SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Gilbert Gonzalez
21-SISN-5-006

Anderson García
21-SISN-5-015

Luis Felipe Quirox
20-EISN-5-002

TEMAS A TRATAR

- 8.1 VULNERABILIDAD Y ABUSO DE LOS SISTEMAS.
- 8.2 VALOR DE NEGOCIOS DE LA SEGURIDAD Y EL CONTROL.
- 8.3 ESTABLECIMIENTO DE UN MARCO DE TRABAJO PARA LA SEGURIDAD Y EL CONTROL.
- 8.4 TECNOLOGÍAS Y HERRAMIENTAS PARA PROTEGER LOS RECURSOS DE INFORMACIÓN.
- 8.5 PROYECTOS PRÁCTICOS.

8.1 VULNERABILIDAD Y ABUSO DE LOS SISTEMAS

- **Importancia de la Seguridad en Sistemas de Información:**

1- **Crucial para cualquier negocio.**

2- Protección inadecuada puede deshabilitar sistemas y poner en riesgo la operación y la información confidencial.

- **Elementos de la Seguridad:**

1- Políticas.
2- Procedimientos.
3- Medidas técnicas.

- **Objetivos de la Seguridad:**

1- Prevenir acceso no autorizado.
2- Prevenir daño a los sistemas de información.
Reforzar la seguridad de los activos organizacionales.
3- Asegurar la precisión de los registros.
4- Asegurar adherencia a los estándares gerenciales.

¿POR QUÉ SON VULNERABLES LOS SISTEMAS?

1- Almacenamiento de Grandes Cantidades de Datos Electrónicos:

Amplía el potencial de acceso no autorizado, abuso o fraude.

2- Interconexión a través de Redes de Comunicación:

Aumenta la exposición a vulnerabilidades.

3- Vulnerabilidades en Cualquier Punto de la Red:

Factores técnicos, organizacionales y ambientales pueden causar fallos.

4- Susceptibilidad en Todas las Capas del Entorno Cliente/Servidor:

Desde errores de usuario hasta la intercepción de datos en transmisión.

SOFTWARE MALICIOSO: VIRUS, GUSANOS, CABALLOS DE TROYA Y SPYWARE

1. Virus:
- Se adjuntan a programas o archivos.
- Se propagan mediante acciones del usuario, como enviar correos electrónicos infectados.

2. Gusanos:
- Programas independientes.
- Se replican y se propagan rápidamente por redes sin intervención humana.

3. Caballos de Troya:
- Parecen inofensivos pero realizan acciones dañinas al ejecutarse.

4. Spyware:
- Monitorea la actividad del usuario sin su conocimiento.

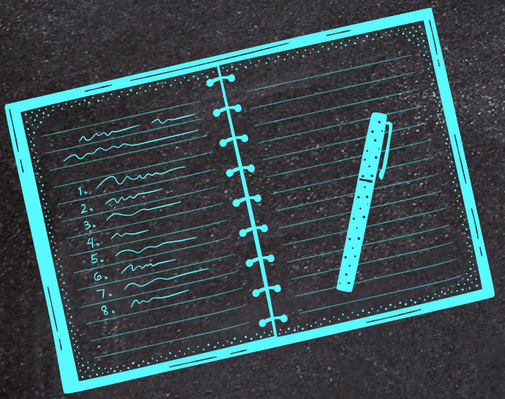
LOS HACKERS Y LOS DELITOS COMPUTACIONALES

1. Acceso Ilegal:
- Hackers acceden ilegalmente a sistemas para robar o destruir información.

2. Técnicas de Hacking:
- Uso de puntos de acceso falsos para capturar credenciales de usuario.

3. Protección Efectiva:
- Requiere estándares de seguridad robustos como WPA2 en redes Wi-Fi.
- WEP es menos seguro y no recomendado.

AMENAZAS INTERNAS: LOS EMPLEADOS



- **Amenaza Interna Significativa:**

Los empleados pueden comprometer la seguridad de los sistemas.

- **Daños Intencionados o por Descuido:**

Pueden causar daños de manera intencionada o por error.

- **Compromiso de la Integridad y Seguridad de la Información:**

La integridad y seguridad de la información pueden verse afectadas.

- **Medidas de Mitigación:**

Vigilancia de la actividad de los empleados.
Implementación de políticas de seguridad.

