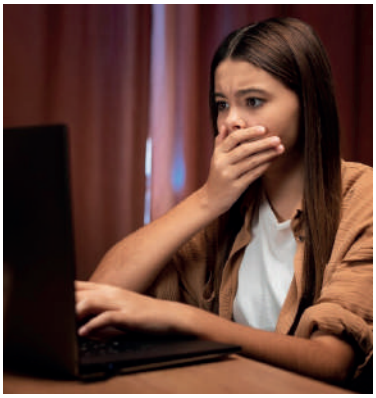
Core Business Corp.

Contramedidas ante Amenazas Cibernéticas

Resumen:

Este artículo aborda las contramedidas ante amenazas cibernéticas, destacando la evolución tecnológica y el incremento de ciberataques. A medida que la tecnología avanza, también lo hacen las amenazas, lo que requiere una constante actualización en las medidas de seguridad. Además, subraya la importancia de una estrategia de ciberseguridad integral que combine tecnología avanzada con una fuerza laboral.

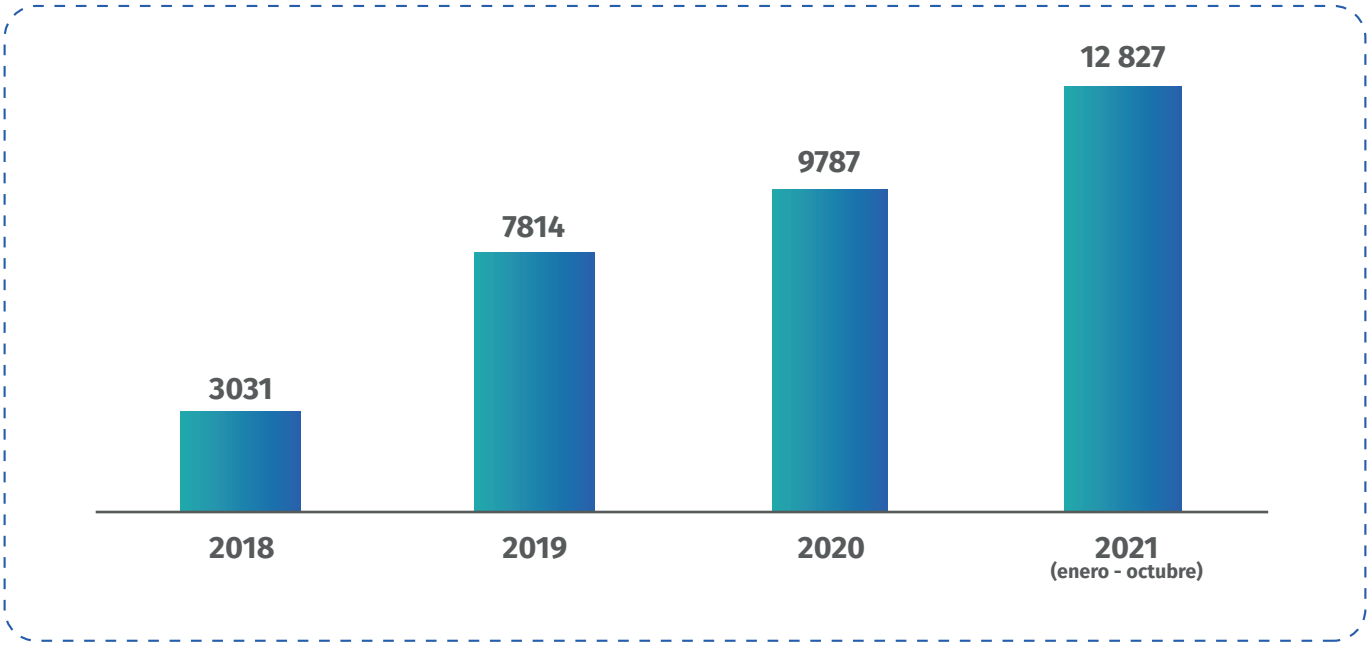
En la actualidad, la tecnología se desarrolla de forma continúa **mejorando incluso la calidad de vida de los seres humanos.** Por un lado, tenemos las versiones de software con mayor funcionalidad, **tecnología sostenible, IA Generativa, así como aplicaciones inteligentes que proporcionan conocimientos de gran alcance entre otros.** Asimismo, contamos con expertos y líderes los cuales mencionan que las organizaciones que adopten usos auténticos de la tecnología serán las que sobresalgan en la nueva era. (Top 5 de Tendencias Tecnológicas en 2024 | Globant Reports). Por otro lado, a medida que la tecnología se desarrolla e incrementan, tenemos la otra cara de la moneda, pues **los casos de denuncias por delitos informáticos o ciberataques ha aumentado.**



