DESDE EL CORAZÓN DEL ESTADO

la Gobernación se cuenta

Año 2 Ciudad del Vaticano Número 2

TRIMESTRAL ABRIL-JUNIO 2025

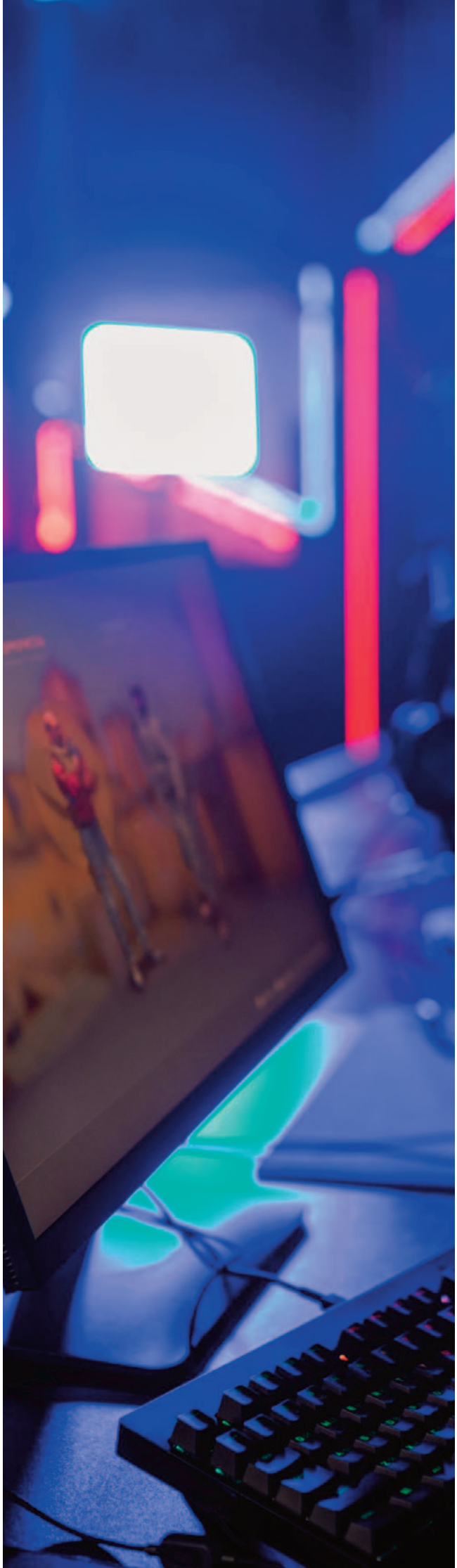
Publicado por la Gobernación del
Estado de la Ciudad del Vaticano

Comunicación Institucional
00120 Ciudad del Vaticano
(Estado de la Ciudad del Vaticano)
Correo electrónico: comunicazione@scv.va

Sitio web: www.vaticanstate.va

X (Twitter): @governatorato
Instagram: Governatorato_SCV

Responsable editorial: Nicola Gori
Editor: Gobernación del Estado de la Ciudad del Vaticano



LA SEGURIDAD INFORMÁTICA ES RESPONSABILIDAD DE TODOS

La decisión de dedicar este número del boletín a la ciberseguridad nace del deseo de ofrecer una suerte de vademécum que sirva de guía y protección en una realidad tan compleja y cambiante. Estamos convencidos de que, a título individual, cada persona tiene su parte de responsabilidad en la seguridad informática.

De hecho, dadas sus implicaciones, las cuestiones relativas a la ciberseguridad trascienden con mucho los aspectos puramente técnicos. Afectan, entre otras dimensiones, a la gestión de riesgos, al derecho, a la comunicación, a la privacidad, a la economía, etc.

Es evidente que la ciberseguridad constituye un ámbito altamente especializado, que involucra a expertos en informática, matemáticas o física. Sin embargo, forma ya parte inseparable de nuestra vida cotidiana, al igual que el entorno digital y, más recientemente, la inteligencia artificial.

Se ocupa de proteger sistemas informáticos, redes, datos y dispositivos frente a amenazas cibernéticas, ataques y vulneraciones de la privacidad. Está al servicio de la confidencialidad y de la disponibilidad de los recursos digitales, con el fin de evitar daños y garantizar protección y seguridad en todas las actividades realizadas en el entorno digital.

En este contexto, resulta esencial tomar conciencia de que, dentro de la Gobernación —donde se utilizan herramientas digitales de forma habitual— cada persona tiene una cuota de responsabilidad en la protección de la estructura.

En este boletín se recogen algunas recomendaciones útiles elaboradas por un grupo de expertos en la materia, que pueden aplicarse a nuestra relación cotidiana con el mundo digital. Entre las indicaciones más relevantes destaca la atención que debe prestarse a los mensajes de origen desconocido, a los archivos

adjuntos y a los dispositivos USB potencialmente inactivos o maliciosos. En caso de duda, lo más sensato es pedir asesoramiento y avisar al responsable de seguridad.

No en vano, los ataques informáticos pueden tener consecuencias muy negativas para la integridad de las estructuras digitales. Los cibercriminales persiguen, por lo general, beneficios económicos, como en el caso de los ataques de tipo ransomware. Pero también buscan apropiarse de información sensible que puede repercutir directamente sobre las personas. Es el caso, por ejemplo, del robo de datos personales —como ocurre con la suplantación de identidad— que luego son vendidos a organizaciones delictivas para fines ilícitos.

Además, un ataque dirigido a una institución puede dañar gravemente la confianza que la sociedad deposita en ella. Por ello, cuando una página web es atacada, el impacto negativo sobre su imagen pública resulta casi inevitable.

En casos extremos, si llega a comprometerse la integridad de los sistemas informáticos, puede verse afectado el propio funcionamiento de la organización. Los efectos pueden ser devastadores, especialmente si el objetivo es el sistema de un hospital o de un servicio de transporte.

Por todas estas razones, es fundamental estar bien informado y ser plenamente consciente de la responsabilidad individual que cada uno tiene para evitar que se den oportunidades a quienes actúan con malas intenciones.

Con este propósito, este boletín recoge una serie de consejos especialmente valiosos y prácticos.

Nicola Gori

LA SEGURIDAD, EN PRIMER LUGAR

La Gobernación del Estado de la Ciudad del Vaticano ha situado siempre la seguridad y la protección de sus sistemas informáticos en el centro de sus prioridades. Se trata de un compromiso que ha acompañado desde sus inicios la implantación y el desarrollo de la red de internet dentro del Estado y de sus sistemas operativos.

