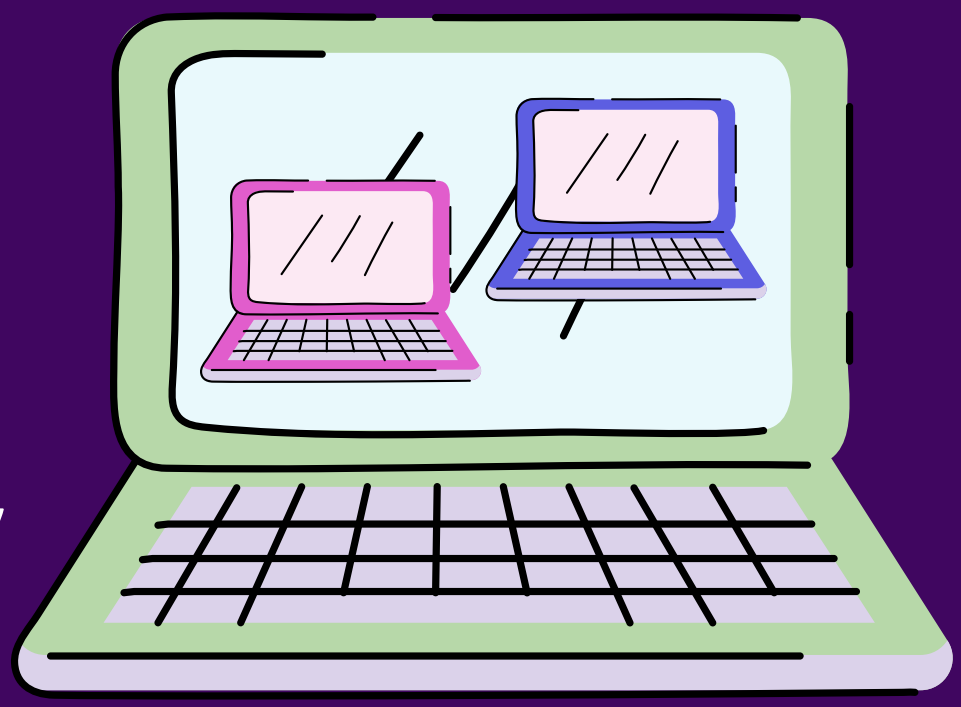
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Máquina virtual (virtual machine o VM): Recurso que se comporta como un computador tradicional, pero no cuenta con su propio hardware, existiendo solo como código. Así, se pueden tener varias VM (llamadas "guests") en una misma máquina física (o "host"), usando, por ejemplo, distintos sistemas operativos.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Command and Control (C&C): El equipo de un ciberdelincuente que controla a otros distancia de forma no autorizada. Desde estos servidores C&C, los atacantes pueden ejecutar acciones en los equipos de sus víctimas, como robar información confidencial, incluso manejar una red de equipos infectados (conocida como botnet).

