

Definiciones Seguridad de la Información

Seguridad de la Información

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: daniel.olarte01@correo.usa.edu.co

Escuela de Ciencias Exactas e Ingeniería

Profesor:

03/02/2023

DEFINICIONES:

1. Evento de seguridad: es una ocurrencia relacionada con la seguridad de la información, puede ser tanto positiva como negativa. que puede incluir la detección de intrusiones o ataques a sistemas, la activación de alarmas de seguridad, la aparición de una amenaza conocida, entre otros. Ejemplo: La detección de una actividad maliciosa en la red de una empresa. Ejemplo: un cambio de configuración en un sistema de seguridad.
2. Incidente de seguridad: es un evento de seguridad negativo que afecta la integridad, disponibilidad o confidencialidad de la información. Ejemplo: un ataque cibernético a una red de computadoras. Ejemplo: Un ataque de ransomware que cifra los archivos de una empresa y exige un rescate a cambio de la clave de descifrado.
3. Amenaza de seguridad: es un agente externo, circunstancia o posible causante que podría causar un incidente de seguridad. Ejemplo: un virus de computadora o un hacker. Ejemplo: Una vulnerabilidad conocida en un sistema operativo que podría ser explotada por un atacante.
4. Vulnerabilidad en la informática: es un punto débil en un sistema o aplicación que puede ser explotado por un atacante para acceder a información confidencial o causar daños o un incidente de seguridad. Ejemplo: una puerta trasera en un software. Ejemplo: Una vulnerabilidad en un software de

navegación web que permite ejecutar código malicioso en el sistema del usuario.

5. Riesgo informático: es la probabilidad de que un incidente de seguridad ocurra y cause daño a una organización con gravedad de las consecuencias. Ejemplo: el riesgo de un ataque de phishing a los usuarios de una organización.
Ejemplo: El riesgo de una brecha de datos por un ataque phishing a empleados de una empresa.
6. Contramedidas en informática: son medidas implementadas para mitigar o prevenir los riesgos informáticos. Ejemplo: la implementación de un software antivirus o la formación sobre seguridad para los usuarios finales. Ejemplo: La implementación de contraseñas seguras y autenticación de dos factores para proteger los accesos a sistemas críticos.