Las inversiones destinadas a la ciberseguridad no son en absoluto secundarias, pues persiguen ante todo proteger y salvaguardar la imagen del Santo Padre, así como garantizar el uso cotidiano de los dispositivos al servicio del Estado que lo asiste.

En esta línea, la Dirección de los Servicios de Seguridad y Protección Civil de la Gobernación firmó, el 18 de julio de 2024, un Protocolo de Entendimiento con la Agencia de Ciberseguridad Nacional de la República Italiana (ACN).

El objetivo de este acuerdo ha sido fomentar el intercambio de información, el desarrollo de actividades formativas y la promoción de proyectos de ciberseguridad, con el fin de fortalecer las capacidades y competencias técnicas y científicas en materia de prevención del riesgo asociado a la criminalidad en el ciberespacio. Se ha tratado, sin duda, de un paso significativo hacia una mayor cooperación en la elaboración de programas de formación en el ámbito de la ciberseguridad.

Con especial atención al intercambio de información, experiencias y procedimientos en este campo, el acuerdo persigue garantizar la protección del espacio cibernético, así como promover proyectos de investigación orientados al refuerzo de las capacidades y competencias técnicas y científicas.

Es evidente que este Protocolo de Entendimiento constituye tan solo una parte del esfuerzo sostenido de la Gobernación por asegurar, en todas sus realidades institucionales, los pilares de la seguridad informática: defensa perimetral, protección de la información, gestión de identidades y accesos (IAM), integridad de los datos y disponibilidad de los sistemas.

A pesar de la importante inversión realizada en materia de ciberseguridad, no basta con sistemas operativos ni con soluciones tecnológicas avanzadas: es indispensable la colaboración activa de todos los miembros de la comunidad laboral de la Gobernación. Esa implicación colectiva marca la diferencia y permite alcanzar un mayor nivel de protección.

Por ello, esta newsletter quiere ser una oportunidad para adquirir y afianzar buenas prácticas que eviten ofrecer resquicios a quienes pretenden infiltrarse.

Con este deseo, os invito cordialmente a una lectura provechosa.

Sor Raffaella Petrini

Presidenta de la Gobernación del Estado de la Ciudad del Vaticano

CIBERSEGURIDAD: UNA VISIÓN ESTRATÉGICA ENTRE TECNOLOGÍA, RESILIENCIA Y CULTURA DE LA SEGURIDAD

En un mundo cada vez más interconectado, donde la digitalización impregna todos los ámbitos de la vida y del trabajo, la **cyber security** (ciberseguridad) ha dejado de ser un asunto técnico reservado a los departamentos de TI para convertirse en uno de los grandes retos estratégicos en la protección de servicios, datos y asset. Las amenazas cyber, capaces de golpear con rapidez, a gran escala y con efectos transversales, exigen una respuesta cada vez más sistémica, coordinada y sostenida en el tiempo.

El momento actual exige desarrollar una visión estratégica a largo plazo que garantice la protección del espacio digital propio. Esta visión ha de sustentarse sobre tres pilares fundamentales:

- Infraestructuras y procesos seguros;
- Competencias técnicas avanzadas;
- Una cultura de seguridad arraigada y compartida.

El análisis de la situación actual revela que las infraestructuras digitales —redes, centros de datos, plataformas— están concebidas hoy para ofrecer robustez, continuidad operativa y fiabilidad, incluso en contextos marcados por la contención del gasto. Sin embargo, la rápida evolución tecnológica y el crecimiento exponencial de las amenazas obligan a adoptar un modelo de evolución continua. No se trata simplemente de actualizar hardware y software, sino de transformar el conjunto del sistema en una infraestructura adaptativa e inteligente, capaz de aprender de los datos y responder en tiempo real. En este sentido, la adopción de modelos de zero trust architecture, la virtualización de sistemas y la integración de la inteligencia artificial en los mecanismos de detección representan elementos clave para una defensa avanzada.
Tradicionalmente, la seguridad informática se ha enfocado en la protección del perímetro: cortafuegos, antivirus, segmentación de redes. Hoy en día, este enfoque resulta claramente insuficiente. Los ataques no se limitan a forzar las "puertas de entrada", sino que explotan vulnerabilidades internas, comportamientos humanos y dispositivos conectados.

Una estrategia de ciberseguridad moderna debe incluir:
-Supervisión continua e **threat intelligence**, con capacidad

para analizar flujos de datos en tiempo real, identificar patrones anómalos y anticipar comportamientos maliciosos.
- **Incident response** y resiliencia operativa, mediante planes estructurados que garanticen la business continuity, incluso en medio de un ciberataque.
- Disuasión cibernética, reforzando las capacidades defensivas para desalentar posibles atacantes, también mediante la cooperación internacional y la diplomacia digital.
- Protección integral de end- to, asegurando la seguridad en cada fase del ciclo de vida de los datos: desde su recogida hasta su destrucción.

Este enfoque supone una transición desde la defensa reactiva hacia una actitud proactiva: identificar, evaluar y neutralizar amenazas antes de que se conviertan en incidentes.
Uno de los aspectos más infravalorados —y, al mismo tiempo, decisivos— de la ciberseguridad es el llamado factor humano. Las estadísticas demuestran que una parte significativa de los ataques informáticos logra su objetivo a causa de errores humanos, despistes o falta de concienciación. Por ello, junto con la innovación tecnológica, resulta imprescindible fomentar una cultura de la seguridad que abarque todos los niveles de la organización: desde la alta dirección hasta los usuarios finales. En este marco, iniciativas como la formación continua del personal, las

campañas de concienciación frente al phishing y social engineering, los simulacros de ataque y los cursos de higiene digital se convierten en herramientas fundamentales para crear un ecosistema seguro.

