GESTIÓN DE SISTEMAS DE INFORMACIÓN

Unidad 4: Seguridad en los sistemas de Información

El término seguridad se refiere a las políticas, procedimientos y medidas técnicas que se toman para evitar el acceso no autorizado o la alteración, robos y daños físicos a los sistemas de información. Es posible promover la seguridad con una serie de técnicas y herramientas que protegen al hardware, el software, las redes de comunicaciones y los datos.

El objetivo de la seguridad informática es mantener la Integridad, Disponibilidad, Privacidad , Control y Autenticidad de la información manejada por sistemas de información.".

Objetivos de la seguridad informática:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Unidad 4: Tipos de Seguridad Informática

Seguridad del hardware: Protege los elementos físicos de cualquier daño, proporciona seguridad un poco más robusta por lo que es importante proteger los sistemas de alimentación ininterrumpida (SAI), los cortafuegos, entre otros.

Seguridad del software: Protege al software de amenazas que pueden ser producidas por un cracker u otras potenciales vulnerabilidades que ponen en peligro a los principios de la seguridad de la información como la confidencialidad, integridad y disponibilidad de los datos. En el software se pueden encontrar diversas formas de vulnerar, por ejemplo a partir de los errores de implementación, defectos presentes en la fase del diseño, por medio de un desbordamiento de buffer, la falta de seguridad en el código, mal manejo de errores, entre otros.

Seguridad de red: Permite la protección de los datos y la red por lo que evita que los datos puedan ser modificado o robados, para proteger la red es necesario contar con varios niveles de seguridad ya que si uno es vulnerado los demás siguen trabajando, entre los componentes de seguridad en una red hay las redes privadas virtuales (VPN), Sistemas de prevención de intrusos (IPS), cortafuegos, entre otros.

Unidad 4: Pilares de la Seguridad Informática

Confidencialidad: asegura que sólo el personal autorizado accede a la información que le corresponde,

a) Autenticación de usuarios.
b) Gestión de privilegios.
c) Cifrado de información.

Integridad: consiste en asegurarse que la información no se pierda ni este comprometida.

a) Monitorear la red para descubrir posibles intrusos.
b) Implementar políticas de auditorías a fin de auditar los sistemas.
c) Implementar sistemas de control de cambios.
d) Copias de seguridad que permitan respaldar la información.

Disponibilidad: permite que la información esté disponible para quien la necesita.

a) Balanceadores de tráfico que minimicen el impacto del DDoS.
b) Copias de seguridad
c) Sitio de contingencia (DRP)

Unidad 4: Seguridad de la Información

Para analizar la Seguridad Informática de un sistema se debe conocer las características de lo que se pretende proteger: ***la Información***

El valor de la información es algo relativo, en muchos casos, no se valora adecuadamente debido a su intangibilidad.

Información pública: puede ser visualizada por cualquier persona

Información privada: sólo puede ser visualizada por un grupo selecto de personas

La Información es:

- Es **Crítica**: es indispensable para garantizar la continuidad operativa.
- Es **Valiosa**: es un activo con valor en sí misma.
- Es **Sensitiva**: debe ser conocida por las personas que la procesan y sólo por ellas.

Unidad 4: Características de la Información

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado.

La **Disponibilidad** u **Operatividad** de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas.

La **Privacidad** o **Confidencialidad** de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas.

La **Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

El **Control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

Unidad 4: Tipos de Controles

- Controles generales
- Controles de implementación
- Controles de software
- Controles de hardware
- Controles de operaciones de computación
- Controles de seguridad de los datos
- Controles administrativos
  - segregación de funciones
  - políticas y procedimientos por escrito
  - supervisión
- Controles de aplicación
- Controles de entrada
- Controles de procesamiento
- Controles de salida

Unidad 4: Tipos de Mecanismos

Preventivos: implica que se implementen mecanismos que los usuarios no puedan anular siendo estos correctos e inalterables, de modo que un cracker o atacante no pueda cambiarlo. La mayoría de los ataques se pueden evitar o disminuir su impacto mediante la aplicación de estos mecanismos. Actualización del sistema, antivirus, corta fuegos, contraseñas, navegación por internet accesos remotos, cifrar información confidencial en reposo, verifique la identidad de la información

Correctivos: ayudan a mitigar o disminuir los efectos de un evento que afecta a los sistemas, corrigiendo brechas de seguridad por medio del bloqueo de direcciones IP, bloqueo de acciones sospechosas, etc.

