**Vulnerabilidad y abuso de los sistemas**

La seguridad en los sistemas de información es crucial para cualquier negocio. Si un sistema no está adecuadamente protegido, puede ser deshabilitado rápidamente, poniendo en riesgo la operación de la empresa y la seguridad de la información confidencial. La seguridad incluye políticas, procedimientos y medidas técnicas para prevenir el acceso no autorizado y el daño a los sistemas de información. Los controles refuerzan la seguridad de los activos organizacionales y aseguran la precisión de los registros y la adherencia a los estándares gerenciales.

**¿Por qué son vulnerables los sistemas?**

Los sistemas de información son vulnerables debido a la gran cantidad de datos almacenados electrónicamente y su interconexión a través de redes de comunicación. Esto amplía el potencial de acceso no autorizado, abuso o fraude. Las vulnerabilidades pueden presentarse en cualquier punto de la red y derivar de factores técnicos, organizacionales y ambientales. Cada capa del entorno de computación cliente/servidor es susceptible a daños, desde los usuarios que introducen errores hasta la intercepción de datos en transmisión.

**Software malicioso: virus, gusanos, caballos de Troya y spyware**

El software malicioso, o malware, incluye virus, gusanos, caballos de Troya y spyware. Los virus se adjuntan a otros programas o archivos y se propagan cuando los usuarios realizan acciones como enviar correos electrónicos con archivos adjuntos infectados. Los gusanos son programas independientes que se replican y se propagan rápidamente a través de redes, sin necesidad de intervención humana. Los caballos de Troya son programas que parecen inofensivos, pero realizan acciones dañinas al ejecutarse. El spyware monitorea la actividad del usuario sin su conocimiento.

**Los hackers y los delitos computacionales**

Los hackers pueden comprometer la seguridad de los sistemas de información al acceder ilegalmente a ellos, a menudo para robar o destruir información. Las técnicas de hacking incluyen el uso de puntos de acceso falsos para capturar credenciales de usuario. La protección efectiva contra estas amenazas requiere el uso de estándares de seguridad robustos como WPA2 en redes Wi-Fi, en lugar del menos seguro WEP.

**Amenazas internas: los empleados**

Los empleados representan una amenaza interna significativa para la seguridad de los sistemas de información. Pueden causar daños intencionadamente o por descuido, comprometiendo la integridad y seguridad de la información. La vigilancia de la actividad de los empleados y la implementación de políticas de seguridad son esenciales para mitigar estos riesgos.

**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

Aquí nos dice que las empresas no deciden invertir mucho en seguridad porque para ellos no representa un ingreso como tal, sin saber que las pérdidas de su información confidencial por una mala seguridad serian mucho peor y las pérdidas de todos los activos e información de la empresa no solo sería una perdida monetaria si no una pérdida de confianza en el público y de credibilidad.

Un control y seguridad inadecuados puede hacer que las empresas que permitieron o que no hicieron nada o no lo suficiente ante una fuga de datos podrían enfrentar problemas legales al permitir la pérdida o robo de los datos de sus clientes sin mencionar que una buena seguridad junto a un buen control de esta hace más eficiente el trabajo de los empleados y reduce los costos de las operaciones.

Debido a la seriedad del tema los estados unidos le exigen a las empresas que se comprometan y aseguren la protección de los datos contra cualquier fuga, robo o acceso sin autorización siguiendo el cumplimiento de varias leyes dependiendo del área donde se desempeñe la empresa, por ejemplo si es de servicios médicos esta la ley de Responsabilidad y Portabilidad de los Seguros Médicos (HIPAA) asegurando los procedimientos y las reglas adecuadas para este tipo de empresas y fundamentalmente la confidencialidad de los datos de los pacientes y de las transacciones con los proveedores al menos por 6 años la cual conlleva de penalizaciones si es violada. Si es de servicios financieros cumple con la ley de Modernización de Servicios Financieros o Ley Gramm-Leach-Bliley, si es una compañía de cotización de bolsa se debe cumplir con la ley de Reforma de Contabilidad Pública de Compañías y Protección al Inversionista o Ley Sarbanes-Oxley.