VULNERABILIDAD DEL SOFTWARE

- El software puede tener vulnerabilidades que son explotadas por atacantes para comprometer los sistemas de información. Los errores de programación, las configuraciones incorrectas y la falta de actualizaciones de seguridad son factores que contribuyen a estas vulnerabilidades. Es crucial mantener el software actualizado y aplicar parches de seguridad regularmente para proteger los sistemas .

8.2 VALOR DE NEGOCIOS DE LA SEGURIDAD Y EL CONTROL

INVERSIÓN EN SEGURIDAD:

- Las empresas no invierten mucho en seguridad porque no genera ingresos directos.
- La falta de inversión puede resultar en pérdidas mayores, como la pérdida de información confidencial, activos, confianza pública y credibilidad.

CONSECUENCIAS DE UNA SEGURIDAD INADECUADA:

- Empresas enfrentan problemas legales por permitir la pérdida o robo de datos de clientes.
- Una buena seguridad y control mejoran la eficiencia del trabajo y reducen costos operativos.

REQUISITOS LEGALES EN EE.UU.:

- Las empresas deben proteger datos contra fugas, robos o accesos no autorizados.

Cumplimiento de leyes específicas según el sector:

- Sector Médico: Ley HIPAA (confidencialidad de datos de pacientes).
- Servicios Financieros: Ley Gramm-Leach-Bliley.
- Compañías Cotizadas en Bolsa: Ley Sarbanes-Oxley.

IMPORTANCIA DE LA SEGURIDAD DE DATOS:

- Protección contra delitos como fraude en la bolsa, malversación de fondos, robo de secretos comerciales y delitos informáticos.
- Mayor parte de los datos y evidencias electrónicas están en formato digital, almacenadas tanto físicamente como en la nube.

8.3 ESTABLECIMIENTO DE UN MARCO DE TRABAJO PARA LA SEGURIDAD Y EL CONTROL

Aun con las mejores herramientas y técnicas es inútil si no se sabe cómo y donde implementarla, por eso se idean controles de los sistemas de información como controles que manipules desde la aplicación hasta la estructura de los datos usando hardware, software y procedimientos manuales para garantizar un entorno de control general, sin embargo, hay controles más específicos que se usan en cada aplicación independiente como nomina o procesamiento de pedidos separando los controles en tres partes:

1- Controles de entrada
2- Controles de procesamiento
3- Controles de salida

TAMBIÉN ESTÁN LOS CONTROLES GENERALES QUE SON:

1- Controles de software (Monitorean el uso del software de sistemas y previenen el acceso no autorizado)

2- Controles de hardware (Aseguran la seguridad del hardware y garantizan respaldo continuo)

3- Controles de operaciones de computadora (Supervisan los procedimientos para asegurarlos)

4- Controles de seguridad de datos (Protegen archivos valiosos contra acceso, modificación y destrucción)

5- Controles de implementación (Auditan el desarrollo de sistemas y aseguran un buen control y gestión)

6- Controles administrativos (Establecen estándares para asegurar la correcta ejecución de controles)

EVALUACIÓN DE RIESGO

Esta parte habla de evaluar que activos requieren más protección y a que grado, este tipo de evaluación nos dice el nivel de riesgo de cada activo, evaluando puntos como el valor de activo, sus puntos débiles, la frecuencia con la que ocurriría un evento comprometedor y la perdida que se tendría en caso de dicho evento. Para esta evaluación se pueden tomar tres puntos importantes de riesgo como lo son la probabilidad de ocurrencia, el rango de perdidas promedio y las pérdidas anuales esperadas.

POLÍTICA DE SEGURIDAD

Una vez sabiendo los riegos se deben crear políticas de seguridad para proteger los activos, las cuales controlan el uso de los recursos y quienes puede usar dichos recursos. Una de las políticas conocidas es la política de uso aceptable (AUP), esta política indica las responsabilidades con los datos y el uso de los equipos y esta define los usos inaceptables en la compañía. También está la administración de identidad consiste en los procesos de negocios y las herramientas de software para identificar a los usuarios válidos de un sistema, y para controlar su acceso a los recursos de este.

