ASEGURANDO NUESTRA IDENTIDAD DIGITAL

2025

Anticiparse para vivir en un entorno digital expuesto

En un contexto global caracterizado por avances tecnológicos exponenciales, la inteligencia artificial que crece por todos lados y amenazas cada vez más sofisticadas, dado que los ciberdelincuentes también se actualizan con estas nuevas tecnologías. Las organizaciones enfrentan el desafío de proteger sus activos críticos sin frenar la innovación.

La ciberseguridad, la privacidad y la gobernanza digital ya no son aspectos técnicos aislados, sino componentes estratégicos del negocio, claves para la resiliencia operativa, la confianza del cliente y la sostenibilidad en el futuro a largo plazo.

EL NUEVO ROSTRO DEL RIESGO: AMENAZAS QUE IMITAN LA REALIDAD

Entre 2024 y 2025, el auge de la ingeniería social potenciado por IA generativa marca un antes y un después en el escenario de amenazas. Los deepfakes han elevado el realismo de ataques como el CEO Fraud, exponiendo la urgencia de adoptar políticas de verificación de identidad y canales de validación cruzada. En paralelo, el ransomware ha evolucionado hacia ataques dirigidos a sectores críticos, exigiendo planes específicos de respuesta y estrategias de segmentación de red, mientras el phishing sigue explotando el error humano, obligando a reforzar la educación continua del usuario y los controles antiphishing automatizados.

IDENTIDAD DIGITAL: DEL PASSWORD AL CONTROL SOBERANO DEL DATO

El futuro apunta a modelos de autenticación passwordless, con biometría y llaves de seguridad, y a la exploración de Identidades Digitales Autosoportadas (SSI), que permiten a los usuarios gestionar sus credenciales con mayor control y privacidad. Estas soluciones deben evaluarse con visión estratégica, alineadas a la madurez tecnológica y las exigencias regulatorias de cada industria.

CUMPLIMIENTO NORMATIVO: DE LA OBLIGACIÓN A LA OPORTUNIDAD ESTRATÉGICA

América Latina avanza hacia un marco regulatorio más robusto y alineado con estándares internacionales. Países como Brasil, Argentina, México y Colombia están fortaleciendo sus legislaciones de protección de datos, inspirados por modelos como el RGPD europeo y nuevas regulaciones como el AI Act. Este entorno requiere una postura proactiva de las empresas: monitoreo legislativo constante, formación legal-técnica y políticas que trasciendan el cumplimiento mínimo, proyectando una cultura de confianza digital.

ÉTICA Y TRANSPARENCIA EN IA: CONSTRUIR CONFIANZA ALGORÍTMICA

La adopción de inteligencia artificial plantea dilemas éticos complejos: sesgos algorítmicos, uso de datos personales, explicabilidad de decisiones automatizadas. Las organizaciones deben implementar marcos de gobernanza de IA que contemplen la diversidad de datos, la anonimización, la trazabilidad de modelos y la creación de comités éticos que garanticen un uso responsable de la tecnología.

La protección de la información y la privacidad en la economía digital no puede depender únicamente de soluciones tecnológicas, sino de un ecosistema integral que combine l**iderazgo, cumplimiento, innovación y concientización** permanente a todos los niveles de la organización.

CIBERSEGURIDAD PERSONAL

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.

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.

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 descargararchivos 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.

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 ennuestro nombre, transferir nuestro dinero a sus cuentas y hacerse pasar por nosotros para cometer delitos, entre otras cosas.

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.

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

DECÁLOGO de la ciberseguridad personal

Actualización de dispositivos y aplicaciones: Mantén siempre al día los sistemas operativos (móviles y computadoras) y revisa con frecuencia las actualizaciones de apps. Activa la opción de actualizaciones automáticas para reducir el riesgo de vulnerabilidades conocidas.

Contraseñas fuertes y gestión segura: Crea contraseñas únicas y robustas (mayúsculas, minúsculas, números, símbolos). Utiliza **frases de paso** o un **gestor de contraseñas** para no reutilizar credenciales en diferentes sitios.

Autenticación Multifactor (MFA): Activa la **verificación en dos pasos** (o MFA) en correos, redes sociales, aplicaciones de banca, etc. De preferencia, emplea **aplicaciones de autenticación** (Google Authenticator, Authy) en lugar de SMS.

Protección antimalware y uso de firewall: Instala un antivirus confiable y manténlo activo y actualizado. Verifica que el cortafuegos (firewall) de tu sistema operativo esté habilitado.

Prevención contra phishing e ingeniería social: Sé escéptico con correos, mensajes o llamadas que soliciten datos personales o credenciales. Verifica el remitente y la URL antes de hacer clic. No descargues archivos adjuntos sospechosos o de fuentes desconocidas.

Copias de seguridad (Backups) personales: Realiza respaldos periódicos de fotos, documentos y archivos importantes en discos duros externos o servicios de nube confiables. Almacena tus copias en **ubicaciones separadas**, para mayor seguridad.

Seguridad en redes inalámbricas: Cambia la contraseña predeterminada de tu router Wi-Fi y usa cifrado WPA2 o WPA3. Limita el uso de redes Wi-Fi públicas; en caso necesario, utiliza una VPN para proteger la conexión.

Uso responsable de dispositivos móviles: Bloquea tu smartphone con PIN, patrón, huella o reconocimiento facial. Desactiva Bluetooth y NFC cuando no los utilices, para evitar conexiones indebidas.

Supervisión familiar: Informa a los miembros de tu familia (niños, adolescentes, adultos mayores) sobre los riesgos digitales básicos. Utiliza herramientas de control parental para regular el acceso a contenidos sensibles.

Desconfía de ofertas "demasiado buenas": Sospecha de promociones, premios o sorteos que te pidan dinero o datos personales de forma urgente. Valida la información en sitios oficiales o con familiares/amigos antes de compartir datos.

CIBERSEGURIDAD EMPRESARIAL

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
Director DRAS & DPO de BDO en Argentina

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.

