Curso de Introducción a la ciberseguridad

Para entender lo que es la ciberseguridad es necesario entender los siguientes conceptos:

- Seguridad que se define como la ausencia de peligro o riesgo
- Seguridad de la información que se basa en la protección de la información que es relevante o que tiene valor de una organización reduciendo los riesgos y mitigando las amenazas

Teniendo en cuenta estos conceptos podemos definir la ciberseguridad como un conjunto de medidas de protección de la información tratada por los sistemas de información que se encuentran interconectados. Se diferencia de la seguridad de la información en que la ciberseguridad se centra más en la parte digital

Existen distintas categorías de protección:

- Seguridad de red- se basa en la protección de las redes informáticas
- Seguridad de aplicaciones- se basa en mantener el software en buen estado ya que si no lo está podría causar una vulnerabilidad
- Seguridad de los datos- se basa en la protección de la información tanto en tránsito como almacenada
- Seguridad operacional- son los procesos y decisiones para el manejo y protección de los activos de datos
- Recuperación ante desastres y continuidad de negocio- es como una organización responde a un incidente de seguridad o cualquier otro evento que cause una pérdida de datos o de las operaciones.
- Concienciación de usuarios finales- se centra en el factor menos predecible de todos, las personas. Es por esta causa por la que se suelen producir la mayor parte de los problemas.

Del mismo modo que podemos clasificar la protección podemos clasificar a las amenzas :

- Ciberactivistas- motivados políticamente buscan dar a conocer una causa o bien castigar a una organización o gobierno que consideran está actuando de forma poco ética
- Cibercriminales- se dedican a tareas tales como el espionaje corporativo o al cobro de rescates
- Terroristas- los grupos terroristas se han dado cuenta de que un ataque digital podría tener consecuencias catastróficas para un país
- Agentes estatales- muchos gobiernos cuentan con equipos digitales para producir desinformación, cortar suministros...

Con la dependencia tecnológica de muchas empresas y con los procesos de transformación digital que muchas organizaciones están acometiendo, el nivel de amenaza se ha incrementado exponencialmente pudiendo causar grandes pérdidas a estas, es por este motivo que la ciberseguirdad ha tomado un papel muy importante.

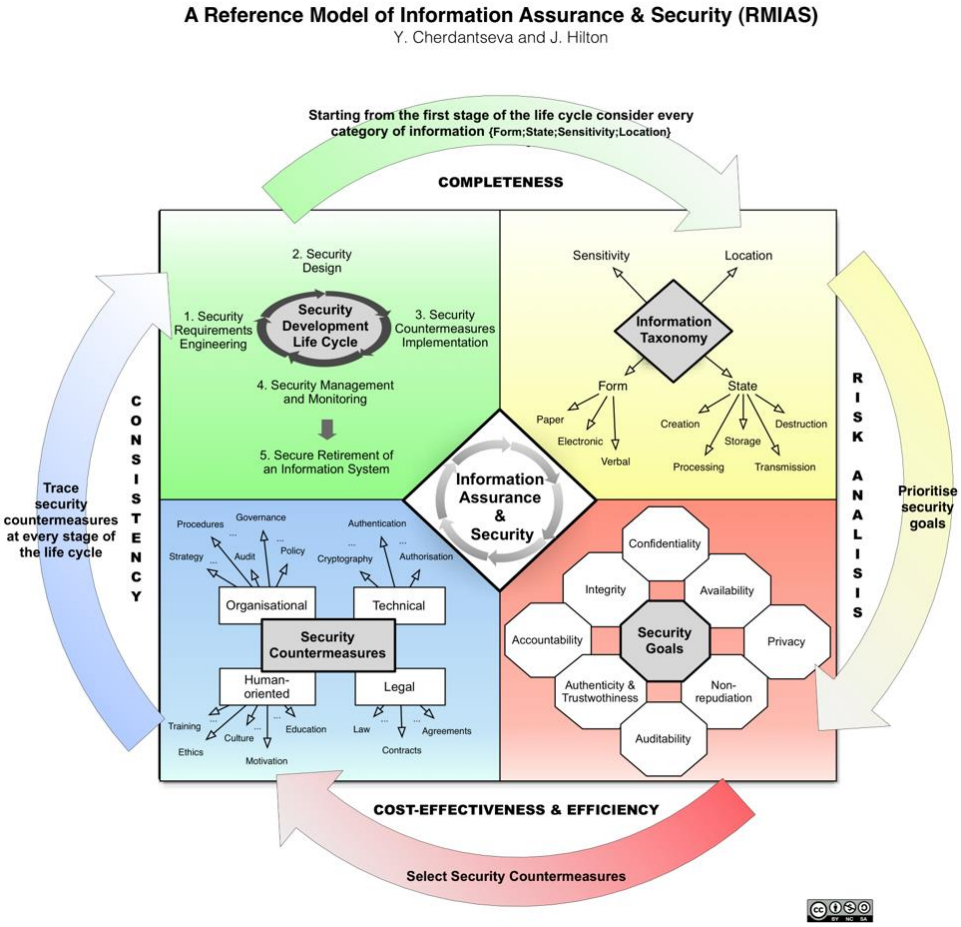
La seguridad se puede definir por varias dimensiones:

