Título:	Fundamentos de la Seguridad de la Información
Tipo:	Monografía
Autor:	Franklin Alexis Díaz Díaz
Fecha:	Abril 2018
Palabras claves:	Confidencialidad, integridad, disponibilidad
Aprobado por:	Decano de la Facultad de Ingeniería Mg. Ing. Enrique Durand Bazán
Firma:	

INTRODUCCIÓN

Los datos, considerado el nuevo petróleo del mundo, al ser procesados se convierten en información con los cual las organizaciones pueden realizar sus operaciones y así poder brindar sus servicios u ofreciendo productos

Para un adecuado funcionamiento del negocio, las organizaciones poseen información la cual debe ser protegida frente a los riesgos y amenazas que siempre están latentes, y de esa manera evitar la ocurrencia de incidentes que puedan afectar la continuidad normal del negocio.

En la actualidad, no basta solamente con asegurar la información ya sea en formato digital o impresa; sino que existen una variedad de activos, entiéndanse éstos como aquellos que dan valor a la organización, que necesitan ser protegidos ante ataques internos o externos. Entre la variedad de activos que tienen relación directa con información empresarial, aparte de lo tecnológico, se tiene a la infraestructura, los procedimientos, el personal, la documentación. Todos lo mencionado poseen vulnerabilidades que agentes sin la autorización respectiva querrán hacerse de la información que manejan.

Para ello la seguridad de la información debe garantizar un conjunto de 3 elementos, conocidos comúnmente como la tríada CID: confidencialidad, integridad, disponibilidad.

La Seguridad de la Información

La seguridad de la información se puede definir como como la protección de la confidencialidad, integridad y disponibilidad de los activos de información, según sean necesarios, para alcanzar los objetivos de negocio de la organización.

Además:

- La seguridad de la información se obtiene como resultado de la implementación de un conjunto de controles, que comprenden políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software.
- Los controles deben ser establecidos, implementados, monitoreados, evaluados y mejorados continuamente con el fin de cumplir con los objetivos del negocio y la seguridad de la organización.
- La identificación de los controles adecuados requiere una planificación detallada.

Objetivos de la seguridad de la información

1. Confidencialidad: comprende la protección de los datos transmitidos contra ataques pasivos, es decir, el acceso no autorizado, que incluirá medidas tales como el control de acceso y encriptación. La pérdida de la confidencialidad se produce cuando hay una violación de la confidencialidad de cierta información (por ejemplo, la contraseña de un usuario o administrador del sistema) permitiendo que quede expuesta la información restringida, las cuales estaban disponibles sólo a un determinado grupo de usuarios.
2. Autenticidad: está interesada en garantizar que la comunicación sea auténtica, es decir, origen y destino pueden verificar la identidad de la otra parte implicada en la comunicación, con el fin de confirmar que la otra parte es quien dice ser. El origen y el destino son normalmente usuarios, dispositivos o procesos.
3. Integridad: es la garantía contra ataques activos a través de los cambios o de remociones no autorizadas. La integridad es también un prerrequisito para otros servicios de seguridad. Por ejemplo, si la integridad de un sistema de control de acceso a un sistema operativo es violada, también se viola la confidencialidad de sus archivos. La pérdida de la integridad se produce en un momento en que cierta información está expuesta a la manipulación por personal no autorizado.

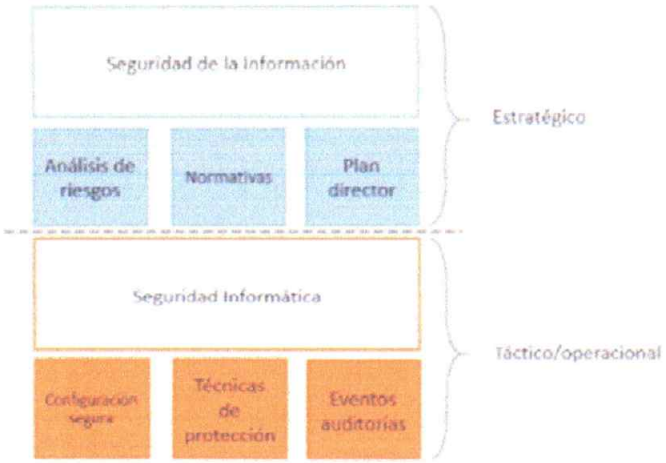
Seguridad de la Información vs Seguridad Informática

- La Seguridad de la Información

  Es la disciplina que se encarga de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información de activos.

- La Seguridad Informática

  Implementa medidas técnicas que preservaran las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.



La seguridad de la información se encuentra en el nivel estratégico de una organización, ya que se encarga de la planificación de administrarla, para lo cual se elabora el Sistema de Gestión de Seguridad de la Información (SGSI).

Mientras que la seguridad informática se encuentra en el nivel táctico y operativo, ya que se encarga de elaborar los procedimientos planteados en el SGSI para su respectiva ejecución.