El **Ministerio Público del Perú** menciono lo siguiente:
"Cada vez se registran más denuncias por delitos informáticos en el país, en el 2021 recibieron 18 mil 596 denuncias de casos de cibercrimen, lo que representa un incremento porcentual de 92,9% en comparación con el 2020."

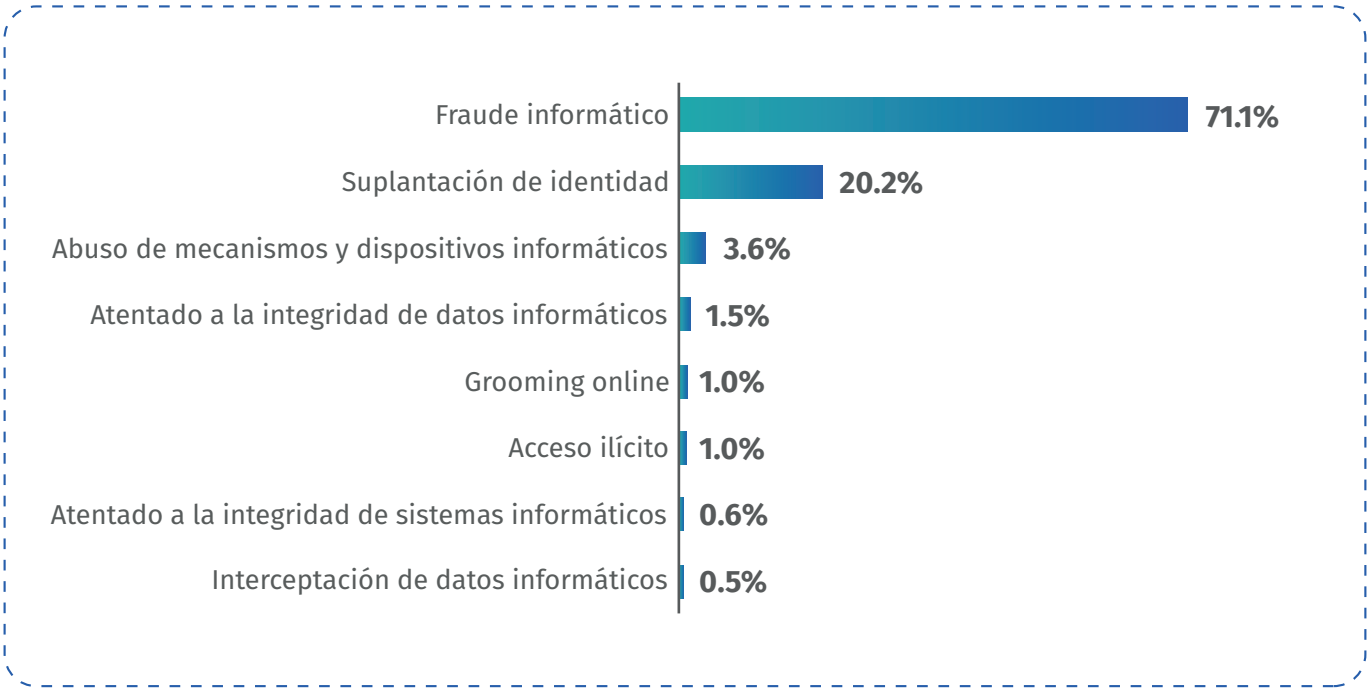
Asimismo, la **Defensoría del Pueblo**, en el informe defensorial L N° 001-2023-DP/ADHPD **detalla las siguientes cifras preocupantes sobre la ciberdelincuencia en el Perú:**

Denuncias de ciberdelitos ante la PNP (Perú, 2018-2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

Tipos de ciberdelitos denunciados ante la PNP (Perú, 2021)



