados, generando incertidumbre en su funcionamiento.

3. **Falta de flexibilidad:** La adaptación limitada de la IA a contextos nuevos o inesperados se debe a su dependencia de los datos de entrenamiento, limitando su aplicabilidad en situaciones cambiantes.

4. **Privacidad y seguridad:** La utilización de datos sensibles en IA plantea preocupaciones sobre privacidad y seguridad, aumentando el riesgo de manipulación y sabotaje de sistemas vulnerables.

5. **Costos y accesibilidad:** Los altos gastos asociados con el desarrollo y la implementación de IA pueden restringir su adopción a organizaciones con recursos financieros sustanciales.

6. **Responsabilidad y ética:** La capacidad de la IA para tomar decisiones cruciales implica dilemas éticos y desafíos en la determinación de la responsabilidad en caso de resultados adversos.

7. **Interpretabilidad de resultados:** La complejidad de los algoritmos de IA puede dificultar la comprensión de cómo se llega a ciertos resultados, lo que plantea desafíos en la explicación y comunicación de las decisiones tomadas por el sistema.

¿QUÉ ES CHATGPT?

La Potente Herramienta de Generación de Diálogos con Inteligencia Artificial.

ChatGPT ha sido minuciosamente diseñado para sobresalir en la generación de diálogos de texto, lo que le capacita para responder y generar interacciones conversacionales de manera efectiva. Esta herramienta de OpenAI puede mantener conversaciones interactivas con usuarios y ofrecer respuestas relevantes y coherentes, contextualizadas en el flujo de la conversación.

Fundamentado en la arquitectura GPT (Generative Pre-trained Transformer), ChatGPT se basa en la versión GPT-3.5, una de las iteraciones más avanzadas del modelo. A través de un amplio entrenamiento con datos de texto de la web, se ha educado al modelo para predecir las secuencias de palabras y frases en texto, lo que le confiere una comprensión del lenguaje humano. Sus respuestas se presentan de manera coherente y contextual, emulando la comunicación humana.

Este motor conversacional es empleado en diversas aplicaciones en el campo de la inteligencia artificial, incluyendo asistentes virtuales, soporte al cliente, tutoriales interactivos y generación de contenido, entre otros. ChatGPT ejemplifica cómo la tecnología actual puede simular interacciones humanas, potenciando una variedad de plataformas y servicios con una comunicación natural y precisa.

ÉTICA EN EL USO DE CHATGPT

Pautas para una Interacción Responsable.

Reconocemos que esta herramienta es invaluable para aumentar la eficiencia en la creación de contenido escrito, disminuyendo el tiempo y los costos. Sin embargo, no debemos utilizarla sin considerar las posibles consecuencias o de manera engañosa. Para un uso ético y correcto de ChatGPT, es imperativo atender a las siguientes directrices:

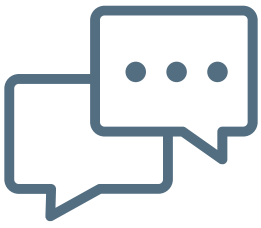
Es crucial aclarar que se está interactuando con una inteligencia artificial al comienzo de la conversación. Esta transparencia es esencial para establecer expectativas adecuadas y prevenir malentendidos.

Se debe evitar depositar una confianza ciega en el modelo. Los usuarios deben comprender que las respuestas no siempre serán precisas o actualizadas. Se recomienda verificar la información proporcionada en fuentes confiables adicionales antes de aceptarla como válida.

En caso de identificar información incorrecta o sesgada en las respuestas, es fundamental corregirla y proporcionar la información precisa. Esta práctica es esencial para prevenir la diseminación de desinformación en línea.

La responsabilidad de los usuarios se extiende a evitar solicitar o generar contenido inapropiado, discriminatorio, ilegal o dañino. Utilizar el modelo de manera ética y respetuosa es esencial para mantener la integridad y la ética en la comunicación generada.

Si se encuentra una respuesta problemática, sesgada o inapropiada, se aconseja proporcionar retroalimentación a los desarrolladores del modelo, como OpenAI. Este proceso contribuye a la mejora continua y al perfeccionamiento de los modelos de lenguaje en futuras iteraciones.