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

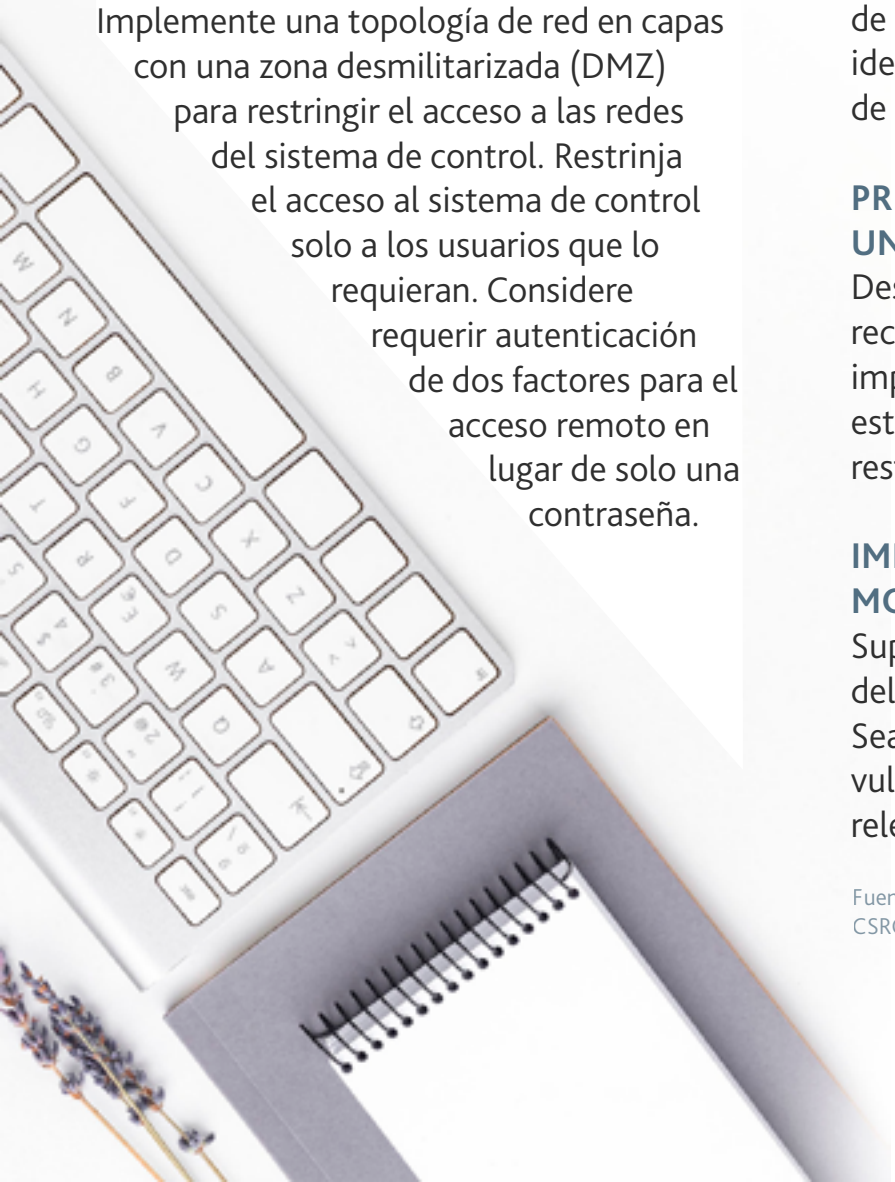
Capacite a los usuarios del sistema de control sobre sus responsabilidades de ciberseguridad y busque cosas fuera de lo común, que pueden ser evidencia de un incidente de ciberseguridad.

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

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.

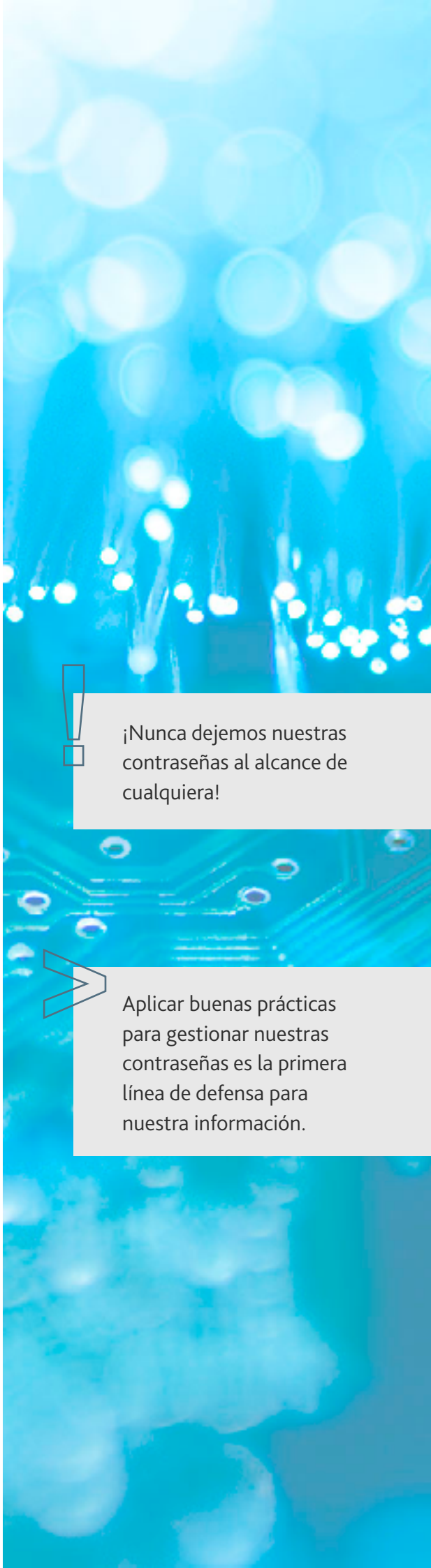
En la actualidad, prácticamente todos utilizamos un nombre de usuario y contraseña para poder ingresar a sitios, servicios, equipos o dispositivos. La contraseña funciona como una llave digital que nos permite acceder a toda nuestra información.

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.

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.

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

10 CASOS ACTUALES DE MITOS Y REALIDADES DE CIBERSEGURIDAD

Todo **mito** conlleva una conversación por desconocimiento, miedos o simplemente clamor popular, que no es realmente cierto. Por eso a cada uno de estos mitos le corresponde una **realidad** lo mas cercano a la verdad.

Mito: "No soy un objetivo, solo los grandes corporativos sufren ciberataques."
Realidad: Cualquier persona (independientemente de su perfil) puede convertirse en víctima de un ataque o fraude.

Mito: "Cambiar contraseñas con frecuencia es más seguro que tener una robusta."
Realidad: Es preferible una contraseña sólida (o frase de paso) única para cada sitio que cambiarlas frecuentemente sin reforzar su complejidad.

Mito: "Si uso un antivirus gratuito, estoy totalmente protegido."
Realidad: Aunque ayuda, un antivirus gratuito no reemplaza las actualizaciones del sistema, la autenticación multifactor ni las buenas prácticas de seguridad.

Mito: "Si nadie sabe mi nombre de usuario, no podrán hackear mi cuenta."
Realidad: Los atacantes pueden usar técnicas de fuerza bruta o ingeniería social para averiguar credenciales. Ocultar el usuario no basta.