Conviene, por ejemplo, incorporar y poner en valor los cinco factores clave de la cyber hygiene dentro de la dinámica organizativa.
- Segmentación. La red de datos debe dividirse en zonas delimitadas que garanticen la protección del conjunto del sistema y hagan que los puntos de acceso no sean vulnerables a los ataques. Este tipo de protección permite también adaptarse a las necesidades del trabajo en remoto. En caso de producirse una brecha, la seguridad intrínseca de la red debe ser capaz de contenerla sin comprometer el resto de las operaciones.
- Cifrado. Si los firewall y los protocolos de acceso han sido vulnerados y las demás defensas fallan, el encryption asegura que todos los datos sensibles almacenados resulten inservibles para los cyber criminals. Si no se dispone del método para descifrarlos y recomponerlos, los datos cifrados se convierten en un rompecabezas prácticamente irresoluble. Una buena cyber hygiene implica cifrar archivos y datos antes de compartirlos. Lo mismo se aplica, siempre que sea posible, al cifrado del tráfico de red.
- Autenticación de doble factor. La seguridad está cada vez más ligada a la persona; el reconocimiento facial y las huellas dactilares son ejemplos evidentes. Incluso la implementación de una autenticación básica two-factor puede ser eficaz para frenar una primera oleada de accesos indebidos. Cuanto más personal es el sistema de autenticación, más seguras serán las redes. A fin de cuentas, robar una huella dactilar es mucho más difícil que adivinar un PIN.
- Actualización constante. El malware evoluciona constantemente, volviéndose cada vez más sofisticado. Por ello, es imprescindible estar al día y reaccionar de inmediato mediante las actualizaciones diseñadas específicamente para hacerle frente.
- Privilegio mínimo. Aunque se confíe plenamente en los empleados, no todos necesitan disponer del mismo nivel de acceso. Una buena política de seguridad consiste en conceder a cada usuario únicamente los permisos estrictamente necesarios para desempeñar su función. Cuanto más se restrinja el acceso a los datos sensibles, menor será la superficie de exposición ante posibles vulnerabilidades.

Para concluir, si miramos hacia el futuro, el concepto clave no es únicamente la cyber security, sino la más amplia y ambiciosa cyber resilience. Esto significa:
- anticiparse a lo imprevisible,
- responder con flexibilidad y agilidad ante eventos críticos,
- restablecer las funciones en plazos definidos,
- adaptarse y mejorar continuamente.

En el ciberespacio, la resiliencia importa más que la invulnerabilidad.
La máxima protección se alcanza invirtiendo en la construcción de una identidad cibernética sólida, basada en infraestructuras resilientes, personas plenamente conscientes y una acción estratégica multicapas. Solo así será posible afrontar con éxito los retos de la seguridad digital del presente y del mañana.

Ing. Antonino Intersimone
Director de la Dirección de Telecomunicaciones y Sistemas Informáticos

DIEZ REGLAS DE ORO PARA ESTAR EN LA RED CON SEGURIDAD: CÓMO PROTEGER TU VIDA DIGITAL FRENTE A AMENAZAS Y ESTAFAS

La seguridad en línea es una de las principales preocupaciones de la era digital. Proteger los propios datos e identidad en la Red resulta fundamental para evitar fraudes, robos de identidad y ataques informáticos. A continuación, se presentan **diez reglas esenciales** para navegar con seguridad y reducir los riesgos.

1. Utiliza contraseñas robustas y únicas; opta preferentemente por el uso de frases de paso (passphrases)

Según las directrices del **National Institute of Standards and Technology (NIST)**, una contraseña segura debe tener entre **12 y 16 caracteres** como mínimo, incluir **letras mayúsculas y minúsculas**, **números y caracteres especiales**, y evitar palabras de uso común. Se recomienda emplear un **password manager** para generar y almacenar de forma segura las credenciales, evitando reutilizar la misma clave en distintos servicios.

En el ámbito de la ciberseguridad, el uso de passphrases o frases de paso representa una práctica cada vez más extendida y recomendable. A diferencia de las contraseñas tradicionales, las frases de paso constituyen una secuencia más larga y estructurada de palabras, diseñada para ofrecer un nivel de protección superior en los procesos de autenticación.

Mientras que las contraseñas convencionales suelen limitarse a una cadena de hasta dieciséis caracteres, una frase de paso puede alcanzar o incluso superar los cien. Su estructura, basada en una combinación de palabras, signos de puntuación y letras en mayúscula y minúscula, la convierte en un método altamente resistente frente a los ataques informáticos, sin dejar de ser fácil de recordar para el usuario.

El uso de frases de paso no solo refuerza la seguridad frente a accesos no autorizados, sino que también mejora la usabilidad: a diferencia de las secuencias alfanuméricas complejas de las contraseñas tradicionales, las frases de paso tienen sentido gramatical, lo que las hace más intuitivas y menos propensas al olvido.

Este tipo de autenticación se emplea ampliamente en contextos que exigen altos estándares de seguridad, como la encriptación de datos y la protección de sistemas operativos y aplicaciones avanzadas. El creciente apoyo a las passphrases por parte de diversas plataformas digitales subraya la necesidad de evolucionar en las prácticas de protección de accesos, buscando un equilibrio entre seguridad y facilidad de uso.

2. Activa la autenticación multifactor (MFA)

La autenticación multifactor (MFA) añade una capa adicional de seguridad, al requerir más de un método de verificación para acceder a las cuentas. Además de la contraseña, puede incluir códigos OTP enviados por SMS o generados por una aplicación de autenticación, reconocimiento biométrico o llaves físicas de seguridad, dificultando los accesos no autorizados. El NIST **recomienda** preferir las **aplicaciones de autenticación** o **llaves físicas** frente a los SMS, ya que estos pueden ser interceptados.

3. Desconfía de correos electrónicos y mensajes sospechosos (Phishing)

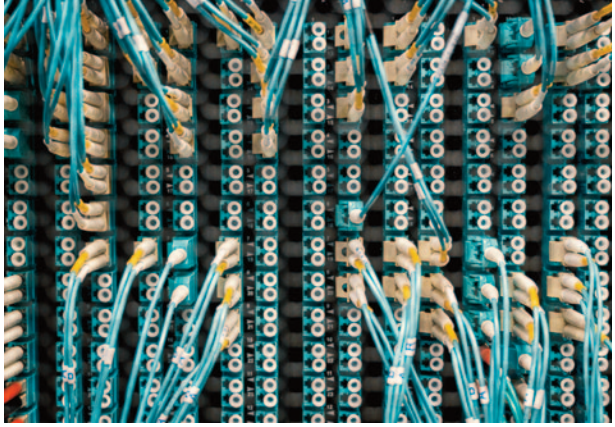
Las estafas de phishing buscan obtener información sensible simulando comunicaciones oficiales. Es fundamental no hacer clic en enlaces sospechosos y verificar siempre el remitente antes de introducir datos personales o bancarios. Según el **Centro Na-**

cional de Ciberseguridad (NCSC), más del **90 % de los ataques informáticos** comienzan con un correo electrónico de phishing.

4. Mantén los dispositivos y programas actualizados
Las actualizaciones del sistema y de las aplicaciones suelen incluir **parches de seguridad** que protegen frente a vulnerabilidades conocidas. Activar las actualizaciones automáticas es una práctica muy recomendable. El **NIST** y otros organismos de seguridad aconsejan aplicar de inmediato los parches de seguridad para evitar ataques basados en exploits ya identificados.

