**Seguridad Informática:**

La seguridad de la información hace referencia a todas aquellas medidas preventivas, reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad y la integridad de la misma.

**Evento de seguridad de la información**: ocurrencia identificada en un sistema, servicio o estado de una red que indica una posible violación de la política de seguridad o falla en los controles, o una situación previamente desconocida que podría ser *relevante para la seguridad.*

**Incidente de seguridad de la información**: evento individual o serie de eventos de seguridad de la información inesperados o no deseados que tiene una *probabilidad significativa de comprometer* las operaciones del negocio y amenazar la seguridad de la información.

**Sistema de Gestión de Seguridad de la Información (SGSI)**

Busca establecer y mantener programas, controles y políticas que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información. Es un proceso continuo

Debe comprender:

Elementos administrativos

Políticas de Seguridad.

Organización y División de Responsabilidades

Seguridad Lógica.

**Principios Básicos de la Seguridad de la Información:**

Integridad, Confidencialidad, Disponibilidad.

**Plan de respuesta a Incidentes:**

Fases

* Acción inmediata para detener o minimizar el incidente.
* Investigación del incidente.
* Restauración de los recursos afectados.
* Reporte del incidente a los canales apropiados.

Componentes

* Equipo de expertos
* Una estrategia legal revisada y aprobada
* Soporte financiera de la organización
* Soporte ejecutivo de la gerencia superior de la compañía o áreas afectadas
* Recursos físicos

**Atacantes**:

Hacker, Cracker, Lammer, Copyhacker, Bucaneros, Phreaker, Newbie, Script Kiddie.

**Principales Ataques a las Organizaciones**:

* Propagación de malware por e-mail y spam
* Botnets
* Ataques de phishing alojados en sitios web
* Ataques XML sobre arquitectura orientada a servicios (SOA) y Web Services

**Seguridad Lógica:**

Restringir el acceso a los programas y archivos.

Asegurar que los usuarios puedan trabajar sin supervisión minuciosa sin afectar ningún dato, programa ni archivo que no deban.

Asegurar que se están utilizando los datos, archivos y programas correctos en cada situación.

Que la información transmitida sea recibida sólo por el destinatario deseado.

Que la información recibida sea la misma que ha sido enviada

Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

Servicios de Seguridad:

No repudio de origen: Prueba que el mensaje fue enviado por la parte específica.

No repudio de destino: Prueba que el mensaje fue recibido por la parte específica.

Tipos de Usuario:

Propietario, Administrador, Usuario principal o referente (Key User), Usuario de explotación, Usuario de auditoria.

Sistemas de Cifrado:

|  |  |  |
| --- | --- | --- |
| Simétrico | Asimétrico | Híbrido |
|  |  |  |

**Seguridad Física:**

Administración de respaldos de información (Backups)

Alta disponibilidad

Gestión de centros de cómputos principales y secundarios

**ISO/IEC 27000**

Marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización.

ISO/IEC 27001: Norma principal de la serie.

ISO/IEC 27002: Es una guía de buenas prácticas.

|  |  |
| --- | --- |
| **ITL:**  Gestión de la Seguridad de la Información | **ONTI**  Oficina Nacional de Tecnología Informática |
| Asegura que la información que estamos utilizando cumple con los requisitos legales del ámbito que le atañe.  Fases: Planificación, Ejecución, Seguimiento. |  |

**Firma Digital:**

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales. La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

**Firma Electrónica:**

Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, *que carezca de alguno de los requisitos legales para ser considerada firma digital*. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.