Mito: "A mis hijos no les pasará nada en internet, ellos son 'nativos digitales."
Realidad: Ser hábil con dispositivos no implica entender los riesgos; menores también pueden ser víctimas de grooming, ciberacoso o robo de datos.

Mito: "Almacenar contraseñas en el navegador es totalmente seguro."
Realidad: Los navegadores pueden ser vulnerados; un gestor de contraseñas dedicado suele ofrecer cifrado adicional y mayores garantías.

Mito: "La autenticación en dos pasos es un fastidio y apenas aporta seguridad."
Realidad: El doble factor reduce drásticamente el riesgo de acceso no autorizado, incluso si alguien roba tu contraseña.

Mito: "No existe peligro en usar Wi-Fi públicas porque solo reviso redes sociales."
Realidad: Cualquier información intercambiada sin cifrado (cookies de sesión, credenciales) puede ser interceptada en redes públicas.

Mito: "Apagar el router por la noche es suficiente para evitar ciberataques."
Realidad: Aunque reduzca la exposición temporal, las vulnerabilidades persisten mientras el dispositivo esté encendido o mal configurado.

Mito: "Si no ves algo raro en la pantalla, no hay malware en tu dispositivo."
Realidad: Muchas amenazas actúan en segundo plano, registrando actividad o robando datos sin síntomas visibles.

PRIVACIDAD

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.

DECÁLOGO de la privacidad personal

Configuración de privacidad en redes sociales: Revisa quién puede ver tus publicaciones (público, amigos, solo tú). Limita la visibilidad de tu información personal (cumpleaños, teléfono, ubicación) únicamente a contactos de confianza..

Control de permisos en dispositivos: Verifica las aplicaciones que tienen acceso a tu cámara, micrófono, ubicación, contactos y archivos. Revoca permisos innecesarios para proteger tu información personal.

Geolocalización y etiquetado: Desactiva la localización cuando no sea imprescindible. Evita etiquetar lugares frecuentes (casa, trabajo, colegio de tus hijos) en redes sociales.

Mensajería segura: Prefiere servicios con **cifrado de extremo a extremo** (E2EE) para conversaciones personales o sensibles. No envíes datos confidenciales (contraseñas, documentos oficiales) a través de SMS o correos sin cifrar.

Derechos de privacidad: Conoce la legislación local (por ejemplo, Ley de Protección de Datos Personales) para ejercer tus derechos de acceso, rectificación o supresión. Solicita la **eliminación** de tu información en servicios que ya no uses o que no deseas conservar.

Uso de VPN al conectarte a redes públicas: Hoteles, aeropuertos y cafeterías son entornos comunes para atacantes que intentan capturar datos sin cifrar. Una VPN (red privada virtual) cifra el tráfico, protegiendo tu información.

Suscripciones y newsletters: Revisa periódicamente los correos a los que estás suscrito. Cancelar suscripciones innecesarias reduce el spam y la posible exposición de datos.

Elimina perfiles y cuentas inactivas: Las cuentas antiguas en foros, tiendas en línea o redes que ya no usas se convierten en potenciales puertas de entrada a tu información. Haz un rastreo de tu "huella digital" y solicita bajas o eliminaciones donde corresponda.

Contratos y políticas de privacidad: Antes de descargar una app o usar un servicio, revisa los puntos más importantes de su política de datos. Asegúrate de que su modelo de negocio y su reputación sean confiables.

Gestión de cookies y navegadores: Configura tu navegador para **borrar** cookies y datos de navegación al cerrarlo, o para bloquear cookies de terceros. Utiliza navegadores centrados en la privacidad (Brave, Firefox con extensiones antirrastreo, etc.).

10 MITOS Y VERDADES SOBRE LA PRIVACIDAD DIGITAL QUE NO CONOCEMOS

El uso masivo de cookies, casas inteligentes y redes sociales genera múltiples ideas erróneas sobre la confidencialidad de nuestros datos. Conoce las principales equivocaciones y la forma correcta de enfrentarlas. Estos diez mitos y realidades te ayudarán a comprender mejor las prácticas esenciales de protección de datos.

Mito: "No tiene consecuencias aceptar todas las políticas de cookies.."
Realidad: Aceptar cookies de terceros permite el rastreo intenso de tu actividad en línea y la creación de perfiles de comportamiento..

Mito: "Con borrar el historial de búsqueda basta para cuidar mi privacidad en internet."
Realidad: Tu ISP, sitios web y redes publicitarias pueden seguir registrando tus actividades; se necesitan más medidas (VPN, modo privado).

Mito: "Si elimino mis redes sociales, me vuelvo anónimo en internet."
Realidad: Puede reducir tu huella digital, pero información previa (fotos, datos de registro, publicaciones) puede seguir en servidores o en cachés.

Mito: "Solo las compañías grandes deben preocuparse por GDPR, LGPD o leyes de privacidad."
Realidad: Cualquier persona o negocio (grande o pequeño) que maneje datos personales puede estar sujeto a regulaciones y responsabilidades legales.

Mito: "Mi smartwatch solo mide pasos, no puede comprometer mi privacidad."
Realidad: Registra datos de localización, salud y rutinas diarias; si se filtran o venden, pueden usarse para fines maliciosos.