- Confidencialidad: es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.
- Integridad: Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.
- Disponibilidad- Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.
- Trazabilidad- Se trata del conjunto de procesos, técnicas y herramientas que permiten saber dónde ha estado, quién ha accedido y/o modificado el dato, etc.
- No repudio/Autenticidad- El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

Existen otra serie de conceptos que es importante conocer:

- Amenaza- Circunstancia desfavorable que puede ocurrir y que tendría consecuencias negativas sobre los activos, provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Puede tener causas naturales, ser accidental o intencionada.
- Auditoría de seguridad- Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en TI con el objetivo de identificar posibles amenazas o debilidades en el sistema
- Business Impact Analysis (BIA)- Se trata de un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio.
- Defensa en profundidad- Se basa en la premisa de que todo componente de un sistema puede ser vulnerado, y por tanto no se debe delegar la seguridad de un sistema en un único método o componente de protección. De esta forma propone el uso de distintas técnicas que permitan, al menos, duplicar los elementos de protección para limitar los daños en caso de una intrusión en la primera línea de defensa o componente más expuesto.
- Fuga de información- Es la pérdida de la confidencialidad de la información privada de una persona o empresa
- Incidente de seguridad- Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa.
- SGSI: Un Sistema de Gestión de Seguridad de la Información es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad.
- Vulnerabilidad: Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota

Modelo RMIAS



El RMIAS promueve un enfoque integral para la seguridad de la información y la seguridad. Es independiente de la tecnología y puede ser aplicado por una organización de cualquier tamaño en cualquier dominio.

Este modelo cuenta con 4 dimensiones:

- Ciclo de vida de la seguridad

  Incorpora un modelo genérico en 5 fases:

  1. Ingeniería de requisitos de seguridad- En esta fase se deben analizar los requisitos de seguridad que un sistema deberá tener en base a la criticidad de la información gestionada, así como otros requisitos externos como el cumplimiento de leyes, regulaciones y estándares o bien requisitos contractuales con clientes de la organización.
  2. Diseño de la seguridad- En esta fase se deberán recopilar y analizar todos los requisitos de seguridad y realizar el diseño de alto nivel para su implementación
  3. Implementación de contramedidas- En esta fase se deben implementar las contramedidas a bajo nivel en base al diseño en alto nivel realizado en la anterior fase.

4. Gestión y monitorización de la seguridad- La seguridad debe ser monitorizada de forma continua, así como el desempeño y cumplimiento de las diferentes medidas. A la vez se revisará de forma regular o tras que el sistema haya sufrido cambios con impacto en la seguridad. Así, ante posibles cambios en el entorno o problemas en los controles se podrá comenzar de nuevo el ciclo (dado que este, como se puede ver en el diagrama es un ciclo continuo)
5. Retirada del SI- Una vez que un sistema vaya a ser retirado por no ser necesario o bien ser sustituido por un nuevo sistema, se deberá tener en cuenta varios aspectos de seguridad como la eliminación segura de la información gestionada por el mismo.