PLANIFICACIÓN DE RECUPERACIÓN DE DESASTRES Y PLANIFICACIÓN DE LA CONTINUIDAD DE NEGOCIOS

La recuperación de desastres y la continuidad de negocios son esenciales para continuar con los servicios y operaciones después de interrupciones. A continuación mencionare tres puntos fundamentales en este proceso:

1- Recuperación de desastres o recuperación de los activos físicos

2- Continuidad de negocios o restauración de las operaciones

3- Auditoría (Evalúa la efectividad de la seguridad y los controles de sistemas de información)

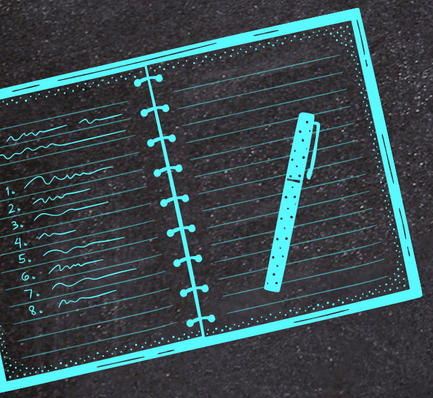
ADMINISTRACIÓN DE LA IDENTIDAD Y LA AUTENTICACIÓN

Administración de la Identidad:

- Las grandes y medianas empresas emplean software especializado para gestionar las identidades digitales de los usuarios.
- Cada usuario registrado recibe una identidad digital única que se asocia con sus privilegios y accesos dentro de la organización.

Autenticación:

- **Contraseñas:** La forma más común de autenticación, aunque a menudo insuficiente debido a vulnerabilidades.
- **Autenticación Avanzada:** Incluye el uso de tecnologías como tokens, tarjetas inteligentes y métodos biométricos.



Tecnologías de Autenticación Avanzadas:

- **Tokens:** Dispositivos físicos o digitales que generan códigos únicos de un solo uso para verificar la identidad del usuario.
- **Tarjetas Inteligentes:** Tarjetas con microchips que almacenan información y proporcionan un método seguro de autenticación.
- **Autenticación Biométrica:** Verifica la identidad basándose en características físicas únicas del usuario, tales como:

- **Huellas Digitales:** Escaneo de huellas para confirmar la identidad.
- **Iris:** Escaneo del patrón del iris del ojo.
- **Voz:** Reconocimiento de la voz del usuario.

FIREWALLS, SISTEMAS DE DETECCIÓN DE INTRUSOS Y SOFTWARE ANTIVIRUS

Firewalls:

- Tipos:
  - Firewalls de Red: Protegen redes enteras, generalmente a nivel de hardware.
  - Firewalls de Host: Protegen computadoras individuales, típicamente a nivel de software.
- Funciones:
  - Bloquean tráfico malicioso.
  - Controlan el acceso a la red.
  - Monitorean y registran intentos de conexión.

Sistemas de Detección de Intrusos (IDS):

- Tipos:
  - IDS Basado en Red (NIDS): Monitorea todo el tráfico de red en tiempo real.
  - IDS Basado en Host (HIDS): Monitorea las actividades de un solo equipo o dispositivo.
- Funciones:
  - Detectan ataques de red, como escaneos de puertos y vulnerabilidades.
  - Generan alertas cuando se detectan actividades sospechosas.
  - Ayudan en la respuesta a incidentes al proporcionar información detallada sobre las amenazas detectadas.

Software Antivirus:

- Funciones:
  - Escaneo de archivos y programas en busca de malware.
  - Monitoreo en tiempo real para interceptar amenazas.
  - Actualización constante de las definiciones de virus para reconocer nuevas amenazas.
- Componentes Clave:
  - Motor de Escaneo: Analiza los archivos en busca de patrones de malware conocidos.
  - Base de Datos de Definiciones: Contiene las firmas y características de los malwares conocidos.
  - Módulo de Actualización: Permite la actualización automática de la base de datos y el motor de escaneo para mantenerse al día con nuevas amenazas.

ASPECTOS DE SEGURIDAD PARA LA COMPUTACIÓN EN LA NUBE Y LA PLATAFORMA DIGITAL MÓVIL

Computación en la Nube y sus desafíos:

- **Acceso no autorizado:** Riesgo de que actores malintencionados accedan a datos sensibles.
- **Fugas de datos:** Posibilidad de que los datos se filtren o sean expuestos accidentalmente.
- **Violaciones de privacidad:** Uso indebido de datos personales almacenados en la nube.
- **Amenazas internas:** Empleados o administradores con acceso privilegiado que puedan abusar de sus permisos.