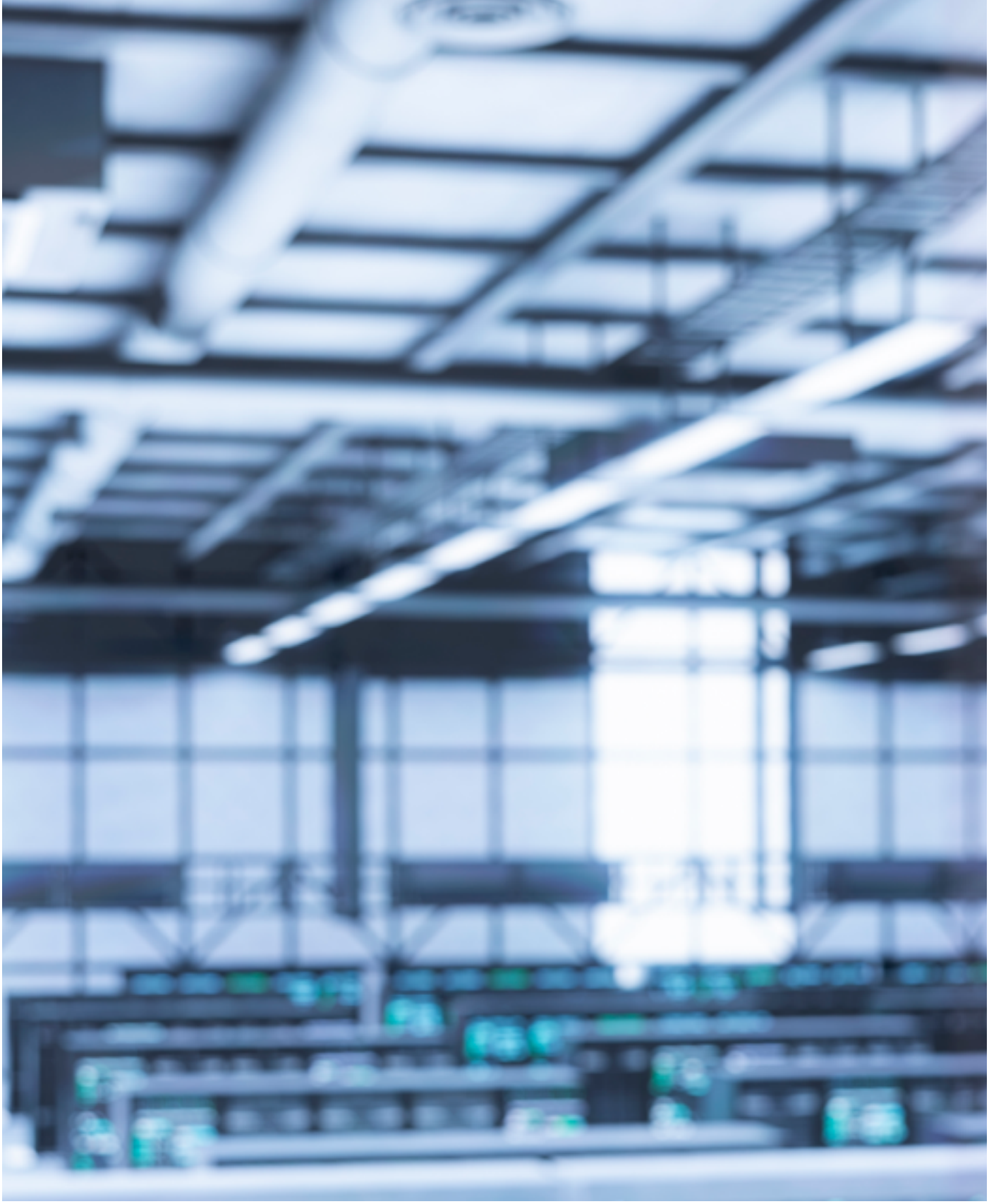
Mito: "Eliminar mensajes de texto o chats equivale a borrarlos para siempre."
Realidad: Muchas apps hacen copias de seguridad y tus datos pueden seguir guardados en la nube o en el dispositivo receptor.

Mito: "Las casas inteligentes son 100% seguras si vienen de una marca reconocida."
Realidad: Cualquier dispositivo IoT puede tener vulnerabilidades o configuraciones inseguras, sin importar la marca.

Mito: "Usar un proxy gratuito me protege tanto como una VPN de pago."
Realidad: Muchas veces los proxys gratuitos no cifran tu tráfico, registran tu actividad o venden tus datos.

Mito: "Con el cifrado extremo a extremo, no necesito preocuparme de nada más."
Realidad: El cifrado protege la comunicación, pero si tu dispositivo está infectado, tus chats pueden ser leídos, o incluso registrados.

Mito: "Las apps de mensajería con cifrado no pueden ser vulneradas."
Realidad: Aunque el cifrado de extremo a extremo es valioso, el dispositivo del usuario puede ser atacado (malware, robo de sesión).



INTELIGENCIA ARTIFICIAL

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. **Responsibility and Ethics:** : 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.

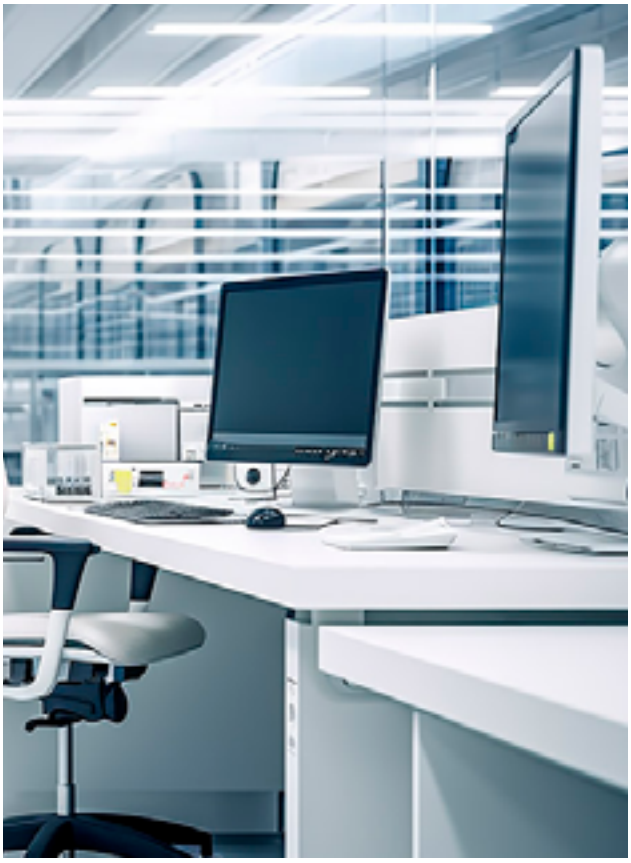
Este motor conversacional es empleado en diversas aplicaciones en el campo de la inteligencia artificial, incluyendo asistentes virtuales, soporte al cliente, tutoriales interactivos y generación de contenido, entre otros. ChatGPT ejemplifica cómo la tecnología actual puede simular interacciones humanas, 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:

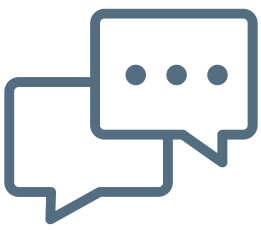
Es crucial aclarar que se está interactuando con una inteligencia artificial al comienzo de la conversación. Esta transparencia es esencial para establecer expectativas adecuadas y prevenir malentendidos.



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.

MEJORES PRÁCTICAS EN LA IMPLEMENTACIÓN DE IA

Reforzamos la **relación intrínseca** entre **la inteligencia artificial, la ciberseguridad y la privacidad,** en tal sentido se han delineado prácticas y lineamientos que ayudan a las organizaciones —y a los usuarios a nivel personal— a:

- **Conocer** los fundamentos y aplicaciones de la IA en seguridad.
- **Implementar** modelos de IA de manera responsable, evitando vulnerabilidades y sesgos.
- **Proteger** la privacidad de las personas y el cumplimiento legal en cada paso del ciclo de vida de la IA.
- **Establecer** un gobierno y una ética claros en torno al desarrollo y uso de la IA.