- Taxonomía de la información- permite comprender la naturaleza de la información a proteger

  Los diferentes atributos de la información son los siguientes:

  - Forma (Formato): Papel, digital o verbal.
  - Sensibilidad (Criticidad): La importancia o criticidad de la información en base a criterios como su valor económico, el impacto que podría en los medios un incidente que le afecte, su impacto en el negocio, el incumplimiento de leyes, regulaciones y estándares, etc).
  - Localización: Dependiendo de dónde se encuentre la información o desde donde podrá ser accedida, se tendrán una serie de riesgos u otros. Por ello es necesario establecer para cada sistema dónde se alojarán los sistemas y la información así como su accesibilidad
  - Estado: Se consideran 5 estados para la información. Creación, transmisión, almacenamiento, procesamiento y destrucción. Se deberán contemplar diferentes controles para cada estado con el objetivo de asegurar la seguridad de la información en todo momento.

- Objetivos de Seguridad

Los objetivos de la seguridad son los siguientes:

- Rendición de cuentas (Acountability): La habilidad de un Sistema para mantener a los usuarios responsables por sus acciones.
- Auditabilidad: La habilidad de un Sistema para realizar monitorización persistente y no puenteable de todas las acciones realizadas por usuarios u otros sistemas en el propio Sistema.
- Autenticidad/Confiabilidad: La habilidad de un Sistema para verificar la identidad y establecer la confianza en una tercera parte y la información que provee.
- Disponibilidad: Un sistema debería asegurar que todos los componentes del sistema están disponibles y operativos cuando son requeridos por un usuario autorizado.
- Integridad: Un sistema debería asegurar la completitud, exactitud y ausencia de modificaciones no autorizadas en todos sus componentes.

    - No repudio: La habilidad de un Sistema para proveer (con validez legal) la ocurrencia/no ocurrencia de un evento o la participación/no participación de una parte en un evento.
    - Privacidad: Un Sistema debería obedecer cualquier legislación sobre la privacidad de datos y permitir a los individuos controlar su información personal.
- Contramedidas de Seguridad

    - Controles técnicos- Se refiere a medios técnicos para alcanzar los objetivos de seguridad. Por ejemplo, la identificación, autenticación y autorización permiten alcanzar respectivamente la integridad, confidencialidad y rendición de cuentas.
    - Controles organizacionales- Se refiere a las actividades administrativas de una organización con el objetivo de construir y mantener un entorno seguro donde los controles de seguridad pueden ser implementados y gestionados de forma efectiva.
    - Controles orientados a personas- Es habitualmente el eslabón más débil de la cadena. Las personas deben ser consideras en un sentido amplio, no solo el personal de la organización a todos los niveles sino otros como proveedores, otras terceras partes, etc.
    - Controles legales- Se refiere al uso de la legislación con el propósito de la protección de la información.

Además, se deben realizar los siguientes controles

- Controles administrativos- Son aquellos controles procedimentales, administrativos y/o documentales que establecen las reglas a seguir para la protección del entorno. Tienen en cuenta aspectos como la documentación requerida para estandarizar la práctica de seguridad (como las políticas y procedimientos), la formación y concienciación, el gobierno de la seguridad, la seguridad en la gestión de recursos humanos, etc.
- Controles lógicos- Son aquellos controles basados en una combinación de hardware y software. Tienen en cuenta aspectos como la protección de servidores, puntos finales y la red, la gestión de las identidades y el control de acceso, la protección de información almacenada y en tránsito, etc.
- Controles físicos- Son aquellos tipos de controles tangibles orientados a la protección del entorno y de los recursos físicos de la organización. Tienen en cuenta la protección contra accesos físicos no autorizados (puertas de seguridad, cámaras de vigilancia, sensores de movimiento, tornos, etc), protección del equipamiento (supresores de subidas de tensión, Sistemas de Alimentación Ininterrumpida, etc) y contra amenazas medioambientales (protección contra incendios o inundaciones, protección contra vibraciones, etc).