Introducción a SGSSI

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Introducción a SGSSI

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Indice

- ¿Qué es la seguridad informática?
- ¿Quién se encarga?
- Análisis de riesgos
- Principios de seguridad

¿Qué es la seguridad informática?

Bienes / activos: aquello que se desea proteger (Datos, software, hardware, infraestructura, personal, información, etc.)

Riesgos / amenazas: posibilidad de que algún bien sufra daños o desaparezca (Robo, modificación, suplantación, interceptación, etc.)

¿Qué es la seguridad informática?

Todas las acciones que se toman para asegurar que:

- Los bienes / servicios son usados como se debe
- Los bienes / servicios sólo dan acceso a quien tiene permiso para ello
- Los bienes / servicios cumplen la legislación vigente

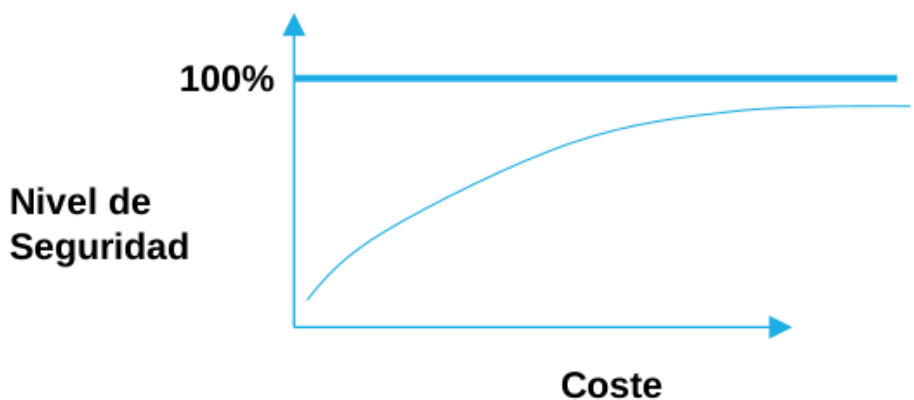
¿Qué es la seguridad informática?

Objetivos:

- Detectar los riesgos y amenazas para evitar que se produzcan o minimizar su efecto
- Garantizar el uso adecuado de los bienes
- Limitar las posibles pérdidas y asegurar la recuperación del sistema lo antes posible
- Cumplir la legislación correspondiente

¿Qué es la seguridad informática?

Es imposible lograr el 100% de seguridad: la seguridad es un proceso, no un estado



¿Quién se encarga?

- Administración de seguridad
- Dirección
- Usuarios

¿Quién se encarga?

Administración de seguridad:

- Responsable de identificar bienes a proteger y riesgos
- Realiza el plan de seguridad y lo implementa

¿Quién se encarga?

Dirección:

- La seguridad debe ser un objetivo estratégico
- Hay que invertir dinero
- Organizar el departamento de seguridad

¿Quién se encarga?

Usuarios:

- Deben recibir formación
- Deben conocer la política de seguridad de la empresa
- Deben involucrarse en la seguridad
- Deben conocer la legislación

Análisis de riesgos

Identificar los bienes a proteger

Estimar el valor (V) de esos bienes

Identificar las amenazas que sufren dichos bienes

Estimar la probabilidad (P) de que esas amenazas realmente se produzcan

Análisis de riesgos

Analizar las medidas necesarias para eliminar esas amenazas

Estimar el coste (C) de implantar esas medidas

C < P * V (Cuando el coste es menor que la probabilidad multiplicada por el valor, aplicar las medidas)

Principios de seguridad

- **C**onfidencialidad
- **I**ntegridad
- **D**isponibilidad
- **A**utenticidad
- **N**o repudio

Confidencialidad

Se garantiza que la información transmitida o almacenada en un sistema informático sólo podrá ser leída por su legítimo destinatario

Si dicha información cae en manos de terceras personas no podrán acceder al contenido original

Integridad

Se garantiza que la información no ha sido modificada desde su creación o durante su transmisión

Permite detectar si se ha añadido, modificado o eliminado parte de la información almacenada, procesada o transmitida

Disponibilidad

La información debe estar disponible para sus legítimos usuarios y propietarios

Se garantiza el correcto funcionamiento del sistema informático mediante un diseño suficientemente robusto frente a ataques e interferencias

Autenticidad

Se puede comprobar la identidad del usuario que crea o accede a la información

También se habla de autenticidad de un equipo que se conecta a una red o intenta acceder a un servicio

No repudio

Se demuestra la autoría de la información mediante un mecanismo probatorio que impida al usuario que la ha creado y enviado negar esta circunstancia

Se aplica la misma situación al destinatario de la información

Especialmente importante en transacciones comerciales

Noticias - que principio?