CICLO DE VIDA SEGURO DE LA IA

Recolección de datos

- **Validez y autenticidad:** Asegurar que los datos provengan de fuentes confiables.
- **Cumplimiento legal:** Respetar las leyes de protección de datos (LGPD, leyes locales
- **Segregación:** Evitar mezclar datos sensibles con datos abiertos en repositorios inseguros.

Despliegue y Operación

- **Monitoreo continuo:** Alertas en tiempo real sobre comportamientos anómalos del modelo.
- **Escalabilidad:** Diseñar la infraestructura para soportar incrementos de datos y usuarios sin disminuir la seguridad.
- **Actualizaciones y parches:** Mantener los entornos de producción con los últimos parches de seguridad.

Recomendaciones concretas

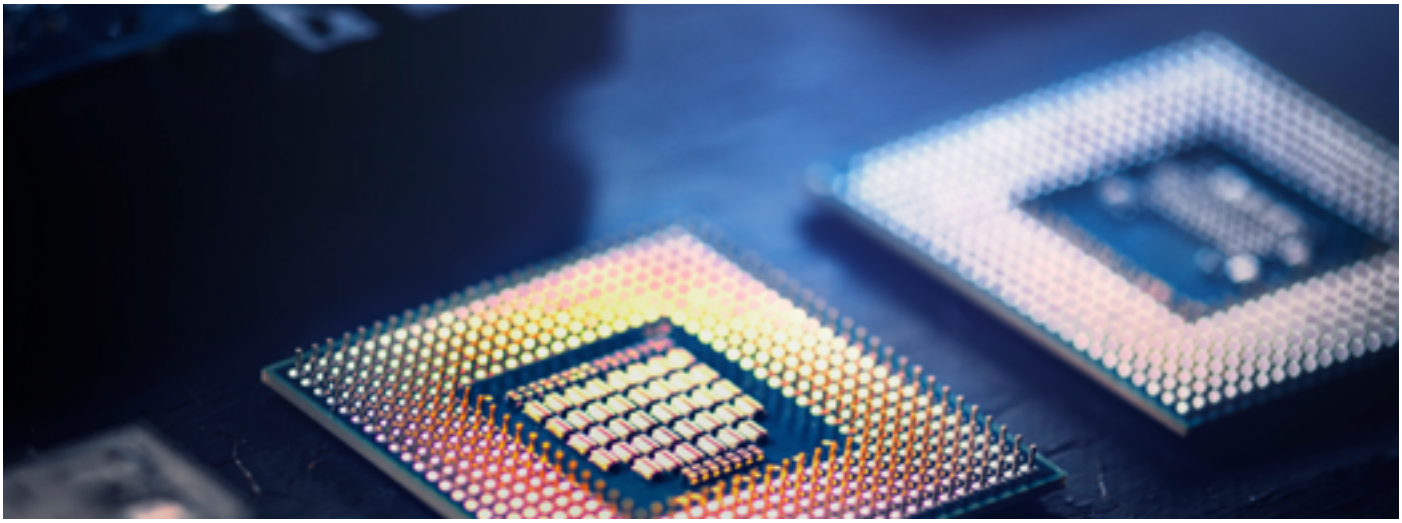
- **Comité de Ética y Cumplimiento:** Supervisar el uso y desarrollo de la IA para mantener estándares de calidad y ética.
- **Gestión de la información:** Clasificar los datos y aplicar las medidas de seguridad correspondientes (cifrado, accesos restringidos).
- **Auditorías periódicas:** Revisar la performance de los modelos y la integridad de los datos de entrenamiento.

Entrenamiento de modelos

- **Calidad de datos:** Implementar procesos de limpieza y etiquetado correcto para evitar sesgos.
- **Reducción de sesgos:** Verificar la representatividad de la muestra y realizar validaciones cruzadas.
- **Evaluación de robustez:** Someter el modelo a pruebas de adversarios para medir su resistencia ante ataques.

Transparencia y explicabilidad (Explainable AI)

- **Herramientas de auditoría:** Integrar soluciones que permitan rastrear cómo el algoritmo toma decisiones.
- **Reportes ejecutivos:** Presentar hallazgos e interpretaciones de forma clara a la alta dirección y partes interesadas.
- **Responsabilidad:** Definir qué área de la organización es dueña de los modelos de IA y rinde cuentas sobre sus resultados.



RECOMENDACIONES DE CIBERSEGURIDAD PARA SOLUCIONES DE IA

Seguridad del pipeline de datos

- **Cifrado de Datos:** Datos en reposo y en tránsito deben estar cifrados con protocolos robustos (TLS 1.2/1.3, AES-256).
- **Controles de Acceso:** Implementar roles y privilegios mínimos (modelo de cero confianza o Zero Trust) para el equipo que manipula datos.
- **Documentación y Trazabilidad:** Mantener un registro detallado de qué datos se utilizaron, cómo y cuándo fueron procesados para fines de auditoría.

Evaluaciones periódicas de riesgos

- **Pentesting y red teaming:** Someter la infraestructura de IA a pruebas de intrusión para detectar vulnerabilidades.
- **Revisión de Modelos:** Utilizar técnicas de adversarial testing para identificar posibles manipulaciones.
- **Plan de Respuesta a Incidentes (PRI):** Definir procedimientos claros para aislar sistemas comprometidos y notificar a las partes afectadas.

Gestión de identidad y accesos

- **Autenticación Multifactor (MFA):** Exigir MFA para todos los accesos a los sistemas críticos de IA.
- **Privilegios Mínimos:** Asignar únicamente los permisos indispensables para ejecutar tareas específicas (principio de least privilege).
- **Supervisión Continua:** Monitorear la actividad de los usuarios con acceso a modelos y datos sensibles, detectando patrones sospechosos.

PROTECCIÓN DE LA PRIVACIDAD EN PROYECTOS DE IA

Cumplimiento legal y marco normativo

- **Revisión de regulaciones locales:** Asegurarse de cumplir con las leyes de protección de datos de cada país donde se opera.
- **Consentimiento informado:** Incluir cláusulas claras sobre el tratamiento de datos en formularios y contratos.
- **Retención de datos:** Definir tiempos prudentes de conservación y mecanismos para su eliminación segura.

Anonimización y seudonimización

- **Anonimización:** Proceso que impide la identificación del individuo dentro de un conjunto de datos. Ideal para proyectos de investigación o análisis de grandes volúmenes.
- **Seudonimización:** Remplazar información que identifica de forma directa a un individuo por un seudónimo, permitiendo ciertas tareas analíticas sin exponer datos sensibles.
- **Buenas prácticas:** Combinación de técnicas de masking, encriptación y fragmentación de datos.