Fuente: Sistema de Registro de Denuncias de Investigación Criminal PNP
Elaboración: Defensoría del Pueblo

Además, en el 2023 Fortinet menciona que se reportaron **200 millones intentos de ciberataques en América Latina,** siendo el **ransomware y malware uno de los principales ataques**. También, en el Informe de Fortiguard Labs de 2023 se menciona que existen menos cantidad de ataques, pero porque son diseñados para objetivos específicos, lo que los vuelve más sofisticados y con mayor posibilidad de éxito si las organizaciones **no cuentan con defensas de ciberseguridad** integradas, automatizadas y actualizadas. (Brodersen, 2024)

De todo lo mencionado anteriormente, se percibe que cada vez que se implementa un nuevo software de seguridad o existe un desarrollo de una nueva tecnología, ya existe un hacker que sabe cómo descifrarlo y conoce sus puntos más débiles. Por ello, l**as organizaciones deben ver la seguridad de la información como un proceso continuo que nunca termina.**

La Ciberseguridad (Cibersecurity) **es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.** Condición de estar protegido de forma física, social, financiera, política, emocional, ocupacional, psicológica, educacional entre otros tipos o consecuencias de fallas, daños, errores, accidentes o algún otro evento en el ciberespacio que se considere "no deseable".(¿Qué es la ciberseguridad?, 2023)}

Si hay algo por lo cual los profesionales de la ciberseguridad corporativa tienen mayor preocupación, es la idea de un **ataque que se valga de una amplia gama de técnicas avanzadas diseñadas para robar información valiosa de la organización.** Es por ello, que debemos conocer las implicancias y como nuestro enemigo actúa para protegernos de forma correcta.(¿Qué es una amenaza avanzada persistente (APT)?, 2023)

La detección y prevención de amenazas es un aspecto crítico de la protección de la ciberseguridad hoy en día. La importancia de **poder detectar factores de riesgo aumenta tan rápidamente como los malos actores adaptan sus metodologías de ataque.** Una estrategia sólida de detectar amenazas tendrá la capacidad de detener un ataque antes de que se convierta en una brecha. Esto es esencial para minimizar los daños y las pérdidas financieras tanto como para la organización como para los clientes. Pero antes de empezar a explicar los métodos, vamos a ver los tipos de amenazas que existen:

Tabla 1: Tipos de amenazas

Amenaza	¿Qué busca?	Impacto al negocio
Agencias de inteligencia	Comercialización de secretos políticos, comerciales y/o de defensa.	Pérdida de secretos comerciales y/0 de ventaja competitiva.
Grupos criminales	Transferencias de dinero, oportunidades de extorsión, información personal y/o cualquier secreto con potencial de venta.	Pérdidas financieras, divulgación no autorizada de datos de clientes (a gran escala) y/o pérdida de secretos comerciales.
Grupos activistas	Información confidencial y/o "disrupción" de servicios.	Divulgación no autorizada de datos y/o pérdida de servicios.

Ahora veremos los niveles de **contramedidas de seguridad** a tomas en cuenta ante las amenazas mencionadas (de forma enunciativa más no limitativa):

1. Medidas básicas de tecnología de seguridad:

Controles mínimos de seguridad para amenazas comunes, pero insuficientes para controlar APTs (amenaza avanzada persistente).

- **Antivirus:** Son sistemas de defensa, generalmente basados en software utilizados ampliamente para prevenir y remover malware. Pueden ser:
  - **Basados en firmas:** funcionamiento basado en patrones maliciosos conocidos.
  - **Basados en heurística:** funcionamiento basado en comportamiento asociado con malware.
- **Sistemas de Detección de Intrusos:** Hardware o software que monitorea constantemente el tráfico de red para identificar actividad maliciosa. El tráfico es examinado sobre patrones o heurística.
- **Firewalls:** Tecnología que ayuda al control de entrada o salida de tráfico de red analizando los paquetes y determinando si deben ser aceptados o rechazados, de acuerdo con un conjunto de reglas y políticas.

2. Medidas avanzadas de tecnología de seguridad:

Medidas más avanzadas (que las básicas). Refuerzan la seguridad haciendo imprácticos ciertos tipos de ataques.