5. Protege los datos sensibles y la privacidad
Evita compartir información personal o financiera en sitios no seguros y limita la cantidad de datos que publicas en redes sociales. Es conveniente revisar periódicamente los ajustes de privacidad para controlar quién puede ver tu contenido. El **Reglamento General de Protección de Datos (RGPD)** subraya la importancia de proteger los datos personales para evitar un uso indebido de los mismos.

6. Verifica la seguridad de los sitios web
Antes de introducir datos sensibles en una página web, asegúrate de que utiliza el protocolo **HTTPS** y que el certificado SSL esté en vigor. Los sitios de confianza muestran un icono de candado junto a la dirección en la barra del navegador. Según el **Google Transparency Report**, los sitios que no emplean HTTPS son más vulnerables a interceptaciones y ataques de tipo man-in-the-middle.



7. Evita redes Wi-Fi públicas no protegidas
Las redes Wi-Fi abiertas suelen ser vulnerables a ataques. Si es necesario utilizarlas, conviene navegar únicamente en sitios seguros y emplear una VPN (Red Privada Virtual) para proteger los datos transmitidos. El **Federal Bureau of Investigation (FBI)** recomienda no acceder a cuentas bancarias ni introducir datos sensibles mediante Wi-Fi pública sin protección adecuada.

8. Presta atención a los archivos adjuntos y descargas
Los archivos y programas descargados de fuentes poco fiables pueden contener malware. Es una buena práctica verificar la procedencia de los archivos antes de abrirlos y contar con un **antivirus actualizado**. Según la **Cybersecurity and Infrastructure Security Agency (CISA)**, los archivos adjuntos con extensiones .exe, .zip y .js se encuentran entre los vectores de malware más frecuentes.

9. Supervisar regularmente las propias cuentas
Es fundamental vigilar la actividad de las cuentas en línea para detectar posibles accesos sospechosos. Servicios como **"Have I Been Pwned"** permiten comprobar si las credenciales han sido comprometidas en alguna filtración de datos. El Centro Nacional de Ciberseguridad (NCSC) recomienda activar notificaciones para accesos no reconocidos y modificar de inmediato las contraseñas en caso de posibles violaciones de seguridad.

10. Utilizar herramientas de seguridad fiables
El uso de un **antivirus actualizado**, un **firewall activo** y una red privada virtual **(VPN)** contribuye a proteger los datos frente a malware y accesos no autorizados. Es importante escoger herramientas de seguridad fiables y desarrolladas por proveedores reconocidos. El National Institute of Standards and Technology (**NIST)** recomienda habilitar siempre las funciones de seguridad integradas en los sistemas operativos, como el cortafuegos y el control de accesos.

Conclusión
Seguir estas diez reglas ayuda a **reducir considerablemente el riesgo de sufrir ataques informáticos** y a mantener protegida la identidad digital. La concienciación y la prudencia constituyen las mejores defensas frente a las amenazas de la Red. Adoptar estas prácticas proporciona una protección eficaz ante los peligros del entorno digital.

RANSOMWARE: LA ÚLTIMA FRONTERA DE LA EXTORSIÓN DIGITAL Y CÓMO DEFENDERSE

Encender el ordenador una mañana y encontrarse con un inquietante mensaje en la pantalla:

«Tus archivos han sido cifrados. Para recuperarlos, paga un rescate en criptomonedas en un plazo de 72 horas».
Este escenario dramático es, hoy en día, una realidad habitual para muchas empresas y usuarios particulares, debido al ransomware: una de las amenazas más destructivas en el panorama de la ciberseguridad.

¿Qué es el ransomware?
El ransomware (del francés antiguo ranson = rescate, y ware, abreviatura de software) es una forma de malware diseñada para bloquear el acceso a los datos de un sistema mediante técnicas de cifrado. Los atacantes exigen posteriormente el pago de un rescate —normalmente en criptomonedas como Bitcoin, Ethereum u otras— a cambio de la clave de descifrado necesaria para recuperar los archivos.

Existen dos tipos principales de ransomware:
Locker ransomware: impide el acceso completo al dispositivo, haciéndolo inoperativo.
Crypto ransomware: cifra únicamente archivos concretos (documentos, imágenes, bases de datos), dejando operativo el sistema para facilitar la comunicación con los atacantes.

¿Cómo se producen los ataques?
Los ataques de ransomware se propagan mediante diversas técnicas, entre las que destacan:
- Correos de phishing: los atacantes envían mensajes que aparentan provenir de fuentes legítimas. Estos correos incluyen enlaces o archivos adjuntos maliciosos que, al abrirse, instalan el ransomware en el dispositivo de la víctima.
- Descargas desde sitios web comprometidos: acceder a páginas no seguras o descargar software de procedencia dudosa puede exponer al usuario a código malicioso oculto.
- Explotación de vulnerabilidades: los delincuentes aprovechan fallos de seguridad en sistemas operativos o aplicaciones no actualizadas. Es una de las vías más comunes cuando no se aplican parches de seguridad.
- Dispositivos USB infectados: los medios físicos, como memorias USB, también pueden servir para propagar ransomware si se conectan a un dispositivo sin precaución.
- Ataques dirigidos: las grandes organizaciones son a menudo objeto de ataques cuidadosamente planificados, en los que los ciberdelincuentes analizan previamente la red en busca de puntos débiles.

¿Por qué el ransomware es tan peligroso?
El ransomware representa una amenaza crítica por diversas razones:
- Pérdida de datos: sin copias de seguridad adecuadas, los archivos cifrados pueden ser irrecuperables.
- Impacto económico: el rescate exigido, junto con los costes de recuperación y la interrupción de la actividad, puede generar grandes pérdidas.

- Reputación comprometida: para las empresas, un ataque puede afectar gravemente la confianza de clientes, socios y accionistas.
- Evolución constante: el ransomware se actualiza y perfecciona continuamente, dificultando su detección y prevención.