Mecanismos de control y auditoría

- **Revisión de terceros:** Contratar servicios de auditoría externa o certificaciones (e.g., ISO 27001, SOC 2) que validen las prácticas de privacidad en los procesos de IA.
- **Herramientas de Data Governance:** Soluciones que facilitan la gestión del ciclo de vida de los datos y aseguran la trazabilidad de cada uso.

GOBIERNO DE LA IA Y ÉTICA EMPRESARIAL

Políticas y lineamientos internos

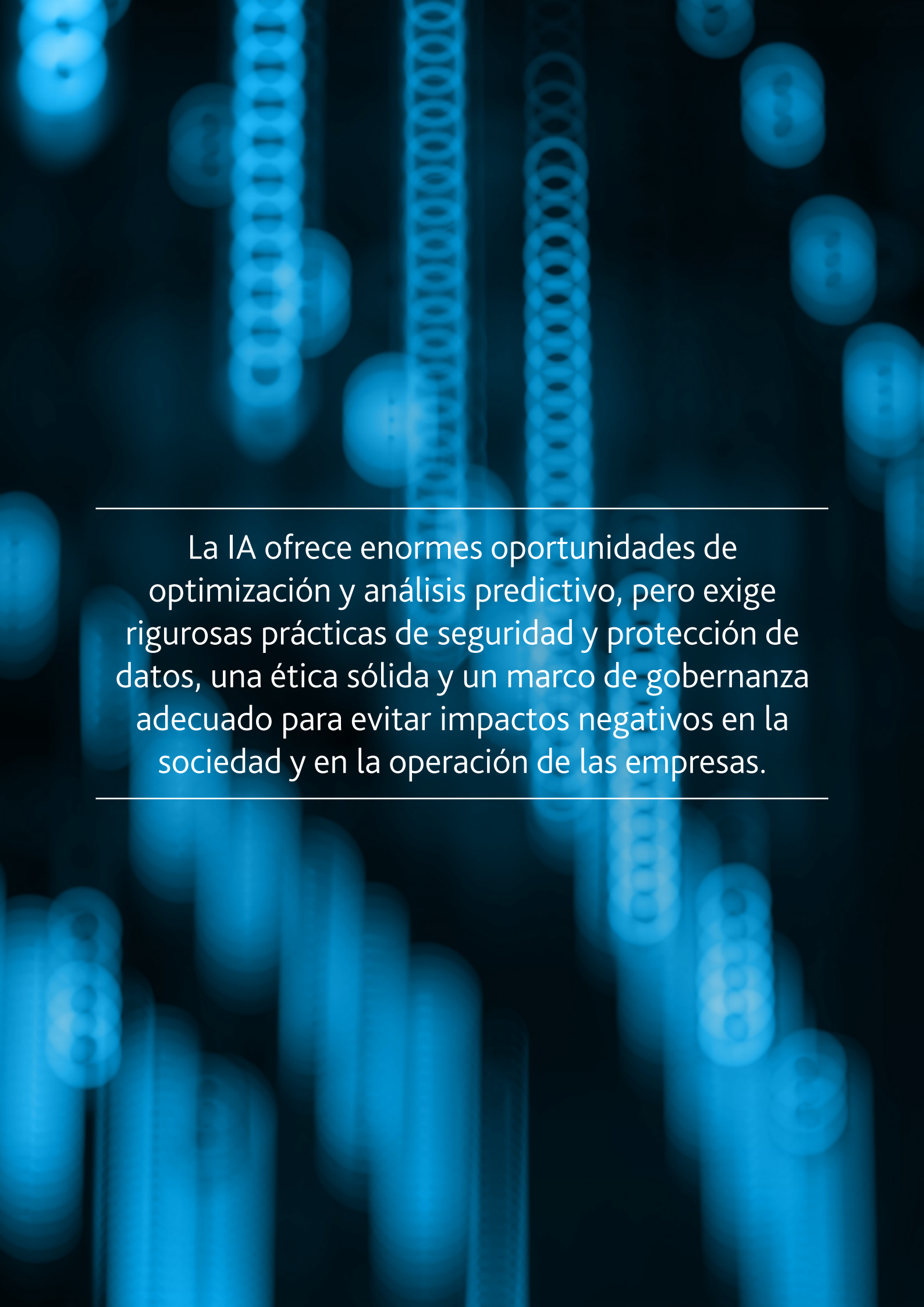
- **Marco de referencia:** Definir una política corporativa que establezca la visión, misión y objetivos del uso de la IA.
- **Roles y Responsabilidades:** Determinar quién supervisa la implementación (Comité de IA, Dirección de Innovación, CISO, etc.).
- **Códigos de conducta:** Incluir pautas específicas sobre el tratamiento de datos y la no discriminación en los algoritmos.

Detección de sesgos y discriminación

- **Evaluaciones de Equidad:** Herramientas que miden el impacto de los algoritmos en diferentes grupos (género, raza, región).
- **Mecanismos de Corrección:** Ajuste constante de los modelos cuando se detectan sesgos, garantizando la neutralidad del sistema.
- **Transparencia:** Compartir de forma clara con los usuarios y colaboradores la lógica fundamental detrás de las decisiones automatizadas.

Rendición de cuentas y transparencia

- **Comité de Revisión:** Un grupo multidisciplinario que evalúa los proyectos de IA, tanto en fase de diseño como de despliegue.
- **Reportes a la Alta Dirección:** Informes periódicos sobre el estado de la IA, incidentes relevantes y actualizaciones normativas.
- **Comunicación a Stakeholders:** Mantener a clientes, socios y empleados informados de cómo se usan los datos y las implicaciones éticas de los modelos.



La IA ofrece enormes oportunidades de optimización y análisis predictivo, pero exige rigurosas prácticas de seguridad y protección de datos, una ética sólida y un marco de gobernanza adecuado para evitar impactos negativos en la sociedad y en la operación de las empresas.

DECÁLOGO del uso personal de la inteligencia artificial

Selección de herramientas de IA confiables: Revisa la reputación de la aplicación o servicio de IA (reseñas, política de datos). Descarga solo desde fuentes oficiales (Google Play, App Store, sitios verificados).

Limitación de datos personales: Evita compartir información muy sensible (documentos oficiales, contraseñas, datos bancarios) con asistentes virtuales o chatbots. Si es inevitable, verifica que el servicio garantice cifrado y políticas claras de retención de datos.

Configuración de privacidad: Desactiva o limita la recolección de datos innecesarios (micrófono, historial de voz, etc.). No permitas a la IA acceder a tus contactos o ubicación si no es imprescindible para su funcionamiento.