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

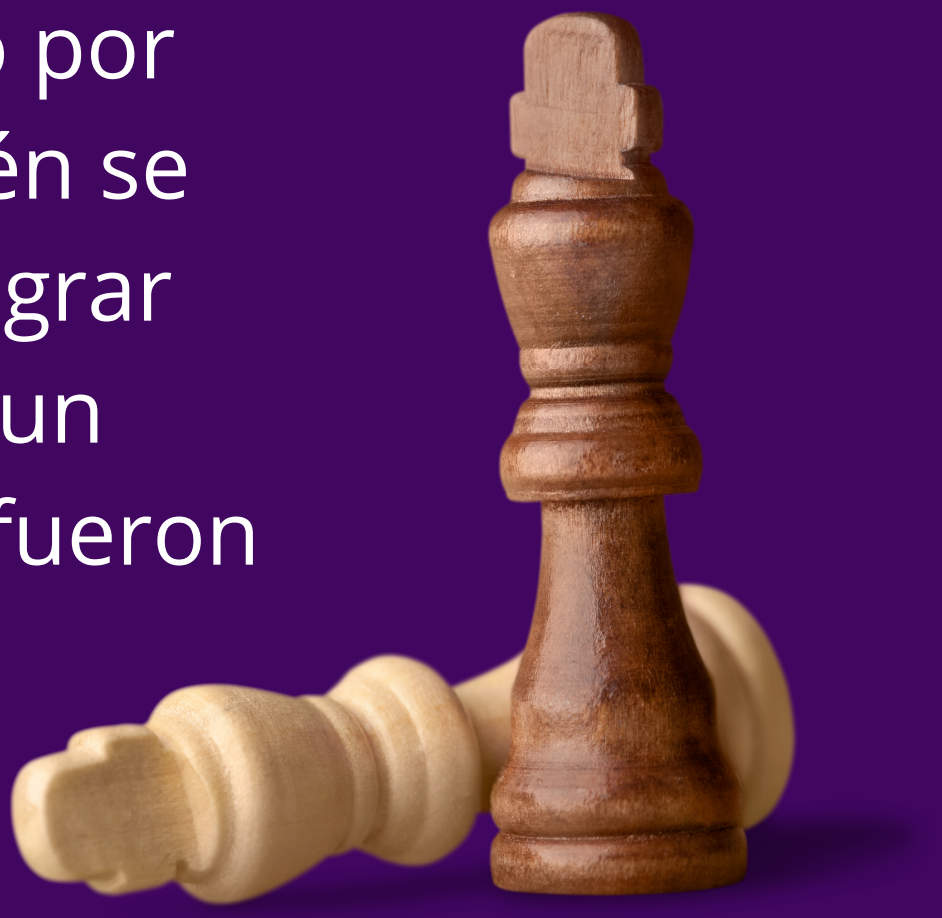
Ciber diccionario

Indicadores de compromiso (IoC): En ciberseguridad, se les llama así a indicios de un acceso no autorizado a un sistema, como pueden ser códigos específicos o actividades sospechosas. Si una entidad sufre un ataque, es útil que comparta con la comunidad los IoC que logra obtener, para así facilitar que otras organizaciones mejoren sus defensas.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

"pwn": Concepto proveniente del mundo de los videojuegos, se usa como verbo para describir cuando alguien es absolutamente derrotado o engañado. Viene de "owned", en inglés, ser dominado por alguien más. Así, también se usa informalmente al lograr acceso no autorizado a un sistema (cuyos dueños fueron "pwnd" o "pwn3d" por el atacante).