¿Cómo protegerse frente al ransomware?
La prevención es la herramienta más eficaz. Estas son algunas estrategias clave para reducir significativamente el riesgo:
- Copias de seguridad regulares: realizar backups frecuentes en dispositivos externos o en servicios en la nube seguros. Es esencial que estén desconectados de la red principal para evitar su cifrado en caso de ataque.
- Actualizaciones y Patch : mantener el sistema operativo y los programas actualizados. Muchas infecciones se aprovechan de vulnerabilidades conocidas que pueden resolverse con actualizaciones a tiempo.
- Formación del personal: en el ámbito empresarial, es vital concienciar a los empleados sobre el riesgo de correos sospechosos y otras técnicas de ingeniería social. Una formación continua reduce los errores humanos.
- Soluciones de seguridad avanzadas: utilizar antivirus con protección contra ransomware, cortafuegos y sistemas de detección y respuesta ante amenazas.
- Autenticación en dos factores (2FA): añadir una segunda capa de verificación para acceder a cuentas sensibles, dificultando la intrusión.
- Gestión de privilegios: aplicar el principio del mínimo privilegio, otorgando a cada usuario solo los accesos necesarios. Esto reduce el impacto si se compromete una cuenta.
- Supervisión y auditorías periódicas: revisar regularmente la seguridad de los sistemas para detectar posibles fallos antes de que sean explotados.
- Planes de respuesta ante incidentes: disponer de un protocolo claro para actuar en caso de ataque, que incluya cómo aislar los sistemas, comunicar con las partes implicadas y recuperar los datos.

¿Qué hacer en caso de ataque?
Ante un ataque de ransomware, es crucial actuar con rapidez:
- Aislar los sistemas comprometidos: desconectar inmediatamente los dispositivos infectados para frenar la propagación del malware.
- Nunca pagar el rescate: pagar no garantiza la recuperación de los datos y además financia nuevas actividades delictivas.
- Informar a las autoridades: notificar el incidente a las fuerzas de seguridad o a organismos especializados.
- Consultar con expertos en ciberseguridad: profesionales cualificados pueden ayudar a contener el ataque y a restaurar los sistemas. Una herramienta de referencia es www.nomoreransom.org.

Conclusión
El ransomware se ha consolidado como una de las amenazas más graves en la era digital. Sin embargo, con una estrategia de prevención sólida, es posible reducir de forma drástica el riesgo de ser víctima.
Invertir en la formación del personal, en tecnologías de protección y en talento especializado en ciberseguridad ya no es una opción, sino una necesidad imperiosa.
La seguridad informática no debe verse como un lujo, sino como un elemento esencial para proteger la información, garantizar la continuidad del negocio y preservar la confianza en un mundo cada vez más interconectado.

CYBER SECURITY Y SMART HOME: LA PROTECCIÓN DE LOS DISPOSITIVOS CONECTADOS Y LAS NUEVAS AMENAZAS PARA LA PRIVACIDAD

Introducción
La creciente implantación de la tecnología en el ámbito doméstico ha transformado radicalmente nuestra forma de interactuar con el entorno. Desde los electrodomésticos conectados hasta los sistemas de seguridad avanzados, el concepto de hogar inteligente ha hecho nuestras viviendas más eficientes y confortables. Sin embargo, la integración de estos dispositivos plantea nuevos desafíos en materia de ciberseguridad y privacidad que no pueden pasarse por alto.

La vulnerabilidad de los dispositivos IoT
Uno de los principales riesgos reside en la vulnerabilidad de los dispositivos IoT (Internet of Things). A diferencia de ordenadores y smartphone, que suelen incorporar medidas de seguridad sólidas, muchos dispositivos domésticos inteligentes se diseñan con estándares de protección mínimos. Esto los convierte en objetivos fáciles para los ciberdelincuentes, que pueden acceder a cámaras de vigilancia, termostatos o asistentes de voz, comprometiendo así la seguridad del hogar y la privacidad de los usuarios. Una vez que un dispositivo ha sido vulnerado, el atacante podría utilizarlo para espiar la actividad doméstica, recopilar información sensible o incluso tomar el control de otros dispositivos conectados a la red.

El desconocimiento de los usuarios
Otro aspecto crítico es la escasa concienciación de los usuarios en materia de seguridad informática. Muchos consumidores adquieren dispositivos inteligentes sin conocer los riesgos que ello implica. A menudo no cambian las credenciales predeterminadas ni actualizan el software con regularidad, dejando así abiertas vías de acceso para los atacantes. Esta falta de atención a medidas básicas incrementa notablemente el riesgo de intrusión. Además, el tráfico de red doméstico rara vez es supervisado por los propios usuarios, lo que dificulta la detección de anomalías o comportamientos sospechosos.

La protección de los datos personales
Más allá de los ataques directos a los dispositivos, existe una creciente preocupación por la protección de los datos personales. Los dispositivos inteligentes recopilan una gran cantidad de información sobre los usuarios, desde rutinas diarias hasta datos biométricos. Si esta información cae en manos indebidas, podría utilizarse para el robo de identidad, la vigilancia no autorizada o la elaboración de perfiles detallados con fines publicitarios. Algunos fabricantes aplican políticas poco transparentes respecto al tratamiento de datos, lo que dificulta que los usuarios sepan cómo y dónde se almacenan sus datos personales.

Ciberataques a gran escala
Las amenazas informáticas no afectan únicamente a los usuarios individuales, sino que pueden tener consecuencias a gran escala. Los ciberdelincuentes pueden aprovechar la falta de seguridad en dispositivos IoT para crear botnets, redes de dispositivos infectados que se utilizan para lanzar ataques masivos, como los de denegación de servicio distribuida (DDoS). Un ejemplo emblemático fue el ataque de la botnet Mirai en 2016, que explotó miles de dispositivos IoT vulnerables para colapsar servicios online de gran envergadura. Este caso demuestra cómo una gestión inadecuada de la ciberseguridad doméstica puede tener repercusiones incluso a nivel global.

Soluciones y responsabilidades
Enfrentar estos desafíos requiere un compromiso conjunto por parte de fabricantes, usuarios e instituciones. Los fabricantes deberían adoptar estándares de seguridad más exigentes, implementar cifrado avanzado y garantizar actualizaciones automáticas del software que subsanen posibles vulnerabilidades. Los usuarios, por su parte, deberían aplicar prácticas básicas de seguridad, como cambiar las contraseñas predeterminadas, activar la autenticación en dos pasos y monitorizar periódicamente los dispositivos conectados.

El papel de la regulación
En el ámbito normativo se han dado algunos avances mediante regulaciones que exigen estándares mínimos de seguridad para los dispositivos IoT. La Unión Europea, con el Reglamento General de Protección de Datos (RGPD), ha puesto un fuerte énfasis en la salvaguarda de la información personal; sin embargo, la rápida evolución de la tecnología exige una actualización constante del marco normativo para garantizar una protección eficaz. Es fundamental que las empresas asuman la responsabilidad en la protección de los datos de los usuarios y que se establezcan medidas más estrictas para prevenir posibles violaciones.