Transparencia y explicabilidad: Elige aplicaciones que ofrezcan información comprensible sobre cómo generan sus resultados. Si la IA realiza recomendaciones importantes (ej. salud, finanzas), busca una segunda opinión humana y fuentes adicionales.

Reconocimiento de sesgos: Comprende que la IA puede presentar sesgos (discriminación por género, edad, origen étnico). Si notas resultados tendenciosos, reporta el problema al desarrollador y considera otras soluciones.

Actualizaciones: Mantén la app o herramienta de IA siempre actualizada para corregir posibles fallos de seguridad. Habilita alertas automáticas que informen sobre nuevas versiones.

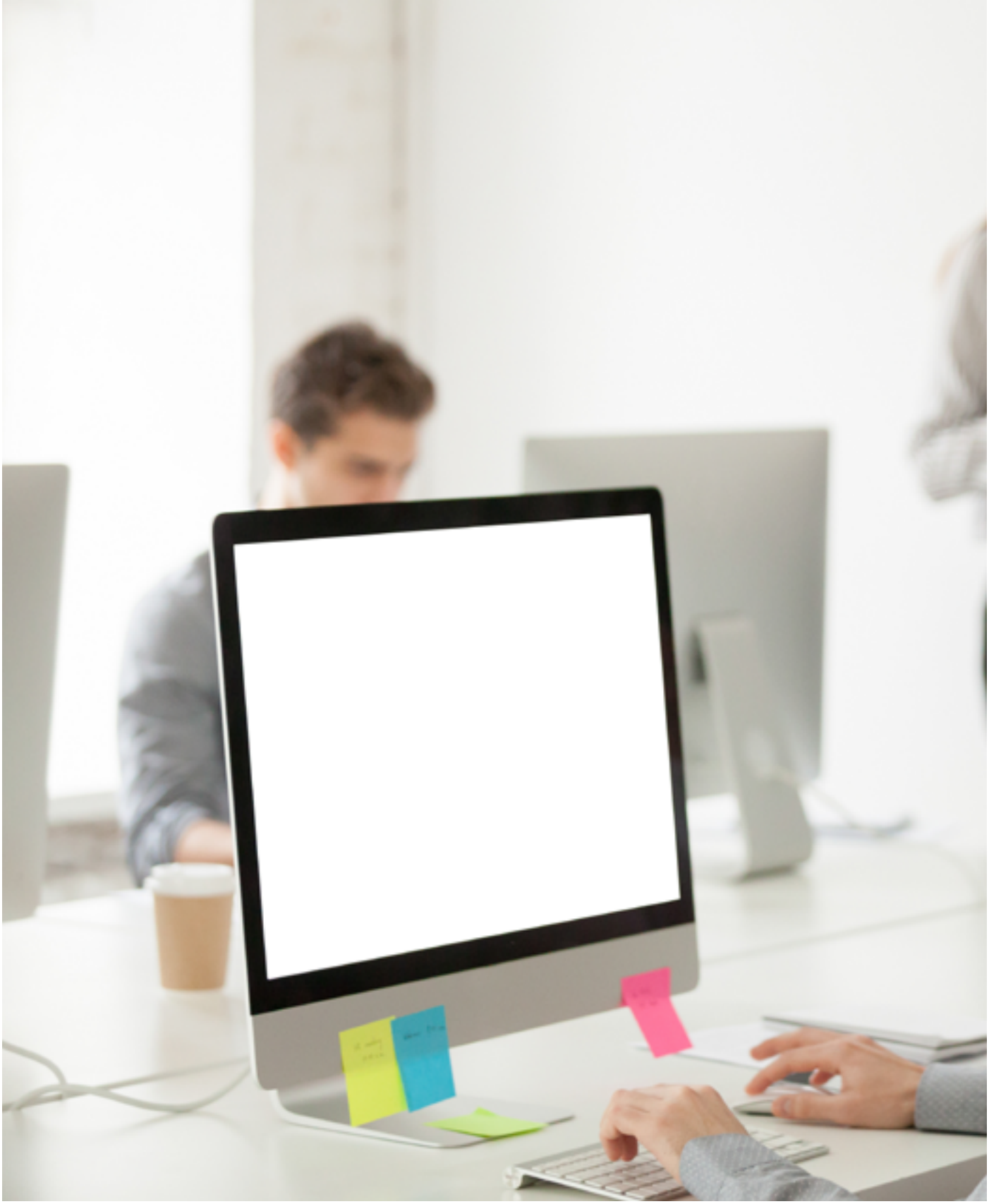
Supervisión en el entorno familiar: Si los niños usan apps de IA (juegos, asistentes), configura controles parentales y supervisa su interacción. Explícales los riesgos de compartir datos personales o imágenes en plataformas de IA.

Uso responsable en redes sociales y contenido: Verifica la veracidad de noticias o información generada por IA antes de difundirla. Ten cuidado con deepfakes o fotos/ videos adulterados que puedan engañar o difamar a personas.

Planes gratuitos vs. planes premium: Revisa las diferencias en políticas de datos: a veces la versión gratuita recolecta más información para publicidad. Evalúa si vale la pena pagar por más privacidad y mejores garantías de seguridad.

Futuro e innovación: Mantente actualizado sobre nuevas tendencias en IA y sus implicaciones. Participa en debates y foros que promuevan un uso ético y responsable de estas tecnologías.

La ciberseguridad, la privacidad y el uso responsable de la IA son elementos clave para tu bienestar digital. Una combinación de buenas prácticas y sentido crítico es la mejor defensa contra los riesgos actuales en línea, tanto para ti como para tus seres queridos.



CONCIENTIZACIÓN GENERAL

50 TIPS PARA MEJORAR LA CALIDAD DE VIDA DIGITAL

PROTECCIÓN DE LA IDENTIDAD Y CREDENCIALES

- **Crea contraseñas robustas y únicas:** Evita usar la misma contraseña para múltiples servicios y combina mayúsculas, minúsculas, números y símbolos.
- **Habilita la autenticación multifactor (MFA):** Aumenta la seguridad requiriendo un factor adicional como SMS, app o llave física.
- **Usa un gestor de contraseñas:** Simplifica y protege tus credenciales almacenándolas en aplicaciones especializadas con cifrado.
- **Cambia regularmente tus contraseñas:** Especialmente si sospechas de actividades sospechosas o hay brechas de seguridad reportadas.
- **Revisa la configuración de recuperación de cuentas:** Asegúrate de tener métodos de recuperación seguros y actualizados (email alternativo, número de teléfono).
- **No compartas tus credenciales:** Ni con familiares, compañeros de trabajo o proveedores de servicios; tu cuenta es personal e intransferible.
- **Elimina cuentas obsoletas:** Cuentas antiguas sin uso representan un riesgo potencial; desactiva o elimina las que ya no utilices.
- **Utiliza frases de paso:** En lugar de contraseñas cortas; combina palabras aleatorias, espacios y números para mayor complejidad.
- **Verifica la legitimidad de enlaces de restablecimiento:** Nunca restablezcas tus credenciales a través de correos o mensajes sospechosos.
- **Activa notificaciones de inicio de sesión:** Recibe alertas cuando tu cuenta se use desde dispositivos o ubicaciones no reconocidas.

