Ciberseguridad – Cyber Diagnosis

Sabía que:

- De acuerdo con el informe semestral del panorama global de amenazas de FortiGuard Labs, Perú recibió 15 mil millones de intentos de ciberataques en 2022, lo que representa un aumento del 35% con respecto a 2021. Esto coloca a Perú en el cuarto lugar de los países con mayor número de intentos de ciberataques en América Latina, después de México (187 mil millones), Brasil (103 mil millones) y Colombia (20 mil millones).
- Los tipos de ciberataques más comunes en Perú fueron el phishing, el malware y los ataques de denegación de servicio (DoS).
    - El **phishing** es un tipo de ataque cibernético en el que los atacantes intentan engañar a las víctimas para que compartan información confidencial, como contraseñas o números de tarjetas de crédito.
    - El **malware** es un software malicioso que puede dañar o interrumpir sistemas informáticos.
    - Los **ataques de DoS** intentan saturar un sistema informático con tráfico de red para que no pueda atender a los usuarios legítimos.

Los ciberataques pueden tener un impacto significativo en las personas, las empresas y las sociedades. Pueden causar pérdidas financieras, daños a la reputación y la interrupción de los servicios.

Dependiendo del **objetivo del cibercriminal**, de su **modus operandi** y de las **herramientas que utilice**, estas son las principales causas o motivos del ciberataque:

1. Filtración de contraseñas en la **Dark Web** (obtenidas mediante fuerza bruta o **phishing**)
2. Pérdida de información o secuestro de datos y dispositivos (**ransomware**)
3. Modificación de la información existente
4. **Suplantación de identidad**, secuestro de cuentas de usuario o **cuentas bancarias**
5. Robo de dinero, **blanqueo de capitales** o **financiación del terrorismo**
6. Espionaje industrial o **inteligencia competitiva**
7. Denegación de servicio
8. Instalación de programas no deseados (**malware** del tipo spyware, **keyloggers**, **virus**, adware, bundleware, junkware,..)
9. **Monitorización** de la conexión y control del dispositivo, **obtención de nuestra huella digital**, etc.

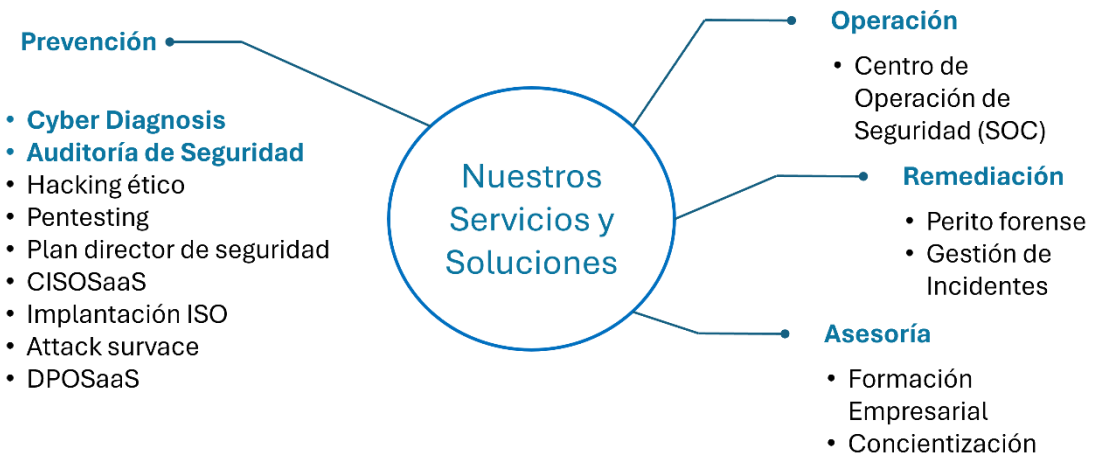
Ciberseguridad – Cyber Diagnosis

KONFIDI TECHNOLOGIES S.A., brinda los siguiente Servicios y Soluciones:

Por dónde empezar?

Recomendamos:

Iniciar un **Diagnóstico** de los puntos vulnerables de seguridad informática y de la información. Nosotros lo combinamos con una metodología objetiva y **NO Intrusiva** y otra Subjetiva basado en un cuestionario.



En qué consiste el servicio:

Hacking pasivo (Análisis y exposición del DNS de la empresa)	Cuestionario (122 preguntas en 10 Categorías)
A partir de un **empleo de técnicas de hacking pasivo**, **visualizamos** el **grado** de **exposición de la compañía**. Este estudio nos brindará **la posición de defensa** que actualmente se posee ante posibles ataques de seguridad. Realizamos un diagnóstico de todos los **posibles puntos vulnerables** de seguridad informática de la empresa. Analizando: • **Redes Sociales** • **Darkweb** (web oscura, su accesibilidad es limitada) • **Cualquier información pública** por medio de un escaneo pasivo.	**Cuestionario que se hace a personal con perfil de CEO, CTO, DPO, Legal y RRHH que permite tener un resultado rápido** y accesible sobre el nivel de vulnerabilidad, en aspectos básicos como la seguridad lógica, física, el cumplimiento normativo y la continuidad del negocio. Nuestra **herramienta** está diseñada siguiendo las **normativas y recomendaciones** vigentes en materia de **seguridad de la información** a lo que unimos nuestra **experiencia como expertos en ciberseguridad**. A través de un **cuestionario** estructurado en **10 categorías**, realizaremos una **valoración integral** de la **seguridad de su empresa**.

Los Entregables:

- Informe donde se describen, evidencian, evalúan y clasifican los hallazgos
- Valoración cuantitativa por áreas específicas
  - ✓ Seguridad Lógica
  - ✓ Seguridad Física
  - ✓ Movilidad
  - ✓ Protección de Datos
  - ✓ Continuidad del Negocios
- Costo estimado de una brecha para la organización en función de datos robados y horas de inactividad
- Relación de las vulnerabilidades halladas en la huella digital de la empresa

Recuerda, en función del tipo de ciberataque y de la víctima, estas son las repercusiones más habituales:

- Perjuicio económico
- Pérdida de tiempo
- Pérdida de información
- Pérdida de confianza en la información
- Reducción de la productividad
- Crisis reputacional personal o empresarial
- Disminución de la confianza de clientes y otros usuarios
- Posibles repercusiones legales

¡¡¡NO SEAS PARTE DE LAS ESTADÍSTICAS, CONTACTANOS!!!