Conclusiones
En una época en la que la tecnología forma parte integral de nuestra vida cotidiana, garantizar la seguridad de los dispositivos conectados debe ser una prioridad. El hogar inteligente ofrece múltiples ventajas en términos de automatización y confort, pero sin medidas adecuadas de protección, el riesgo de comprometer la privacidad y la seguridad digital es elevado. Solo a través de un enfoque consciente y de la adopción de soluciones avanzadas de ciberseguridad será posible aprovechar plenamente los beneficios de la tecnología sin poner en peligro la integridad de nuestros datos ni nuestra vida privada.

SOCIAL ENGINEERING: CÓMO LOS DELINCUENTES INFORMÁTICOS EXPLOTAN AL SER HUMANO PARA INFILTRARSE EN LOS SISTEMAS

Una jornada laboral cualquiera… Recibimos una llamada urgente de una persona que se presenta como técnico del departamento de informática. Con un tono extremadamente educado y profesional, nos informa de que, debido a un problema crítico con nuestra cuenta, es necesario confirmar ciertos datos personales. Si facilitamos la contraseña y, posteriormente, el código de autenticación, todo podrá resolverse de forma segura y sin demoras. El tono tranquilo y tranquilizador de la conversación podría llevarnos a confiar y colaborar, pero es precisamente en este tipo de situaciones cuando los ciberdelincuentes actúan. Este es un ejemplo clásico de social engineering (ingeniería social).

¿Qué es la Social engineering (ingeniería social)?
La social engineering i es el arte de manipular a las personas para obtener acceso a información o sistemas protegidos. En lugar de intentar vulnerar complejos sistemas de seguridad informática, los delincuentes centran sus esfuerzos en un objetivo no tecnológico: el ser humano.
Los atacantes explotan factores como la confianza, el miedo, la curiosidad o la sensación de urgencia para inducir a la víctima a realizar acciones perjudiciales, como hacer clic en un enlace sospechoso, descargar un archivo malicioso o revelar credenciales confidenciales.

Técnicas comunes de Social Engineering:
1.Phishing
Probablemente la técnica más conocida. Se presenta a través de correos electrónicos, mensajes de texto o llamadas telefónicas (vishing) que simulan provenir de fuentes legítimas. El objetivo es engañar a la víctima para que revele información sensible o descargue malware.
2.Pretexting
Consiste en construir una historia creíble (el pretexto) con el fin de ganarse la confianza de la víctima. Por ejemplo, el atacante puede hacerse pasar por un empleado del departamento de recursos humanos o por un proveedor de servicios.
3.Baiting
Se aprovecha de la curiosidad humana. Un caso típico es el de una memoria USB dejada intencionadamente en un lugar público, con una etiqueta atractiva como "Salarios 2024". Al conectarla a un ordenador, el sistema queda infectado con malware.
4.Tailgating
Es una técnica física: el atacante accede a un edificio restringido aprovechando el paso de otra persona autorizada, fingiendo, por ejemplo, haber olvidado su tarjeta de identificación.

¿Por qué es tan eficaz la Social Engineering ?

Su efectividad se basa en diversos mecanismos psicológicos:
-Confianza: Las personas tienden a confiar en quien adopta un tono profesional o tiene apariencia de autoridad.
-Urgencia: La presión del tiempo puede empujar a tomar decisiones apresuradas.
-Emoción: El miedo o la curiosidad pueden llevar a actuar sin reflexionar.

¿Cómo protegerse?
Protegerse de la ingeniería social exige atención constante, buenos hábitos y el uso de herramientas adecuadas. He aquí algunas recomendaciones, especialmente útiles en el entorno profesional:
1.Formación continua
La concienciación es el primer paso. Participar regularmente en cursos o sesiones breves de formación sobre ciberseguridad resulta fundamental. También es recomendable realizar simulacros de ataque, como intentos ficticios de phishing, para evaluar el

nivel de preparación del equipo.

2.Políticas estrictas de verificación

Nunca debe facilitarse información sensible a quien contacta sin previo aviso, aunque parezca una solicitud legítima. Es mejor detenerse un momento y verificar la identidad del interlocutor. Si un "técnico informático" solicita una contraseña, es preferible llamar directamente al departamento correspondiente utilizando canales oficiales, y no los datos de contacto proporcionados por la propia persona.

3.Cultura de seguridad

Es esencial fomentar una cultura organizativa donde todos se sientan responsables de la seguridad. Hay que promover la comunicación abierta ante solicitudes o comportamientos sospechosos. Nadie debería sentirse incómodo por decir "esto no me parece normal" o pedir una segunda opinión.

4.Protección de los dispositivos

No deben dejarse desatendidos ordenadores portátiles, teléfonos móviles ni otros dispositivos corporativos, sobre todo en espacios públicos o compartidos. Es fundamental utilizar bloqueo de pantalla con contraseña o PIN y configurar el bloqueo automático tras un periodo de inactividad.

5. Autenticación en dos factores (2FA)

Aunque alguien consiga acceder a una contraseña, la autenticación en dos factores proporciona una capa adicional de seguridad. Este sistema, que exige un segundo paso para verificar la identidad del usuario, es esencial para proteger las cuentas corporativas.

6. Control del acceso físico

Es fundamental asegurarse de que solo el personal autorizado pueda acceder a oficinas o zonas sensibles. Herramientas como tarjetas identificativas personales, sistemas de videovigilancia y cerraduras electrónicas son eficaces para prevenir intrusiones físicas.

7. Atención a las señales de advertencia

Prestar atención a los detalles es clave. Correos electrónicos con errores gramaticales, solicitudes inusuales o remitentes desconocidos suelen ser señales de alarma. Antes de hacer clic en un enlace o descargar un archivo adjunto, conviene preguntarse si la solicitud es razonable. En caso de duda, es preferible no arriesgarse.

8. Pruebas y auditorías periódicas

Realizar auditorías de seguridad y pruebas de penetración de forma periódica permite identificar posibles vulnerabilidades en los sistemas y procesos. Estas evaluaciones pueden sacar a la luz debilidades que, de no corregirse, podrían ser aprovechadas por los ciberdelincuentes.

Conclusión

La Social Engineering (ingeniería social) es una amenaza sutil pero no invencible. Ser conscientes de cómo actúan los delincuentes y aplicar buenas prácticas puede reducir significativamente los riesgos. En el entorno laboral, invertir en la formación del personal, fomentar una cultura de la seguridad y utilizar las herramientas adecuadas son pasos fundamentales para proteger la información sensible y los sistemas críticos. Con frecuencia, la seguridad no depende únicamente de la tecnología, sino de hasta qué punto nosotros, como personas, estamos atentos y preparados para reconocer las trampas.