DESAFÍOS DE SEGURIDAD EN EL USO DE CHATGPT

Exploramos los riesgos que plantea ChatGPT en cuanto a la seguridad de datos y cómo protegerse.

Es importante que las empresas tomen medidas para mitigar estos riesgos y protegerse contra posibles amenazas.

1. **Riesgo de seguridad de datos:** La capacidad de ChatGPT para recopilar y almacenar extensos volúmenes de datos aumenta la probabilidad de vulnerabilidades en la seguridad, con la consiguiente amenaza de filtraciones y pérdida de información confidencial.

2. **Riesgo de malware:** Los ciberdelincuentes pueden aprovechar ChatGPT como vehículo para distribuir malware y otros programas maliciosos, poniendo en riesgo la integridad de las redes y los sistemas empresariales.

3. **Riesgo de privacidad:** La recopilación de datos personales por parte de ChatGPT plantea preocupaciones sobre la privacidad, pudiendo infringir los derechos de confidencialidad de los clientes y empleados de la empresa.

4. **Riesgo de ingeniería social:** ChatGPT puede ser explotado por ciberdelincuentes para manipular usuarios y obtener información sensible, exponiendo a la empresa a riesgos significativos en términos de seguridad.

5. **Riesgo de reputación:** En caso de que ChatGPT sea responsable de una brecha de datos o pérdida de información confidencial, la reputación de la empresa enfrenta una amenaza grave, con posibles repercusiones económicas y legales.

10 MANDAMIENTOS PARA GOBERNAR LA CIBERSEGURIDAD EN LA ERA DE CHATGPT

Los 10 mandamientos guías de gobernanza para los líderes empresariales, previniendo riesgos y resguardando activos en la era ChatGPT.

1 **Conciencia de Riesgos:** Es clave que los líderes empresariales comprendan en profundidad los riesgos inherentes al uso de ChatGPT y sistemas de inteligencia artificial. Esta conciencia informada capacita a tomar decisiones estratégicas que protejan los activos y la integridad de la organización en el entorno digital actual.

2 **Directrices Evidentes:** La creación de políticas claras y bien definidas en relación con el uso de ChatGPT e IA es esencial para mantener una postura sólida en ciberseguridad. Estas políticas establecen expectativas claras para el manejo de los datos recopilados, proporcionando una estructura que guía las acciones y protege la información sensible.

3 **Capacitación Integral Permanente:** Empoderar a los empleados con programas de concientización y capacitación exhaustiva es un pilar fundamental en la estrategia de prevención de riesgos. Proporcionar conocimientos sobre el uso seguro de ChatGPT e IA es fomentar la capacidad de detectar posibles amenazas, para asegurar que cada miembro del equipo sea un defensor activo de la ciberseguridad

4 **Protección de Datos:** La implementación de medidas robustas de seguridad para proteger los datos recopilados y alrededor del ecosistema ChatGPT e IA es un mandamiento inquebrantable. Mediante la encriptación avanzada y el control de acceso restringido, se crea una barrera defensiva que salvaguarda la información confidencial de posibles vulnerabilidades y ataques.

5 **Monitoreo Continua:** Mantener una supervisión constante sobre el uso de ChatGPT e IA se erige como una salvaguardia activa contra amenazas latentes. El monitoreo en tiempo real permite la detección temprana de comportamientos anómalos, facilitando una respuesta ágil ante cualquier intento de violación de seguridad.

6 **Actualización de Plataformas:** La actualización regular y estratégica del software de ChatGPT e IA es un mandato crucial en la lucha contra las vulnerabilidades. Mantenerse al día con las últimas versiones y parches de seguridad reduce la exposición a posibles exploits y garantiza un entorno más resiliente.

7 **Preparación ante Incidentes:** Un plan de respuesta a incidentes sólido es esencial para mitigar los efectos de una posible violación de seguridad. Tener protocolos claros y estructurados para gestionar incidentes garantiza una reacción rápida y eficaz, minimizando el impacto en caso de una brecha.