Detectivos: determina el momento en que ocurre un ataque monitoreando varios aspectos del sistema que le ayuda a obtener información, los mecanismos detectivos no evitan que algunas partes del sistema se comprometan. Entre los mecanismos detectivos que se pueden aplicar está la tecnología CAPTCHA y la implementación de controles que emitan alertas sobre intentos fallidos al intentar usar funcionalidades del sistema que no le competen y otras actividades irregulares.

Unidad 4: Desafíos Éticos y Sociales de la TI

Desafíos Éticos y Sociales de la TI

- Fundamentos éticos.
- Modelo conceptual para las cuestiones éticas, sociales y políticas.
- Los dilemas éticos de la Tecnología de Información.
- Delito computacional e implicancias morales
- La responsabilidad ética

Unidad 4: Fundamentos éticos

La ética se refiere a los principios morales que individuos que actúan como agentes libres puedan usar para tomar decisiones que guíen su conducta.

La tecnología de información y los sistemas de información hace que surjan cuestiones de ética para los individuos como para las sociedades, porque crean oportunidades de intenso cambio social, y amenazan las distribuciones de poder, riqueza, derechos y obligaciones.

La tecnología de la información puede servir para lograr un progreso social, pero también para cometer crímenes y amenazar valores sociales muy preciados.

Unidad 4: Modelo conceptual para las cuestiones éticas, sociales y políticas

Cinco dimensiones morales de la era de la información

1. Propiedad: Se refiere a los derechos de propiedad intelectual, como los derechos de autor y las patentes. Las cuestiones éticas relacionadas con la propiedad en la era de la información incluyen la piratería, la violación de derechos de autor, la privacidad y la protección de datos.
2. Acceso: Se refiere a la brecha digital y las inequidades en el acceso a la tecnología de la información. Esto implica la responsabilidad ética de garantizar que todas las personas tengan igualdad de oportunidades para acceder y utilizar la tecnología, evitando la exclusión digital.
3. Control: Se refiere a quién tiene el control y la autoridad sobre la tecnología de la información. Las cuestiones éticas relacionadas con el control incluyen el uso indebido de información, el espionaje, la vigilancia masiva y el poder de las grandes empresas de tecnología.
4. Calidad de vida: Se refiere al impacto de la tecnología de la información en la calidad de vida de las personas. Esto incluye aspectos como la salud, la seguridad, la privacidad, el bienestar emocional y la autonomía personal. Las cuestiones éticas en esta dimensión se centran en garantizar que la tecnología mejore la calidad de vida y no cause daño.
5. Responsabilidad: Se refiere a la responsabilidad ética de los individuos y las organizaciones que desarrollan, utilizan y controlan la tecnología de la información. Esto implica ser consciente de las consecuencias de las acciones y decisiones en el ámbito de la tecnología y asumir la responsabilidad de mitigar los posibles impactos negativos.

Unidad 4: Modelo conceptual para las cuestiones éticas, sociales y políticas

Tendencias tecnológicas claves que hacen surgir cuestiones de ética:

- **La duplicación de capacidad de cómputo**, ha permitido a casi todas las organizaciones utilizar sistemas de información en sus procesos de producción centrales. Como resultado, han aumentado la dependencia de los sistemas y la vulnerabilidad ante los errores de los sistemas y los datos de mala calidad. Los estándares para garantizar la exactitud y confiabilidad de los sistemas de información no gozan de aceptación ni aplicación universal.
- **Los adelantos en las técnicas de almacenamiento de datos y la baja en los costos de almacenamiento** han hecho que proliferen las bases de datos con información acerca de personas, mantenidas por organizaciones privadas y públicas. Estos adelantos han reducido el costo y aumentado la eficacia de violación rutinaria de la privacidad individual.
- **Los adelantos en las técnicas de extracción de datos de bases de datos grandes** intensifican las preocupaciones éticas, porque permiten a las compañías encontrar gran cantidad de información personal detallada acerca de los individuos.
- **Los adelantos en el trabajo con redes**, reducen los costos de trasladar y acceder a grandes cantidades de datos, y abren la posibilidad de explotar depósitos de datos de forma remota, utilizando máquinas de escritorio invadiendo la privacidad en una escala y con precisión inimaginable.

