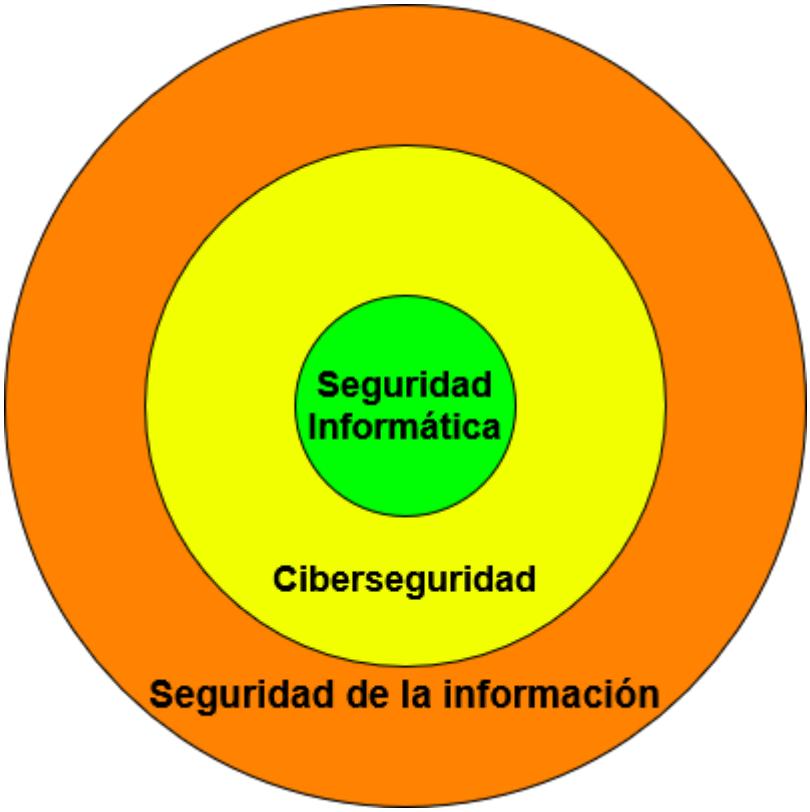
[GSI] Introducción

La seguridad informática no tiene en cuenta el ciberespacio ya que existe desde antes de la existencia de internet. Se centra en proteger un computador o una red de computadores. La seguridad de la información va desde ataques originados en el ciberespacio hasta catástrofes naturales o robos de documentación, se centra en la información.



La ciberseguridad, la seguridad de la información y lo que hay entremedias:

- La **ciberseguridad** tiene que ver con activos que son vulnerables por tecnologías de comunicación y que no tienen por que tener información relevante.
    - Se encarga de proteger activos digitales.
- La **seguridad de la información** son aquellos activos que tienen información relevante que se transmiten sin el uso de tecnologías de la comunicación (Papel, propiedad intelectual...).
- La **seguridad de la información** es importante por que toda la información se ha convertido en información digital.

Seguridad de la información

- Identificar: Usamos el conocimiento sobre la organización para minimizar riesgos.
- Proteger: Se diseñan controles para limitar el impacto de eventos potenciales.
- Detección: Se implementan actividades para identificar eventos de ciberseguridad
- Respuesta: Se toman las medidas apropiadas cuando se detecta un evento de seguridad.
- Recuperación: Plan para ser resilente y recuperar los servicios y capacidades comprometidas.

Gestión de la Seguridad de la Información

La información debe ser gestionada ya que no existe la seguridad total y esta no es la única cosa importante. El nivel de seguridad depende y evoluciona. La seguridad tiene un precio, la gestión de la seguridad de la información busca minimizar la suma del coste causando por los incidentes más el coste de los controles de seguridad. La seguridad de la información tiene como objetivo ayudarnos a decidir que medidas de seguridad deben ser aplicadas para reducir al máximo los riesgos:

- Entendiendo el riesgo de la información
- Identificar oportunidades de mejora
- Asignar recursos de forma efectiva

Recomendaciones generales

- Realizar entrenamiento de ciberseguridad
- Mantener el software y sistemas operativos actualizados
- Usar antivirus
- Realizar revisiones de seguridad regulares
- Usar contraseñas fuertes
- No abrir adjuntos en emails recibidos de desconocidos
- Evitar usar Wi-Fi públicas
- Realizar copias de seguridad.

GRC: Govenance, Risc and Compliance

- Gobernancia: Responsable de la junta directiva y gerrencia de la organización.
- Gestión de Riesgos: Coordinación de actividades que dirigen y controla la empresa con respecto al riesgo
- Cumplimiento: El acto de adherirse a requerimientos definidos por leyes y regulaciones.

Principales organizaciones

- INCIBE: Instituto Nacional de Ciberseguridad
- CCN: Centro Criptológico Nacional
- Oficina de Seguridad del Internauta.
- ENISA: European Network and Information Security Agency
- CSIRT
- NSIT: National Institute of Standards and Technology

Objetivos de seguridad: CIA

- Confidencialidad: Prevenir que la información sea revelada a partes no autorizadas
    - Información Personal: Los datos personales solo deben ser accedidos por el personal autorizado para los propósitos indicados.

    - Negocio: Datos sensibles como ventas o datos de clientes
    - La confidencialidad cubre el alcacenaje, procesado y tránsito de la información.
- Integridad: Proteger la información contra cambios por parte de partes no autorizadas
    - Personal: Datos personales
    - Negocio: Documentos importantes que no deben ser alterados
    - Integridad de los datos: La propiedad que tienen los datos cuando no han sido alterados de forma no autorizada
    - Integridad del sistema: La característica que tiene un sistema cuando realiza las funciones correctamente sin manipulaciones no autorizadas.
- Disponibilidad: La capacidad de dar acceso a la información a las partes autorizaddas cuando es solicitada
    - Personal: Debes poder acceder tus datos personales
    - Negocio: Un gerente debe ser capaz de acceder los datos de la empresa cuando sean necesarios.

Definiciones

- Autenticidad (ISO 27000): Propiedad de una entidad que es lo que dice ser
- No repudio (ISO 27000): La capacidad de probar la ocurrencia, acción y su origen
- Fiabilidad (ISO 27000): Propiedad de tener un comportamiento y resultado consistentes.
- Responsabilidad (NIST): La meta de seguridad que genera el requisito de acciones de una entidad que debe ser trazada de forma única.
- Garantía (NIST): Realiza la medida que protege y defiende información y sistemas de información.