AMENAZAS INVISIBLES: EL CRECIMIENTO DE LOS CIBERATAQUES

Introducción
En la era digital, las amenazas cibernéticas se han convertido en un peligro cada vez más sofisticado y difícil de detectar. Las organizaciones de todos los sectores deben hacer frente a ataques dirigidos contra sus datos sensibles, la continuidad operativa y su reputación corporativa. El aumento de estos ataques conlleva no solo pérdidas económicas directas, sino también una pérdida de confianza por parte de clientes y socios. Este artículo analiza las principales amenazas informáticas, los retos económicos que suponen para las empresas y las estrategias más eficaces para hacerles frente.

1. Principales amenazas cibernéticas
Los ciberataques evolucionan de forma constante y se aprovechan de vulnerabilidades tanto tecnológicas como humanas. Entre las amenazas más habituales se encuentran:
- Ransomware: Software malicioso que cifra los datos corporativos, bloqueando su acceso hasta el pago de un rescate.

- Phishing y spear phishing: Correos electrónicos fraudulentos que, mediante técnicas de ingeniería social, buscan obtener credenciales o datos sensibles.

- Ataques de día cero (Zero-Day): Explotan vulnerabilidades aún desconocidas presentes en el software, antes de que puedan ser subsanadas por los desarrolladores.

Malware y troyanos: Programas maliciosos que se infiltran en los sistemas para robar información o permitir accesos no autorizados.

- Denegación de servicio (DoS) y denegación de servicio distribuida (DDoS): Ataques que saturan los servidores corporativos, impidiendo el acceso a los usuarios legítimos.

-Robo de credenciales y filtraciones de datos: Técnicas orientadas a comprometer cuentas de usuario para acceder a sistemas restringidos.

2. Retos económicos para las organizaciones
Los ataques cibernéticos no solo comprometen los sistemas informáticos, sino que generan un impacto económico considerable. Entre las principales consecuencias destacan:
- Costes de recuperación: Las empresas afectadas deben invertir en análisis forense, restauración de datos y refuerzo de las medidas

de seguridad.
- Sanciones y litigios: Normativas como el Reglamento General de Protección de Datos (RGPD) contemplan sanciones severas en caso de violaciones de datos personales.
- Daño reputacional: La pérdida de confianza por parte de clientes y colaboradores puede afectar gravemente al valor de la marca.
- Interrupción operativa: Un ataque exitoso puede paralizar las operaciones de una empresa durante días o semanas, con pérdidas económicas significativas.

3. Estrategias de defensa y soluciones
Para mitigar los riesgos, las organizaciones deben adoptar una estrategia de ciberseguridad proactiva. Entre las medidas clave se incluyen:

Formación y concienciación: Sensibilizar al personal sobre las amenazas informáticas reduce la probabilidad de ataques basados en el factor humano.
- Implantación de la autenticación multifactor (MFA): Añadir un nivel adicional de verificación refuerza la protección de los accesos.
- Actualizaciones y parches de seguridad: Mantener el software y los sistemas operativos actualizados ayuda a prevenir ataques basados en vulnerabilidades conocidas.
- Copias de seguridad cifradas y periódicas: Realizar backups frecuentes y almacenarlos en entornos seguros garantiza una recuperación ágil ante posibles incidentes.
- Supervisión continua e inteligencia de amenazas (threat intelligence): Emplear herramientas avanzadas para detectar comportamientos sospechosos y responder de forma rápida y eficaz.
- Cortafuegos y sistemas de detección/prevención de intrusiones (IDS/IPS): Proteger la red frente a accesos no autorizados y ataques externos.
- Arquitectura de confianza cero (Zero Trust): Adoptar un modelo de seguridad que no da por fiable ningún acceso por defecto, exigiendo validaciones continuas para cada transacción de datos.

Conclusión
Los ciberataques constituyen una amenaza en constante evolución, con consecuencias relevantes tanto en materia de seguridad como en términos económicos. Adoptar un enfoque proactivo de la ciberseguridad, invertir en la protección de los datos y formar al personal son pasos fundamentales para defenderse de las amenazas invisibles del entorno digital. Solo mediante una estrategia integral y una vigilancia constante es posible proteger eficazmente las infraestructuras corporativas y garantizar la resiliencia operativa.

CIBERSEGURIDAD EN LOS GOBIERNOS: AMENAZAS GLOBALES Y ESTRATEGIAS DE DEFENSA

En los últimos años, la digitalización ha transformado profundamente la manera en que operan los gobiernos, abriendo nuevas oportunidades pero también exponiendo vulnerabilidades inéditas. La seguridad informática se ha convertido en un pilar esencial para la estabilidad nacional, en un contexto en el que las administraciones públicas deben hacer frente a ataques cada vez más sofisticados y dirigidos. La gestión de datos sensibles, el control de infraestructuras críticas y la prestación de servicios esenciales sitúan a los entes gubernamentales en el punto de mira de ciberataques con implicaciones geopolíticas, económicas y sociales.

El coste de los ataques informáticos en el sector público no deja de aumentar, y diversos estudios estiman su impacto financiero en miles de millones de dólares cada año. Un caso emblemático es el del sistema sanitario irlandés, paralizado en 2023 por un ataque de ransomware que ocasionó daños superiores a los cien millones de euros. Incidentes de esta magnitud no constituyen únicamente una cuestión económica, sino que plantean serios problemas de confianza y de seguridad pública. Cuando se compromete la información personal de los ciudadanos, la percepción de vulnerabilidad se propaga con rapidez, debilitando la relación entre el Estado y su ciudadanía.

La reputación de un gobierno puede verse gravemente dañada por una brecha de seguridad informática. En 2020, un ataque a los sistemas sanitarios noruegos expuso los datos personales de casi tres millones de ciudadanos, lo que provocó una drástica caída en el uso de los servicios digitales públicos. El temor a que la información personal pueda ser sustraída o manipulada frena la innovación y obstaculiza la adopción de tecnologías digitales, con repercusiones directas en la modernización de la administración pública y de cualquier estructura gubernamental. Las estrategias de defensa requieren un enfoque multinivel, en el que la prevención y la respuesta ante incidentes desempeñen un papel clave. Muchos de los sistemas utilizados por los entes públicos son tecnológicamente obsoletos, lo que incrementa considerablemente el riesgo de ataque. La modernización de las infraestructuras informáticas debe constituir una prioridad, acompañada de políticas de seguridad estrictas y de una formación continua del personal. El error humano sigue siendo una de las principales causas de las intrusiones informáticas, lo que hace imprescindible desarrollar programas de concienciación y simulacros de ataque que refuercen la capacidad de respuesta frente a las amenazas.