8 **Auditorías Rigurosas:** Las auditorías de seguridad regulares permiten una evaluación exhaustiva de la efectividad de las medidas de seguridad implementadas. Estas evaluaciones periódicas identifican posibles lagunas y oportunidades de mejora, permitiendo que la estrategia de ciberseguridad evolucione con las cambiantes amenazas de ciberseguridad.

9 **Pruebas de Penetración:** Ejecutar pruebas de penetración de manera regular es una directriz proactiva para identificar y remediar posibles debilidades en el sistema. Estas evaluaciones exhaustivas, no solo al servicio en sí mismo, sino a todas las capas de punta a punta en el uso de IA, permiten una revisión minuciosa de la infraestructura y la detección temprana de brechas, antes de que puedan ser explotadas por amenazas externas.

10 **Colaboración con Expertos:** La colaboración con expertos en ciberseguridad aporta una perspectiva externa e invaluable para fortalecer la defensa. La experiencia de estos profesionales permite la identificación temprana de amenazas emergentes y la formulación de estrategias de prevención adaptativas y efectivas. Juntos, pueden guiar a la organización hacia un futuro más seguro y resiliente en el mundo digital.

7 PRINCIPIOS FUNDAMENTALES DE PRIVACIDAD Y SEGURIDAD

Los empleados pueden internalizar la importancia de la ciberseguridad y la privacidad en el entorno digital, contribuyendo a un ecosistema en línea más seguro y resistente.

1. Vigilancia Digital

Evita la despreocupación: Exceso de confianza en la seguridad puede conducir a vulnerabilidades no reconocidas. Mantén humildad digital; asume que cualquier sistema puede ser vulnerable, mejora el control y monitoreo de los mismos.

2. Ética de datos

Realiza una recopilación responsable: La recolección excesiva de datos sin justificación puede comprometer la privacidad de los usuarios. Recopila solo datos necesarios; respeta la privacidad de los usuarios, recolecta solo lo que el negocio necesita.

3. Control Emocional en Línea

Reacciona de manera meditada: Reacciones impulsivas en línea pueden exponer información sensible o a ataques de phishing. Evita reacciones impulsivas en línea; sospecha de enlaces y correos no solicitados. Que la ansiedad no comande tus decisiones, es preferible lento y seguro en estos casos.

4. Creatividad en protección

Supera las repeticiones: La imitación de contraseñas o prácticas de seguridad puede llevar a vulnerabilidades y accesos no autorizados. No imites prácticas de seguridad; crea contraseñas únicas y utiliza autenticación de dos factores. Dos siempre es mejor que solo uno.

5. Actualización permanente

Mantenerte actualizado: Ignorar actualizaciones de seguridad puede dejar sistemas expuestos a explotaciones conocidas. Actualiza regularmente; parches de seguridad contrarrestan vulnerabilidades. Disciplina, procesos y control como parte de tu agenda diaria.

6. Gestión equilibrada de datos

Menos es más: Acumular información sin necesidad aumenta los riesgos de pérdida y robo de datos. Limita la acumulación de datos; conserva solo lo necesario y aplica medidas de seguridad. Una buena dieta hace a una agilidad y privacidad. .

7. Exploración en línea segura

Navega con precaución: Hacer clic en enlaces desconocidos puede conducir a sitios web maliciosos y malware. Haz clic con precaución; verifica la autenticidad antes de hacer clic en enlaces.

LEADERS IN OUR MARKETS

CONEXIÓN GLOBAL. COMPRENSIÓN LOCAL.

BDO EN EL MUNDO

BDO EN ARGENTINA

RANKING

Puesto en el Ranking de auditoría global

Puesto en el Ranking de auditoría local

OFICINAS

164 Países

+1.800

4

- **BUENOS AIRES**
  Retiro
  Distrito Tecnológico
- **CÓRDOBA**
- **SANTA FÉ**
  Rosario

Y colaboradores distribuidos en todo el país

SOCIOS Y STAFF

+111.000

+800

Contactos:

FABIÁN DESCALZO
Socio de Gobierno Tecnológico
y Ciberseguridad
fdescalzo@bdoargentina.com

LAURA DANGELO
Directora de Gobierno Tecnológico
y Ciberseguridad
ldangelo@bdoargentina.com

www.bdoargentina.com