Términos relacionados con la Seguridad de la Información

- Incidente de seguridad

  Cualquier evento adverso relacionado con la seguridad, por ejemplo, ataques de denegación de servicio (Denial of Service, DoS), robo de información, fuga, obtención de un acceso no autorizado.

- Activo

Cualquier elemento que tenga valor para la organización y su negocio. Por ejemplo: BD, software, equipos, servidores, dispositivos de red (router, switch, etc), personas, procesos y servicios.

- Vulnerabilidad

  Cualquier debilidad que puede ser explotada y ponga en peligro la seguridad de los sistemas y datos. Fragilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

- Amenaza

  Cualquier evento que explote vulnerabilidades. Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización.

- Riesgo

  Combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización.

- Ataque

  Cualquier acción que comprometa la seguridad de una organización.

- Impacto

  Resultado evaluado de un evento en particular.

Controles

Para ayudar a mitigar el riesgo, se puede establecer medidas que ayuden a garantizar que se tenga en cuenta un tipo determinado de amenaza. Estas medidas se denominan controles.

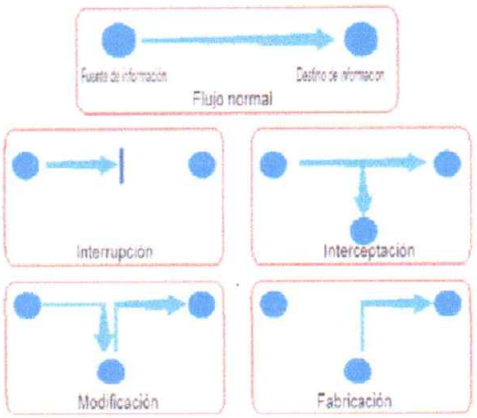
Los controles se dividen en tres categorías:

1. Físicos
   a. Son aquellos controles que protegen el entorno físico en el que se encuentran los sistemas o donde se almacenan los datos.
   b. Dichos controles también controlan el acceso dentro y fuera de dichos entornos.
   c. Los controles físicos pueden no parecer parte de la seguridad de la información, en realidad son uno de los controles más críticos con los que se debe preocupar.
   d. Los controles físicos incluyen elementos como cercas, puertas, cerraduras, protectores, cámaras, pero también incluyen sistemas que mantienen el entorno físico, como sistemas de calefacción y aire acondicionado, sistemas de extinción de incendios y generadores de energía de respaldo.

2. Lógicos
    a. Son aquellos que protegen los sistemas, redes y entornos que procesan, transmiten y almacenan nuestros datos.
    b. Pueden incluir elementos como contraseñas, encriptación, controles de acceso lógico, firewalls y sistemas de detección de intrusos.
    c. Los controles lógicos permiten evitar que se realicen actividades no autorizadas
3. Administrativos
    a. Se basan en reglas, leyes, políticas, procedimientos, pautas y otros elementos que son de naturaleza "en papel", estableciendo las reglas sobre cómo esperamos que se comporten los usuarios de nuestro entorno.
    b. Un concepto importante cuando discutimos los controles administrativos es la capacidad de exigir su cumplimiento. Si no se tiene la autoridad o la capacidad para garantizar que se cumplan nuestros controles, son peores que inútiles, porque crean una falsa sensación de seguridad.

Modelos de ataque

1. Interrupción
   Cuando un activo se destruye o queda indisponible (o inutilizable), caracterizando un ataque contra la disponibilidad. Por ejemplo, la destrucción de un disco duro.
2. Interceptación
   Cuando se accede a un activo por un tercero no autorizado, caracterizando un ataque contra la confidencialidad. Por ejemplo, copia no autorizada de archivos o programas.
3. Modificación
   Cuando se accede a un activo por un tercero no autorizado y se modifica, materializando un ataque contra la integridad. Por ejemplo, cambio de los valores en un archivo de datos.
4. Fabricación
   Cuando una parte no autorizada inserta objetos falsificados en un activo, configurando un ataque contra la autenticidad. Por ejemplo, la adición de registros en un archivo.



Formas de ataque

El ataque es un acto deliberado de tratar de esquivar los controles de seguridad con el objetivo de explotar las vulnerabilidades.

1. Ataques pasivos
   Ataques basados en escuchar y monitorear las transmisiones, con el fin de obtener la información que se está transmitiendo.
2. Ataques activos
   involucran la modificación de datos, la creación de objetos falsos o negación de servicio, y tienen las propiedades opuestas de ataques pasivos.