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

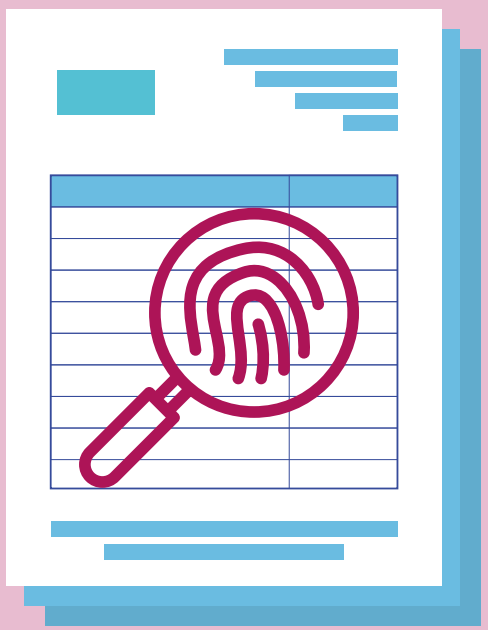
Ciber diccionario

Incidente: Es cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los activos de información de una organización. Puede incluir diversas situaciones, como el acceso (o intento de acceso) no autorizado a un equipo o una red, la filtración o destrucción de datos, el malware, el phishing y los ataques de denegación de servicio.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Indicadores de Compromiso (IoC): Son los rastros que deja un incidente de seguridad, que permiten saber cómo operó y conocer sus características para ayudar a prevenir un nuevo ataque. Su descripción sigue estándares, lo que facilita que sean aplicados por más instituciones, y puedan así prepararse.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Archivo ejecutable: Archivos que contienen instrucciones para el computador, como la descarga e instalación de software. Hacer clic en ellos sin conocer su procedencia es riesgoso: hay delincuentes que envían emails con ejecutables, y mensajes que convencen a su víctima de iniciarlos, resultando en su infección con software malicioso.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Vulnerabilidad: Debilidad de un programa informático que puede ser explotada por ciberdelincuentes. Por eso debemos mantener actualizados nuestros sistemas, ya que en estas actualizaciones se incluyen parches de seguridad para contrarrestar nuevas vulnerabilidades descubiertas.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

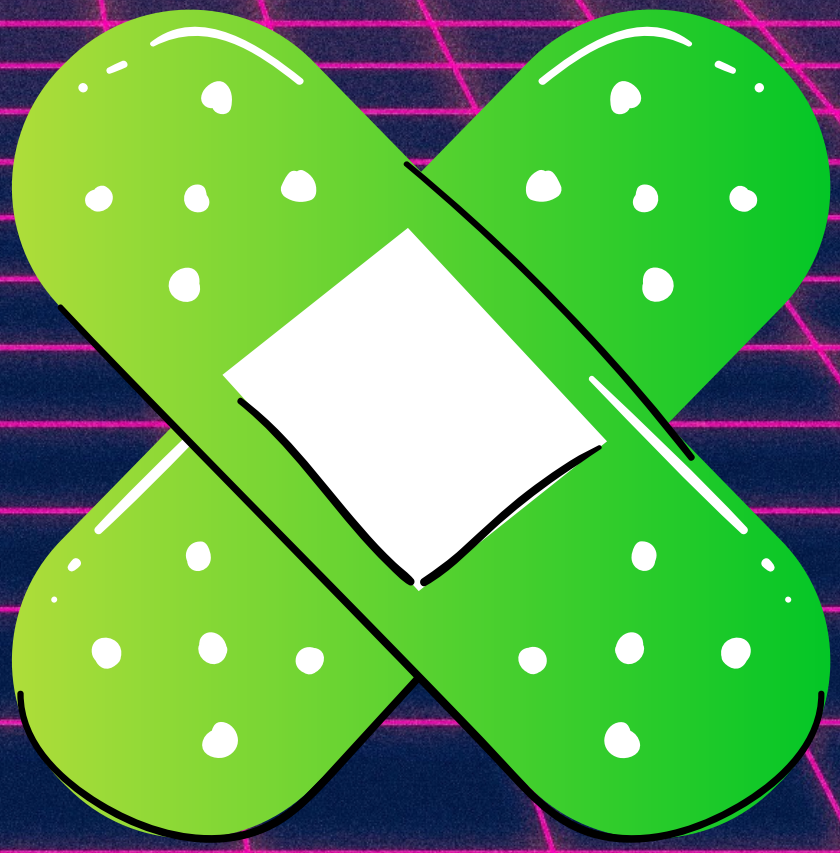
Ciber diccionario

Ghosting: Dejar de comunicarse con una persona, especialmente en aplicaciones de mensajería, sin previo aviso ni explicación, desapareciendo "como un fantasma" (de ahí el nombre). Puede constituir abuso emocional, por lo que debe evitarse.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Parche de seguridad: Actualización que publica el proveedor de software para solucionar un error de seguridad que afecta a alguno de sus programas. Son muy importantes, por lo que siempre debemos mantener nuestros sistemas actualizados.



CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Mitigación de seguridad:
Instrucciones que debe seguir un encargado de ciberseguridad para reducir los efectos de una vulnerabilidad. Esto, a la espera de que el proveedor de software entregue un parche que solucione la vulnerabilidad de forma definitiva.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Ciber diccionario

Doxing o doxxing: Mala prácitca (y potencial delito) que sucede principalmente en las redes sociales. Consiste en revelar datos personales de alguien sin su consentimiento para perjudicarlo, pudiendo poner en riesgo su trabajo e incluso su integridad física y la de sus seres queridos.