Unidad 4: Los dilemas éticos de la Tecnología de Información.

Algunos de los problemas éticos son dilemas éticos obvios, en los que un conjunto de intereses se opone a otro. Otras representan algún tipo de violación de la ética.

- Reducción de tamaño en la compañía, mediante tecnología: muchas de las grandes compañías están usando tecnología de información para reducir el tamaño de su personal.
- Privacidad del correo electrónico: muchas compañías afirman que tienen derecho a monitorear el correo electrónico de sus empleados porque son dueñas de las instalaciones, las proporcionan exclusivamente para fines del negocio y las crearon para operar su negocio.
- El uso de algoritmos implica una revolución en los sistemas de seguridad y videovigilancia almacenando el reconocimiento y comportamiento de las personas
- Los teléfonos celulares individuales pueden rastrearse sin el consentimiento o conocimiento del usuario.

En cada uno de estos casos existen valores opuestos, con grupos que se adhieren a cada una de las partes del debate.

Unidad 4: La responsabilidad ética

La responsabilidad ética en una organización de tecnología de la información (TI) implica reconocer y abordar los desafíos éticos específicos que surgen en este campo. Algunos aspectos clave de la responsabilidad ética en TI incluyen:

1. Privacidad y protección de datos: Las organizaciones de TI tienen la responsabilidad de proteger la privacidad y los datos de sus clientes y usuarios. Esto implica implementar medidas de seguridad adecuadas, obtener el consentimiento adecuado para recopilar y utilizar datos, y cumplir con las leyes y regulaciones de protección de datos.

2. Seguridad de la información: Las organizaciones de TI deben tomar medidas para garantizar la seguridad de la información que manejan. Esto incluye protegerse contra amenazas de ciberseguridad, implementar controles de acceso adecuados, realizar auditorías de seguridad y promover una cultura de seguridad en toda la organización.

3. Ética en el desarrollo de software y tecnología: Las organizaciones de TI tienen la responsabilidad de desarrollar y ofrecer tecnología ética. Esto implica considerar los posibles impactos sociales, económicos y ambientales de la tecnología, evitar la discriminación algorítmica, garantizar la transparencia y la equidad en los algoritmos utilizados, y fomentar la inclusión y la diversidad.

4. Responsabilidad social y sostenibilidad: Las organizaciones de TI deben asumir la responsabilidad de su impacto social y ambiental. Esto implica considerar el uso responsable de los recursos, minimizar la huella de carbono, adoptar prácticas de desarrollo sostenible y promover la igualdad de oportunidades en el campo de la tecnología.

5. Cumplimiento normativo: Las organizaciones de TI deben cumplir con las leyes y regulaciones aplicables, como las relacionadas con la protección de datos, la seguridad de la información, el comercio electrónico y la propiedad intelectual.

Unidad 4: Cumplimiento

El cumplimiento se refiere al acto de cumplir con requisitos, normas, leyes, regulaciones u otros estándares establecidos. Implica adherirse y satisfacer los criterios y condiciones establecidos por una autoridad reguladora, una organización o una legislación específica.

El cumplimiento es esencial en diversos ámbitos, como el cumplimiento legal, el cumplimiento normativo, el cumplimiento de políticas internas o el cumplimiento de estándares de calidad. Algunos ejemplos comunes de cumplimiento incluyen el cumplimiento de normas de seguridad, el cumplimiento de leyes laborales, el cumplimiento de regulaciones ambientales, el cumplimiento de estándares de calidad ISO, el cumplimiento de políticas de privacidad y el cumplimiento de requisitos financieros.

El cumplimiento implica llevar a cabo actividades y medidas para garantizar que una organización cumpla con las obligaciones y requisitos establecidos. Esto puede incluir la implementación de políticas y procedimientos, la realización de auditorías y controles internos, el seguimiento de las actividades y el mantenimiento de registros adecuados.