CIBERHIGIENE Y PREVENCIÓN DE FRAUDES

- **Piensa antes de hacer clic:** Sé escéptico con enlaces o archivos adjuntos, incluso si parecen legítimos o provienen de contactos conocidos.
- **Verifica la ortografía y el remitente:** Los correos de phishing suelen contener errores gramaticales o direcciones dudosas.
- **Realiza copias de seguridad (backups) periódicas:** Almacénalas en un lugar seguro (disco duro externo, servicio en la nube) y desconéctalas después de cada respaldo.
- **Mantén sistemas y aplicaciones actualizadas:** Instala parches y actualizaciones de seguridad para reducir vulnerabilidades.
- **Utiliza software antimalware confiable:** Activa el cortafuegos (firewall) y asegúrate de que el antivirus esté siempre en funcionamiento.
- **No te dejes llevar por ofertas increíbles:** Si parece demasiado bueno para ser cierto, probablemente sea un fraude.
- **Verifica transacciones:** Comprueba periódicamente tus movimientos bancarios en busca de cargos no reconocidos.
- **Sospecha de urgencias inusuales:** Muchas estafas se basan en la presión del tiempo ("haz clic ahora", "responde inmediatamente").
- **Denuncia intentos de fraude:** Reporta a tu departamento de TI o a las autoridades pertinentes para frenar la propagación de ataques.
- **Educa a tu entorno:** Comparte buenas prácticas con familiares, amigos y colegas para crear una cultura de ciberhigiene colectiva.

USO RESPONSABLE DE LA IA Y HERRAMIENTAS DIGITALES

- **Revisa la confiabilidad de las herramientas de IA:** Asegúrate de que provengan de proveedores reconocidos y verifiques su reputación en el mercado.
- **Ajusta la configuración de privacidad:** Desactiva la recolección de datos innecesarios y revisa los permisos en aplicaciones de IA o asistentes virtuales.
- **Evita introducir datos sensibles en soluciones de IA externas:** Especialmente si no cuentas con garantías de cifrado o acuerdos de confidencialidad.
- **Participa en la definición de políticas de IA:** En tu empresa u organización, contribuye a establecer lineamientos claros sobre su uso.
- **Actualiza las herramientas de IA:** Asegúrate de instalar parches de seguridad y mejoras en la versión de la app o software que utilices.
- **Conoce los límites legales de la recolección de datos:** Infórmate sobre las leyes de protección de datos y cumplimiento normativo en tu país.
- **Solicita consentimiento expreso:** Cuando recolectes datos de terceros para entrenar modelos o usar funcionalidades basadas en IA.
- **Mantén auditorías periódicas de tus modelos:** Verifica que no existan sesgos o vulnerabilidades de seguridad en el funcionamiento de la IA.
- **Fomenta la explicabilidad:** Busca soluciones que permitan comprender cómo la IA llega a sus resultados y decisiones.
- **Desconfía de la "IA milagrosa":** Ninguna herramienta es perfecta; mantiene un criterio humano y soluciones de respaldo en procesos críticos.

PRIVACIDAD Y PROTECCIÓN DE DATOS

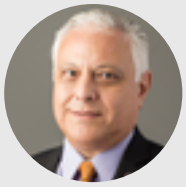
- **Lee la política de privacidad:** Conoce cómo las aplicaciones manejan y comparten tu información personal.
- **Minimiza la información que compartes:** Evita publicar datos sensibles (dirección, teléfono, documentos de identidad) en redes sociales o foros.
- **Configura la privacidad de tus cuentas:** Ajusta quién puede ver tu perfil, fotos y publicaciones, manteniendo solo a contactos de confianza.
- **Desactiva la geolocalización:** Solo actívala cuando sea estrictamente necesario (ej. servicios de mapas o entrega de paquetes).
- **Emplea VPN en redes públicas:** Cifra tu tráfico para evitar el robo de datos en Wi-Fi públicas o de baja seguridad.
- **Controla tus permisos en aplicaciones móviles:** Revisa periódicamente a qué información acceden (contactos, cámara, micrófono) y deshabilita lo innecesario.
- **Usa cifrado en mensajería:** Prefiere plataformas con cifrado de extremo a extremo para conversaciones sensibles.
- **Ten un plan de contingencia:** ¿Qué harás si tu información es comprometida? Prevé pasos legales y técnicos.
- **Solicita la eliminación de datos:** Cuando ya no desees usar un servicio, ejerce tu derecho a ser olvidado (según normativas locales).
- **Monitorea tu huella digital:** Busca tu nombre en línea para detectar información desactualizada o que pueda exponer tu privacidad.

BIENESTAR DIGITAL Y EQUILIBRIO PERSONAL-LABORAL

- **Establece horarios de desconexión:** Define momentos sin dispositivos o notificaciones para preservar tu salud mental.
- **Reduce el consumo digital innecesario:** Limita el tiempo en aplicaciones o redes que no te aporten valor real.
- **Configura notificaciones de forma inteligente:** Evita la sobrecarga de información priorizando alertas realmente importantes.
- **Practica ergonomía:** Acomoda tu postura, ajusta la luz de la pantalla y respeta pausas activas para prevenir fatiga visual y física.
- **Administra tu tiempo en línea:** Herramientas como temporizadores o apps de productividad pueden ayudarte a cumplir metas sin distracciones.
- **Equilibra tu vida personal y profesional:** No mezcles cuentas o dispositivos laborales con los personales.
- **Automatiza tareas rutinarias:** Apóyate en IA o software de gestión para reducir carga operativa y concentrarte en lo estratégico.
- **Fomenta relaciones digitales positivas:** Apoya y colabora con tu equipo de trabajo, intercambia feedback constructivo y buenas prácticas.
- **Reflexiona sobre tu dependencia tecnológica:** Observa si los dispositivos te están controlando en lugar de ser una herramienta a tu servicio.
- **Capacítate continuamente:** Invierte en formación digital y ciberseguridad; el entorno tecnológico cambia con rapidez.

La adopción de estas prácticas no solo fortalece la **postura de ciberseguridad** de cada persona y organización, sino que también contribuye a una **experiencia digital más saludable,** consciente y responsable.

Contacto:



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

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

bdoargentina.com