**Introducción.**



Tema de la unidad III que habla sobre las políticas de cómo se constituye la seguridad en las redes por medio de normas y reglas establecidas en una empresa, por cual evita dichos riesgos, catástrofes y perdida/robo de información.

**Políticas de seguridad**

**¿Cómo podemos proteger el sistema informático?**

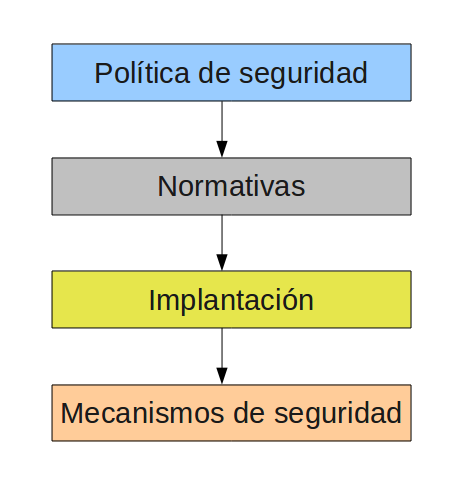
Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

Definimos Política de seguridad como un “documento sencillo que define las directrices organizativas en materia de seguridad” (Villalón).

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas más específicas.

Esquemáticamente:



Los mecanismos de seguridad se dividen en tres grupos:

1. **Prevención**:

Evitan desviaciones respecto a la política de seguridad.

Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

1. **Detección**:

Detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema.

Ejemplo: la herramienta Tripwire para la seguridad de los archivos.

1. **Recuperación**:

Se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Ejemplo: las copias de seguridad.

Dentro del grupo de mecanismos de prevención tenemos:

* **Mecanismos de identificación e autenticación**

Permiten identificar de forma única 'entidades' del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser.

Pasados estos dos filtros, la entidad puede acceder a un objeto del sistema.

En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos más utilizados.

* **Mecanismos de control de acceso**

Los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

* **Mecanismos de separación**

Si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel.

Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

* **Mecanismos de seguridad en las comunicaciones**

La protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH o Kerberos, que cifran el tráfico por la red.

**Políticas de seguridad**

El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

* definir qué es seguridad de la información, cuáles son sus objetivos principales y su importancia dentro de la organización
* mostrar el compromiso de sus altos cargos con la misma
* definir la filosofía respecto al acceso a los datos
* establecer responsabilidades inherentes al tema
* establecer la base para poder diseñar normas y procedimientos referidos a
  + Organización de la seguridad
  + Clasificación y control de los datos
  + Seguridad de las personas
  + Seguridad física y ambiental
  + Plan de contingencia
  + Prevención y detección de virus
  + Administración de los computadores

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concienciación.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

* Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
* Un procedimiento para administrar las actualizaciones
* Una estrategia de realización de copias de seguridad planificada adecuadamente
* Un plan de recuperación luego de un incidente
* Un sistema documentado actualizado

Por lo tanto y como resumen, la política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

**Conclusiones.**

Aprendimos que hay mecanismos para administrar dichas normas y actualizaciones en la planificación e implementación de software para redes e infraestructura, lo cual previene y recupera dichos incidentes a ocurrir lo cual mantiene de una forma correcta de mantener el grupo de trabajo uniformemente estable.