Seguridad en Tecnologías de la Información

Tema 2
Políticas y estándares de seguridad

Manuel J. Lucena López
mlucena@ujaen.es

Departamento de Informática
Universidad de Jaén

16 de septiembre de 2024

Índice

Políticas de seguridad

Estándares de seguridad

Introducción

- Es necesario definir y documentar las condiciones de seguridad en el funcionamiento de cualquier sistema.
- Tenemos que hacer una reflexión realista, que permita:
  - Minimizar las vulnerabilidades.
  - Reducir el tiempo desde la detección de un fallo o ataque, hasta su neutralización.

Es inútil...

- Ignorar los riesgos.
- Dedicar demasiados recursos a amenazas poco probables.
- Carecer de un plan de contingencias.

Definición de política de seguridad

Expectativas de seguridad:

Definen el funcionamiento esperado *real* de un sistema, teniendo en cuenta los posibles riesgos de seguridad.

Política de Seguridad:

- Resultado de documentar las expectativas de seguridad.
- Se estructuran como enunciados o reglas que especifican el funcionamiento correcto o esperado de una entidad (directivas, reglamentos, normas, prácticas, etc).
- Describen cómo una organización gestiona, protege y distribuye información.
- Existen a diferentes niveles, desde la descripción de los objetivos generales de seguridad de una organización, hasta la especificación de cómo debe llevarse a cabo una tarea concreta.

Ventajas del uso de políticas de seguridad

- Explican las intenciones y expectativas sobre la gestión de la seguridad.
  - Por ejemplo, una organización puede cambiar los controles de acceso, pero siempre se harán para evitar que usuarios externos accedan a la información.
- Fijan expectativas claras, para que los empleados tomen decisiones sobre seguridad de manera homogénea.
- Ayudan a cumplir requerimientos regulatorios y legales.
- Mejoran la eficiencia de la organización.

Tipos de políticas de seguridad

Aunque no hay un modelo universal, el NIST distingue tres tipos:

- **De programa:** definen la dirección estratégica sobre seguridad de una organización y asignan recursos para su implementación en la organización. También conocidas como políticas maestras.
- **Específicas:** especifican una guía más concreta para áreas relevantes o de interés para la organización.
  - Por ejemplo, una política de acceso remoto puede indicar que solo se pueda acceder a la red de la empresa a través de una VPN.
- **Del sistema:** especifican qué acciones están permitidas en un sistema en particular, como un cortafuegos, un servidor web o una computadora individual.
  - Son especialmente relevantes para los técnicos que mantienen esos sistemas.
  - Dos elementos: el objetivo de seguridad y las reglas operacionales.

Elementos que componen las políticas de seguridad

1. Propósito y objetivos claros.
2. Ámbito de aplicabilidad.
3. Compromiso de la dirección de la empresa.
4. Políticas realistas y aplicables (y exigibles).
5. Definición clara de los términos importantes.
6. Adaptadas a los niveles de riesgo deseados por la organización.
7. Actualizadas.

Índice

Políticas de seguridad

Estándares de seguridad

Los estándares de seguridad

Propósito y utilidad

- Proporcionan métodos sistemáticos, documentados y basados en objetivos claros, para gestionar la seguridad.
- Permiten evaluar los riesgos de forma metódica, e incorporan directrices sobre *buenas prácticas*.
- Si las políticas responden a las preguntas *¿qué?* y *¿por qué?*, los estándares responden a la pregunta *¿cómo?*
- Pueden obtenerse certificaciones empresariales basadas en los mismos.

El estándar ISO 27000

Origen e historia

- Tiene su origen en dos normas del *British Standards Institution*:
  - BS 7799-1 (guía de buenas prácticas, 1995).
  - BS 7799-2 (esquema de certificación, 1998).
- BS 7799-1 se convirtió en ISO 17799 en 2000.
- BS 7799-2 se convirtió en ISO 27001 en 2005.
- En 2007, ISO 17799 fue renombrada como ISO 27002:2005.
- En la actualidad, se compone de 35 documentos (27000 a 27019 y 27030 a 27044).
- Abarca todos los aspectos relevantes para la gestión de seguridad de una organización.

Otros estándares

- NIST serie 800: Desarrollado por el *National Institute of Standards and Technology* (EE.UU.).
- CobiT (Objetivos de control para tecnologías de la información y similares), del IT Governance Institute. Compatible con ISO 27002.
  - Se estructura en cuatro partes. La principal cubre 34 procesos de TI.
- UNE 71502:2004. Es la norma española certificable, basada en BS7799-2:2002. Anulada en favor de ISO 27001 en 2009.
- *COSO-Entreprise Risk Management /SOX*: Iniciativa del sector privado estadounidense, orientada al mundo financiero.
- ...