Introducción a la Ciberseguridad

1) Amenazas y Adversidades:

- **Definición:** Las amenazas son eventos o acciones que pueden poner en peligro los activos de información. Las adversidades son las condiciones o circunstancias que pueden aumentar la probabilidad de que una amenaza se concrete.
- **Ejemplos:**
  - **Amenaza:** Un hacker que intenta acceder a una red informática.
  - **Adversidad:** Falta de personal capacitado en seguridad informática.

2) Vulnerabilidades y Gestión del Riesgo:

- **Definición:** Las vulnerabilidades son debilidades en los sistemas informáticos que pueden ser explotadas por las amenazas. La gestión del riesgo es el proceso de identificar, evaluar y mitigar los riesgos de seguridad.
- **Ejemplos:**
  - **Vulnerabilidad:** Un software desactualizado con una vulnerabilidad conocida.
  - **Gestión del riesgo:** Implementar un programa de actualización de software.

3) Ataques Comunes. Evaluación Básica de Riesgos:

- **Definición:** Los ataques comunes son las formas más utilizadas por los hackers para explotar las vulnerabilidades. La evaluación básica de riesgos es el proceso de identificar los activos de información, las amenazas y las vulnerabilidades para determinar el riesgo de un ataque.
- **Ejemplos:**
  - **Ataque común:** Ataque de phishing.
  - **Evaluación básica de riesgos:** Identificar los activos de información críticos y las amenazas que los pueden afectar.

4) Ciclo de Vida de la Seguridad:

- **Definición:** El ciclo de vida de la seguridad es un marco de trabajo para gestionar la seguridad de los sistemas informáticos a lo largo de su ciclo de vida.
- **Etapas:**
  - **Inicio:** Identificar los requisitos de seguridad.
  - **Desarrollo:** Implementar los controles de seguridad.
  - **Operación:** Monitorear y mantener los controles de seguridad.
  - **Eliminación:** Destruir los datos de forma segura al final de la vida útil del sistema.

5) Aplicaciones de Criptografía y PKI:

- **Definición:** La criptografía es la ciencia de convertir información en un código secreto para protegerla. La PKI (Infraestructura de Clave Pública) es un sistema que permite la autenticación y el cifrado de datos.
- **Ejemplos:**
  - **Criptografía:** Usar un algoritmo de cifrado para proteger los datos de una tarjeta de crédito.
  - **PKI:** Usar un certificado digital para verificar la identidad de un sitio web.

6) Seguridad de Datos:

- **Definición:** La seguridad de datos es la práctica de proteger los datos de accesos no

autorizados, uso indebido, divulgación, alteración o destrucción.

- **Ejemplos:**
  - **Respaldo de datos:** Hacer copias de seguridad de los datos de forma regular.
  - **Control de acceso:** Limitar el acceso a los datos a las personas que lo necesitan.

7) Modelos de Seguridad:

- **Definición:** Los modelos de seguridad son marcos de trabajo que describen cómo se debe proteger la información.
- **Ejemplos:**
  - **Modelo de seguridad perimetral:** Proteger la información creando un perímetro de seguridad alrededor de los activos.
  - **Modelo de seguridad de confianza cero:** No confiar en ningún dispositivo o usuario por defecto y verificar su identidad antes de conceder acceso.

8) Modelos de Control de Acceso:

- **Definición:** Los modelos de control de acceso son mecanismos que permiten determinar quién puede acceder a qué recursos.
- **Ejemplos:**
  - **Control de acceso discrecional (DAC):** Permitir o denegar el acceso a los recursos en función de la identidad del usuario.
  - **Control de acceso obligatorio (MAC):** Permitir o denegar el acceso a los recursos en función de las etiquetas de seguridad de los usuarios y los recursos.

9) Conceptos Básicos de Seguridad:

- **Confidencialidad:** Asegurar que solo las personas autorizadas puedan acceder a la información.
- **Integridad:** Asegurar que la información no sea modificada sin autorización.
- **Disponibilidad:** Asegurar que la información esté disponible cuando se la necesita.
- **Acceso:** Permitir que solo las personas autorizadas puedan acceder a la información.
- **Autenticación:** Verificar la identidad de un usuario.
- **Autorización:** Determinar qué recursos puede acceder un usuario.
- **No repudio:** Asegurar que no se pueda negar una transacción o comunicación.
- **Privacidad:** Proteger la información personal de los usuarios.

Resumen:

Las amenazas y adversidades aprovechan las vulnerabilidades para realizar ataques. La gestión del riesgo ayuda a identificar y mitigar estos riesgos. El ciclo de vida de la seguridad define las etapas para proteger los sistemas informáticos.

Las aplicaciones de criptografía y PKI se utilizan para proteger la confidencialidad e integridad de la información. La seguridad de datos se enfoca en la protección de la información en sí misma. Los modelos de seguridad y control de acceso definen quién puede acceder a qué recursos. Las propiedades de la seguridad establecen los requisitos básicos para un sistema seguro.