El incumplimiento puede tener consecuencias negativas, como sanciones legales, multas, pérdida de reputación, pérdida de oportunidades comerciales y daño a las relaciones con los clientes y otras partes interesadas. Por lo tanto, es importante que las organizaciones dediquen recursos y esfuerzos para garantizar el cumplimiento de los requisitos aplicables a su ámbito de actuación.

Unidad 4: Certificaciones ISO

ISO 9001:

Las normas ISO son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos.

La ISO 9001 es el estándar internacional publicado por ISO (International Organization for Standardization) para establecer de manera efectiva un Sistema de Gestión de la Calidad.

Se trata de una norma de gestión de la calidad que especifica unos requisitos generales para que pueda ser aplicada en cualquier tipo de organización, sin importar el sector, tamaño o tipo. Por ello, este estándar de calidad puede ser aplicado tanto por un trabajador autónomo, una empresa o una institución sin ánimo de lucro.

Un sistema de gestión de calidad ISO 9001, abreviado con las siglas SGC, está formado por un conjunto de políticas, procesos y procedimientos documentados.

Por lo general, el estándar se implanta cuando una organización necesita:

- Demostrar su capacidad de ofrecer productos y servicios que satisfagan los requisitos de los clientes y cumplir con la legalidad vigente de su entorno.
- Aumentar la satisfacción del cliente a través de una serie de procesos para mejorar su funcionamiento y asegurarse de esta forma la conformidad de todos los requisitos, tanto los exigidos por los consumidores como los reglamentarios.

Unidad 4: Certificaciones ISO

Certificaciones ISO mas comunes relacionadas con la tecnología de la información:

- ISO/IEC 12207: Esta norma establece el estándar para el ciclo de vida del software, definiendo los procesos y actividades necesarios para desarrollar, operar y mantener sistemas de software.

- ISO/IEC 20000: Esta norma establece los requisitos para la gestión de servicios de tecnología de la información (TI). Proporciona directrices para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar los servicios de TI, con el objetivo de ofrecer un alto nivel de calidad y cumplir con los requisitos del cliente.

- ISO/IEC 25000: Conocida como la serie de normas SQuaRE (Software product Quality Requirements and Evaluation), esta serie de normas define un conjunto de modelos y técnicas para la evaluación de la calidad del software, incluyendo características como funcionalidad, confiabilidad, usabilidad, eficiencia y mantenibilidad.

- ISO/IEC 27001: Esta norma establece los requisitos para un sistema de gestión de seguridad de la información (SGSI), que abarca tanto la seguridad física como lógica del software. Proporciona directrices para identificar, evaluar y tratar los riesgos de seguridad de la información en el desarrollo de software.

Unidad 4: Certificaciones ISAE

Certificaciones ISAE :

Estas son algunas de las normas ISAE más comunes utilizadas en el ámbito del aseguramiento de la información y los servicios. Cada norma se aplica a un contexto específico y tiene como objetivo proporcionar garantías y confianza a las partes interesadas sobre diferentes aspectos de una organización y sus servicios.

- ISAE 3402: Como se mencionó anteriormente, esta norma se centra en la auditoría de controles internos en una organización que presta servicios a terceros. Es ampliamente utilizada para evaluar la efectividad de los controles y garantizar la seguridad de los servicios prestados.

- ISAE 3000: Esta norma aborda el aseguramiento de la información fuera del ámbito de la auditoría financiera. Se utiliza para evaluar la confiabilidad e integridad de la información en informes no financieros, como informes de sostenibilidad, cumplimiento normativo, seguridad de la información, entre otros.

- ISAE 3401: Esta norma está relacionada con la prestación de servicios de outsourcing o externalización. Se utiliza para evaluar y auditar los controles en una organización que presta servicios a sus clientes, con el objetivo de proporcionar confianza en la calidad y seguridad de dichos servicios.

- ISAE 3002: Esta norma se enfoca en el aseguramiento de la información relacionada con la seguridad de TI. Se utiliza para evaluar y auditar los controles de seguridad de la información en una organización, garantizando la protección adecuada de los activos de información y la mitigación de riesgos de seguridad.

- ISAE 3410: Esta norma se centra en el aseguramiento de la calidad de los sistemas de información. Se utiliza para evaluar y auditar los controles en el diseño, desarrollo, implementación y mantenimiento de sistemas de información, asegurando la calidad y confiabilidad de los mismos.