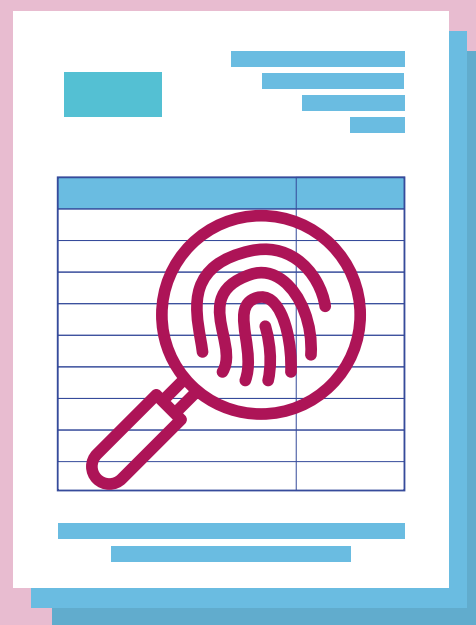


Incidente: Es cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los activos de información de una organización. Puede incluir diversas situaciones, como el acceso (o intento de acceso) no autorizado a un equipo o una red, la filtración o destrucción de datos, el malware,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



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.



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.