Prácticas de Seguridad:

- **Cifrado de Datos:** Encriptar datos tanto en tránsito como en reposo para protegerlos contra accesos no autorizados.
- **Control de Acceso y Gestión de Identidad (IAM):** Implementar políticas estrictas de acceso y autenticar usuarios con métodos robustos como la autenticación multi factor (MFA).
- **Monitoreo y Auditoría:** Realizar un seguimiento continuo de las actividades y auditar el acceso a los datos para detectar y responder a actividades sospechosas.
- **Seguridad en las API:** Asegurar que las interfaces de programación de aplicaciones (API) estén protegidas contra vulnerabilidades.
- **Cumplimiento de Normativas:** Asegurarse de que los servicios en la nube cumplan con las normativas y regulaciones relevantes, como GDPR, HIPAA, etc.

Plataforma Digital Móvil y sus desafíos de seguridad:

- **Pérdida o Robo de Dispositivos:** Riesgo de que dispositivos móviles sean extraviados o robados, exponiendo datos sensibles.
- **Aplicaciones Maliciosas:** Apps fraudulentas que pueden robar información o comprometer la seguridad del dispositivo.
- **Conexiones No Seguras:** Uso de redes Wi-Fi públicas y no seguras que pueden ser explotadas por atacantes para interceptar datos.
- **Fragmentación del Sistema Operativo:** Diversidad de versiones de sistemas operativos que dificulta la implementación de medidas de seguridad uniformes.

Prácticas de Seguridad:

- **Cifrado de Datos:** Asegurar que los datos almacenados en dispositivos móviles estén cifrados para protegerlos en caso de pérdida o robo.
- **Gestión de Dispositivos Móviles (MDM):** Utilizar soluciones MDM para gestionar y asegurar dispositivos móviles, incluyendo la capacidad de borrar datos de forma remota.
- **Actualizaciones y Parches:** Mantener el sistema operativo y las aplicaciones móviles actualizadas con los últimos parches de seguridad.
- **Seguridad en Aplicaciones:** Desarrollar aplicaciones móviles con seguridad en mente, incluyendo prácticas como pruebas de penetración y auditorías de código.
- **Autenticación Fuerte:** Implementar autenticación multi factor (MFA) para acceder a dispositivos y aplicaciones móviles.

ASEGURAMIENTO DE LA CALIDAD DEL SOFTWARE (SQA)

Importancia: El SQA:

- Mejora la confiabilidad y desempeño del software: Al identificar y corregir problemas desde las etapas tempranas del desarrollo, se mejora la calidad general del producto.
- Reducción de costos: Detectar y solucionar problemas en etapas tempranas es más económico que hacerlo después de la implementación.
- Satisfacción del cliente: Un software de alta calidad cumple con las expectativas del cliente y reduce las quejas y devoluciones.
- Cumplimiento normativo: Muchas industrias tienen normativas estrictas que requieren prácticas de SQA para garantizar la seguridad y eficacia del software.

Elementos Clave del SQA:

1. **Planificación de la Calidad:**
   - Definir estándares de calidad y métricas.
   - Desarrollar un plan de calidad detallado que describa las actividades de aseguramiento de calidad, cronograma y responsabilidades.
2. **Control de Calidad:**
   - Actividades de verificación y validación para garantizar que el software cumpla con los requisitos especificados.
   - Pruebas unitarias, de integración, de sistema y de aceptación del usuario.
3. **Auditorías y Revisiones:**
   - Revisiones periódicas de código, diseño y requisitos para detectar y corregir problemas.
   - Auditorías de procesos para asegurar que se siguen los estándares y procedimientos establecidos.
4. **Gestión de la Configuración del Software:**
   - Controlar y rastrear los cambios en el software y sus componentes.
   - Asegurar que todas las versiones y modificaciones del software se gestionen de manera ordenada.
5. **Gestión de Riesgos:**
   - Identificar, evaluar y mitigar los riesgos asociados con el desarrollo del software.
   - Implementar planes de contingencia para enfrentar posibles problemas.
6. **Medición y Análisis:**
   - Recolectar y analizar datos sobre el desempeño del software y los procesos de desarrollo.
   - Utilizar métricas para evaluar la eficacia de las prácticas de calidad y hacer mejoras continuas.

Prácticas Comunes en SQA:

- Pruebas Automatizadas: Uso de herramientas automatizadas para realizar pruebas repetitivas y detectar defectos rápidamente.
- Integración Continua (CI): Integrar y probar código frecuentemente para identificar problemas temprano en el ciclo de desarrollo.
- Desarrollo Ágil: Adoptar metodologías ágiles que promuevan iteraciones cortas y retroalimentación constante para mejorar la calidad del software.
- Análisis Estático de Código: Utilizar herramientas para analizar el código sin ejecutarlo y detectar posibles defectos y vulnerabilidades.

MUCHAS GRACIAS