- **Prevención de Intrusos:** Similares a los IDS, permiten monitorear las actividades de los sistemas y las redes, en búsqueda de actividad maliciosa. También están diseñados para bloquear intrusiones (aunque esto puede ser materia de "falsos positivos").
- **Prevención de Fugas de Datos (DLP):** Tecnología diseñada para detectar y bloquear fugas de datos (potenciales). Funciona en tres niveles: AT REST (almacenamiento), Inmotion (comunicaciones), y Endpoint (en equipos de usuarios).
- **Escaneo de vulnerabilidades:** Software diseñado para evaluar dispositivos de distintas capas tecnológicas (aplicaciones, bases de datos, plataformas y equipos de red) con el propósito de identificar debilidades y/o fallas conocidas.
- **Simulación de Sandbox:** Es un "ambiente seguro" donde puede ser ejecutado código malicioso para estudiar su comportamiento antes de permitirle entrar en la infraestructura de la organización (si acaso). Tiene alcance sobre archivos, ejecutables y/o correo electrónico (como el caso de las cámaras de detonación / detonation chambers).

3. Contramedidas específicas de APTs:

Controles que han demostrado ser útiles para la detección / prevención de APTs.

- **Inspección profunda de paquetes:** (Deep Packet –inspection – DPI) es una tecnología que inspecciona el contenido de tráfico entrante / saliente de red, contra criterios predefinidos en busca de software malicioso, intentos de intrusión y/o contenido no deseado. Tienen capacidad de reportar, redirigir o bloquear comunicaciones.
- **Correspondencia de patrones de comunicaciones:** Una vulnerabilidad de las APTs es que utilizan firmas identificables para sus comunicaciones (por ejemplo, cuando envían mensajes a su servidor central de control y comando), por el uso de protocolos, direcciones o encabezados.
- **Monitoreo de integridad de archivos:** Como una forma de extensión del control anterior, se trata de monitorear elementos de configuración (servidores, bases de datos, dispositivos, respaldo, entre otros) para identificar cambios no autorizados. Tecnologías emergentes tienen la capacidad de monitorear constantemente las

plataformas para obteniendo información a modo de indicadores sobre la presencia de APTs. Incrementan notablemente la posibilidad de detectar y responder (en tiempo real) ante una intrusión.

Administración de eventos de seguridad de la información (SIEM): Tecnología que habilita el análisis y administración de alarmas generadas por distintos sistemas de información. Tiene capacidades de monitoreo, correlación de eventos, y centralizan la recolección, almacenamiento y análisis de archivos con los datos de estos eventos. Son base de controles tales como SOC (Security Operations Center) y CSIRT (Computer Security Information Response Team).

Para maximizar las posibilidades de una defensa continua exitosa, se debe implementar una combinación de varias medidas, que van desde soluciones de seguridad avanzadas como las que se han detallado, hasta una fuerza de trabajo capacitada y con conocimiento en técnicas de ingeniería social, no solo basta contar con una buena herramienta de protección sino tenemos sensibilizados a los colaboradores de la organización.

Está en nuestras manos hacer frente al mundo actual, contando con expertos que den **soporte** a los controles, así como manteniendo una **adecuada gestión** que permita cumplir con los objetivos de la organización, **cuidando y protegiendo los datos** confidenciales **evitando un robo de información** que generaría graves pérdidas.

Referencias:

Brodersen, J. (2024, marzo 27). Fortinet: Detectan un 80% menos de intentos de ciberataques en 2023 pero “más sofisticados y con nuevas variantes”. Clarín. Recuperado de: https://www.clarin.com/tecnologia/fortinet-detectan-80-intentos-ciberataques-2023-sofisticados-nuevas-variantes_0_o8Rohha887.html

Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. (s. f.). Recuperado 19 de abril de 2024, de https://elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru

¿Qué es la ciberseguridad? (2023, diciembre 13). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

¿Qué es una amenaza avanzada persistente (APT)? (2023, abril 19). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Top 5 de Tendencias Tecnológicas en 2024 | Globant Reports. (s. f.). Reports. Recuperado 22 de abril de 2024, de https://reports.globant.com/es/trends/tendencias-tecnologicas-2024/

Lucero Arana Walde
Consultora SST
larana@corebusinesscorp.com

Core Business Corp.