Por último, se debe mantener una seguridad, el control y la administración de los datos ante delitos como los fraude en la bolsa de valores, la malversación de fondos, el robo de secretos comerciales de la compañía, los delitos por computadora y muchos casos más, sabiendo que la mayor parte de los datos o de la evidencia electrónica se encuentra en formato digital en los diferentes medios de almacenamiento tanto físicos 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.

**Recuperación de desastres:** Esta se centra en aspectos técnicos como respaldar archivos y mantener sistemas de respaldo. Ejemplos de esto incluyen centros de cómputo duplicados, y servicios de recuperación de desastres proporcionados por empresas. Estos servicios les permitirán a las empresas ejecutar medidas críticas desde sitios alternativos en caso emergencias.

**Continuidad de negocios:** Aquí nos enfocamos en restaurar las operaciones de negocio tras un desastre. Identificando los procesos críticos y definiendo planes de acción para mantener funciones esenciales.

**Auditoría:** Evalúa la efectividad de la seguridad y los controles de sistemas de información. Esta incluye la revisión de tecnologías, procedimientos y personal, y puede simular ataques para medir la respuesta de la empresa. Las auditorías identifican debilidades, estiman la probabilidad de ocurrencia y evalúan el impacto financiero y organizacional, exigiendo que la gerencia desarrolle planes para abordar las debilidades encontradas.

**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:**

1. **Tokens:** Dispositivos físicos o digitales que generan códigos únicos de un solo uso para verificar la identidad del usuario.
2. **Tarjetas Inteligentes:** Tarjetas con microchips que almacenan información y proporcionan un método seguro de autenticación.
3. **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.

**Importancia:**

* La administración de identidades y autenticación asegura que solo las personas autorizadas puedan acceder a los recursos de información.
* Implementar tecnologías avanzadas de autenticación reduce significativamente el riesgo de accesos no autorizados y mejora la seguridad general de la información.

**Firewalls, Sistemas de Detección de Intrusos y Software Antivirus**

**Firewalls:**

* **Definición:** Dispositivos o programas que filtran el tráfico de red, permitiendo o denegando el paso basado en un conjunto de reglas predefinidas.
* **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):**

* **Definición:** Sistemas que monitorean el tráfico de red o actividades del sistema para detectar actividades sospechosas o maliciosas.
* **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:**

* **Definición:** Programas diseñados para detectar, prevenir y eliminar software malicioso (malware), como virus, troyanos, spyware y adware.
* **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.

**Importancia:**

* **Firewalls:** Actúan como la primera línea de defensa, bloqueando el acceso no autorizado y controlando el tráfico de red.
* **IDS:** Complementan a los firewalls al proporcionar una capa adicional de vigilancia y detección de amenazas dentro de la red.
* **Software Antivirus:** Protege los sistemas individuales contra una amplia gama de malware, asegurando que los dispositivos no se conviertan en puntos de entrada para atacantes.

**Aspectos de Seguridad para la Computación en la Nube y la Plataforma Digital Móvil**

**Computación en la Nube:**

* **Definición:** Provisión de servicios informáticos (servidores, almacenamiento, bases de datos, redes, software) a través de Internet ("la nube").
* **Desafíos de Seguridad:**
	+ **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 multifactor (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:**

* **Definición:** Dispositivos y aplicaciones móviles utilizados para acceder a servicios digitales y almacenar datos personales o corporativos.
* **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 multifactor (MFA) para acceder a dispositivos y aplicaciones móviles.

**Importancia:**

* **Computación en la Nube:** La adopción creciente de servicios en la nube por parte de empresas y usuarios individuales aumenta la necesidad de asegurar que los datos y aplicaciones en la nube estén protegidos contra amenazas externas e internas.
* **Plataforma Digital Móvil:** Con el incremento del uso de dispositivos móviles para tareas personales y profesionales, la seguridad de estos dispositivos es crucial para proteger datos sensibles y prevenir accesos no autorizados.

**Aseguramiento de la Calidad del Software (SQA)**

**Definición:** El Aseguramiento de la Calidad del Software (SQA) es un proceso sistemático para asegurar que el software desarrollado cumple con los requisitos y estándares de calidad establecidos. Involucra una serie de actividades y prácticas que se llevan a cabo durante todo el ciclo de vida del desarrollo del software para prevenir defectos y garantizar que el producto final sea fiable, funcional y seguro.

**Importancia:** El SQA es crucial porque:

* **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.
	* Hay que 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.