La ciberseguridad no es únicamente una cuestión técnica, sino una cuestión de seguridad nacional. Los ataques a infraestructuras críticas pueden tener consecuencias devastadoras, como se evidenció en el caso del Colonial Pipeline en Estados Unidos, donde un ciberataque interrumpió el suministro de carburante en regiones enteras. La cooperación internacional resulta fundamental para hacer frente a amenazas a gran escala, ya que los ciberdelincuentes operan sin fronteras. El intercambio de información entre gobiernos y agencias de seguridad permite anticipar las amenazas y mejorar la resiliencia global.

El panorama de la ciberseguridad gubernamental se encuentra en constante evolución, con amenazas que se adaptan con rapidez a las nuevas medidas de defensa. Invertir en la protección de los datos y de las infraestructuras críticas ya no es una opción, sino una necesidad ineludible para salvaguardar la estabilidad y la seguridad institucional. En un mundo cada vez más interconectado, proteger el ciberespacio equivale a proteger la propia democracia.

Valerio Mercuri

LOS JÓVENES COMO PROTAGONISTAS DE LA ÉTICA GLOBAL: CIBER DIPLOMACIA, DERECHO, ECONOMÍA Y TECNOLOGÍA EN UN MUNDO INTERCONECTADO

¿Cómo distinguir un hecho real de un deepfake? ¿Quién garantiza que un algoritmo no manipule la opinión pública? Estas preguntas guiaron el debate «Ciber diplomacia, derecho, economía y tecnología en un mundo interconectado. IA y el futuro de las instituciones», organizado por la Dirección de Telecomunicaciones y Servicios Informáticos. Entre presentaciones, datos y casos prácticos, estudiantes y docentes reflexionaron sobre un tema crucial: en un mundo híper conectado, donde la inteligencia artificial (IA) puede crear o destruir la verdad con un solo clic, la ética y el conocimiento se convierten en el único antídoto frente a la desinformación.

IA y posverdad: cuando la tecnología desafía la percepción

El núcleo del encuentro fue el impacto jurídico y económico de los delitos informáticos, así como el papel de la IA en la configuración de la realidad. Por un lado, los ciberataques no constituyen únicamente una amenaza tecnológica, sino que plantean un laberinto de desafíos legales, costes económicos exponenciales y riesgos reputacionales. Desde una perspectiva jurídica, los conflictos de jurisdicción (como el contraste entre el Reglamento General de Protección de Datos europeo y el Cloud Act estadounidense) dificultan la persecución de los delitos digitales, mientras que la ausencia de tratados internacionales vinculantes deja espacios grises aprovechados por piratas informáticos y Estados "rebeldes".

El coste económico es igualmente preocupante: según estimaciones recientes, el cibercrimen supone para la economía global unos 8.000 mil millones de dólares anuales, cifra que probablemente aumente con la llegada de la computación cuántica y los ataques a las cadenas de suministro. Incidentes como el ransomware que afectó al oleoducto Colonial (2021), que interrumpió el flujo de combustible en Estados Unidos, provocaron pérdidas directas por valor de 4,4 millones de dólares, sin contar los daños indirectos a la confianza de los consumidores.

Herramientas como los deepfakes de voz o los vídeos sintéticos amenazan con erosionar la confianza en las instituciones: en 2023, audios falsos atribuidos a políticos provocaron volatilidad en los mercados. Sin embargo, la IA también puede convertirse en una aliada: algoritmos de verificación de hechos (fact-checking) y sistemas de detección de manipulaciones ofrecen esperanzas de control. «El problema no es la tecnología, sino el uso que hacemos de ella». «Se necesitan normas claras: un deepfake en una película es creatividad; para influir en unas elecciones, es un delito».

Sabiduría digital: por qué el conocimiento es un patrimonio que debe protegerse

Si los datos son "el nuevo petróleo", la capacidad de interpretarlos constituye la verdadera riqueza, y protegerlos es el gran desafío. Las intervenciones subrayaron cómo las universidades y los centros de investigación deben formar a los jóvenes no solo en la programación de algoritmos, sino también en la reflexión crítica sobre su impacto social.

¿Un ejemplo? El Reglamento General de Protección de Datos (RGPD) europeo, que limita el uso de datos sensibles, nace de una visión ética: proteger a las personas, no solo a los servidores. «La sabiduría digital consiste en saber equilibrar innovación y derechos». El caso "Cambridge Analytica", presentado como

ejemplo paradigmático, puso de manifiesto la inmadurez del marco jurídico actual, en el que el robo de datos ha distorsionado campañas políticas, y ciberataques sistémicos vinculados a gobiernos han provocado impactos socioeconómicos de gran calado.

Reputación y ciberseguridad: el ser humano en el centro

Hoy en día, la reputación de un Estado o de una empresa se juega en el entorno digital. Ataques como el sufrido por SolarWinds en 2020 —que comprometió datos gubernamentales en Estados Unidos— demuestran que un malware puede causar más daño que un misil. Pero la solución no es solo técnica: «Un cortafuegos no detiene la manipulación informativa». Se necesitan "estrategias holísticas":

- Plataformas transparentes que combatan la desinformación sin recurrir a la censura;
- Educación en el pensamiento crítico, para saber reconocer una fake news;
- Colaboración y legislación internacional, nuevas fronteras sobre las que es urgente actuar.

El papel de los jóvenes: custodios de un futuro "humano"

El acto concluyó con un llamamiento dirigido a los nativos digitales: «Somos la primera generación que puede utilizar la IA para amplificar el conocimiento, no para fragmentarlo». Ejemplos concretos no faltan: startups lideradas por menores de 30 años desarrollan herramientas para verificar fuentes periodísticas, mientras otros diseñan chatbots éticos que se niegan a generar discursos de odio.

El evento dejó mensajes sencillos pero urgentes: en una época en la que la IA puede hacer que lo falso resulte más convincente que lo verdadero, defender la verdad es una responsabilidad colectiva. La Ciber Diplomacia se revela esencial para mitigar los impactos político-económicos de consecuencias sociales potencialmente devastadoras.

Y los jóvenes, con su familiaridad tecnológica y su sensibilidad hacia los valores, están llamados a liderar esta silenciosa batalla, a dotarla de normas y a integrarla en la vida cotidiana. No con retóricas apocalípticas, sino con decisiones diarias y tecnológicamente responsables: compartir una noticia solo tras haberla verificado, exigir algoritmos transparentes, defender el conocimiento como un bien común.

Porque, como recuerda un proverbio reinterpretado en clave digital: La verdad es como el agua: siempre encuentra su camino. Pero hace falta alguien que limpie los márgenes.

Valerio Mercuri