Factores críticos para el éxito en la Seguridad de la Información

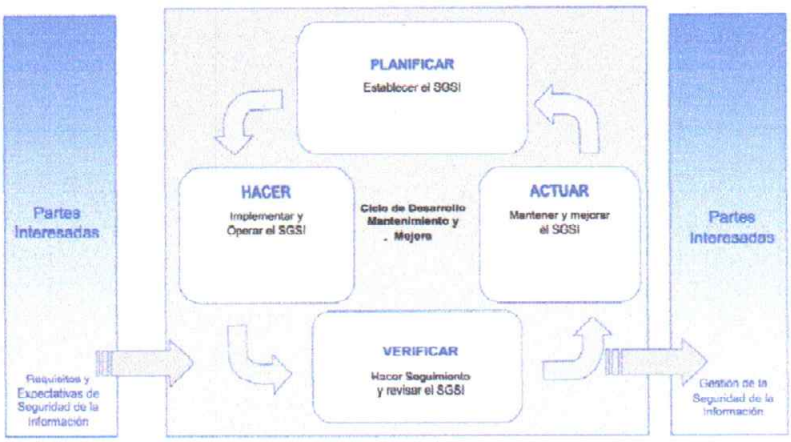
- La política de seguridad de la información, los objetivos y las prácticas deben reflejar los objetivos de negocio de la organización.
- El enfoque y la estructura que han sido adoptados para la ejecución, el mantenimiento, el seguimiento y la mejora de la seguridad de la información deben ser compatibles con la cultura de la organización.
- Todos los niveles gerenciales de la organización deben estar comprometidos y apoyar la seguridad de la información.
- Los requisitos de seguridad de la información, el análisis, la evaluación y la gestión del riesgo deben ser bien entendidos (en detalle).
- La seguridad de la información debe darse a conocer, de manera eficiente, a todas las entidades de la organización (presidentes, directores, gerentes, empleados, contratistas, etc.).

- Distribución y comunicación de directrices, políticas y normas para todas las partes involucradas.
- Suministro de recursos financieros para la gestión de seguridad de la información.
- Establecimiento de un proceso eficiente para la gestión de incidentes de seguridad.
- Implementación de un sistema de medición de la gestión de seguridad de la información.

El ciclo o modelo de Deming

El Ciclo de Deming o Ciclo PDCA (Plan, Do, Check, Act) es un enfoque para mejorar continuamente la calidad de las empresas mediante una metodología de resolución de problemas utilizada en los sistemas de gestión, compuesta de cuatro puntos fundamentales y cuyo objetivo último es la calidad.

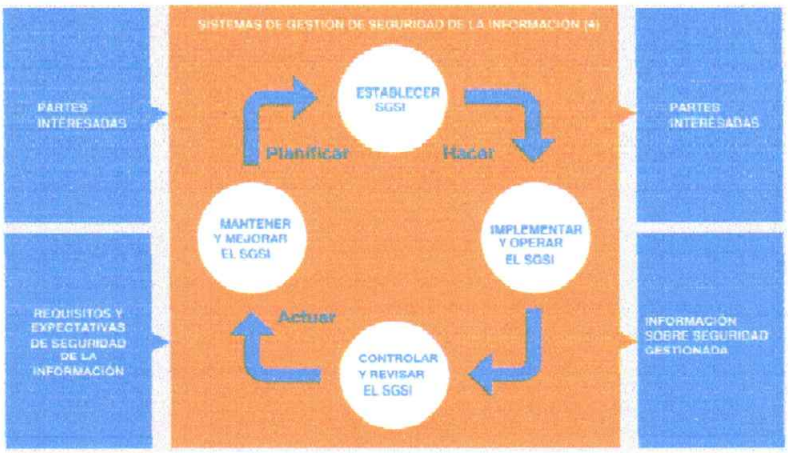
1. Planear
   Establecer políticas, objetivos, procesos y procedimientos del SGSI, para la gestión del riesgo y la mejora de la seguridad de información.
2. Hacer
   Implementar y operar las políticas, controles, procesos y procedimientos del SGSI.
3. Verificar
   Evaluar y medir el desempeño de un proceso con base en la política, los objetivos y la experiencia práctica del SGSI y presentar los resultados para la revisión de la dirección.
4. Actuar
   Llevar a cabo acciones correctivas y preventivas, basadas en los resultados de la auditoría interna del SGSI y el análisis realizado por la dirección u otra información pertinente, para lograr la mejora continua del SGSI.



Etapas de un Sistema de Gestión de Seguridad de la Información

Las etapas de un Sistema de Gestión de Seguridad de la Información (SGSI) toma como referencia y adopta el Modelo de Deming para crear sus propias etapas, las cuales son:

1. Establecer el SGSI
2. Implementar y operar el SGSI
3. Monitorear y analizar críticamente el SGSI
4. Mantener y mejorar el SGSI



BIBLIOGRAFÍA

Areitio, J. (2008). Seguridad de la Información. España: CENGAGE Learning.

Postigo, A. (2020). Seguridad Informática. España: Ediciones Paraninfo.

Vega, E. (2021). Seguridad de la Información. España: Ediciones 3Ciencias.

Miguel, J. (2015). Protección de datos y seguridad de la información. España: Editorial RA-MA.

Menéndez, S. (2022). Auditoría de Seguridad Informática Curso Práctico. España: Editorial RA-MA.

Ortega, J. (2024). Ciberseguridad Manual Práctico. Colombia: Ediciones ECOE.