

CONTROL Y SEGURIDAD DE LOS SISTEMAS

TEMAS SEMANA 2:

- a) Administración y gestión de la seguridad.
- b) Arquitectura de los sistemas de gestión de la seguridad.
- c) Acceso a la información confidencial: técnicas.

- ¿A qué se refiere la administración y gestión de la seguridad?

Se refiere a implementar un Sistema de Gestión de la Seguridad de la Información (SGSI). ISMS es el concepto equivalente en idioma inglés, siglas Information Security Management System.

El SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

El SGSI (Sistema de Gestión de Seguridad de la Información) es el **concepto central sobre el que se construye ISO 27001**. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

- **¿Para qué sirve un sistema de gestión de la seguridad de la Información?**

Como sabemos la información, junto a los procesos y sistemas que hacen uso de ella, son activos más importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Hoy día las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria

CONTROL Y SEGURIDAD DE LOS SISTEMAS

o involuntariamente desde dentro de la propia organización o aquello provocados accidentalmente por catástrofes naturales y fallos técnicos.

Los que un SGSI es entonces una de las herramientas esenciales de gran utilidad y de importante ayuda para lograr que una adecuada gestión de la seguridad en las organizaciones. Ya que nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo.

En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad SGSI debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.



CONTROL Y SEGURIDAD DE LOS SISTEMAS

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

- ¿Cuál es la estructura de un sistema de gestión de la seguridad de la información?

Un Sistema de Gestión de la Seguridad de la Información está basado en ISO 27001 con la siguiente estructura:



Documentos de Nivel 1

Manual de seguridad: Por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Documentos de Nivel 2

Procedimientos: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- **Alcance del SGSI:** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas)
- **Política y objetivos de seguridad:** documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Procedimientos y mecanismos de control que soportan al SGSI:** aquellos procedimientos que regulan el propio funcionamiento del SGSI.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

- **Enfoque de evaluación de riesgos:** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables
- **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- **Plan de tratamiento de riesgos:** documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc
- **Procedimientos documentados:** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados
- **Registros:** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI
- **Declaración de aplicabilidad:** (SOA -Statement of Applicability-, en sus siglas inglesas aplicabilidad); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

- **Control de la documentación:** Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:
 - Aprobar documentos apropiados antes de su emisión.
 - Revisar y actualizar documentos cuando sea necesario y renovar su validez.
 - Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
 - Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
 - Garantizar que los documentos se mantienen legibles y fácilmente identificables.
 - Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
 - Garantizar que los documentos procedentes del exterior están identificados.
 - Garantizar que la distribución de documentos está controlada.
 - Prevenir la utilización de documentos obsoletos.
 - Aplicar la identificación
- **¿Cuáles son las técnicas de acceso más comunes que utilizan los carckers y cómo protegerte?**

A partir de un estudio reciente del 2017 la Universidad de California en Berkeley, y Google elaboraron un informe en el que se analizó, cuáles son las técnicas preferidas de los ciberdelincuentes a la hora de atacar a sus usuarios este es el resultado:

Phishing

Los autores del estudio identificaron 12,4 millones de credenciales cuentas que fueron robadas usando una técnica conocida como phishing

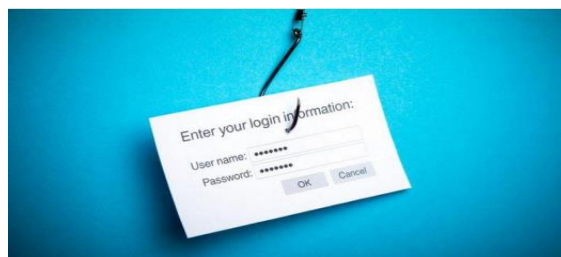
Ese término informático proviene del vocablo inglés que en español se traduce como "pescar" y se refiere al robo de identidad por parte de los estafadores para obtener datos personales de los usuarios.

El objetivo puede variar desde nombres de usuario y contraseñas, hasta datos bancarios y cuentas de acceso a otros servicios en línea.

Los "pescadores" acceden a la información usando mensajes falsos como "cebo" para sus víctimas, haciéndose pasar por otras personas o entidades a través de email, mensajes o llamadas telefónicas.

"Spear-phishing": la mujer a la que la engañaron para acceder a su información personal en internet y a la que pidieron sexo como recompensa.

"Una contraseña no es suficiente para acceder a Google, por eso hackers más sofisticados trataron de recabar datos sensibles que podríamos preguntar para verificar la autenticidad del usuario, como la dirección IP y localización, el número de teléfono o el modelo del dispositivo"



Keyloggers

La segunda amenaza son los keyloggers, un tipo de programas que **permiten registrar cada tecleo** que realizamos en la computadora **o todo lo que vemos a través de la pantalla** y lo envían a un servidor externo. Este tipo de estafa digital ocurre con frecuencia en lugares de conexión pública, como cibercafés. Suele formar parte de infecciones mayores a través de malware (programas maliciosos).

"Gracias a este programa, los delincuentes pueden robar un gran volumen de información confidencial sin que la víctima se percate de ello", explican en el blog de la empresa de seguridad informática rusa Kaspersky Lab.



Huecos o brechas de Seguridad

La tercera vía que usan los hackers, son las brechas de seguridad en servicios de terceros. En esos casos, los ciberdelincuentes **roban las bases de datos de una empresa.**

La compañía identificó **1.900 millones de datos** producto de estas fallas y comprobaron después si algunos de esos datos comercializados servían para acceder a cuentas de Gmail y otros de sus servicios.

Y concluyeron que el 7% de las víctimas de este tipo de robo de datos corrían el riesgo de que los ciberdelincuentes ingresaran en su cuenta de Google a través de este sistema.

CONTROL Y SEGURIDAD DE LOS SISTEMAS

Esto fue lo que le ocurrió a Yahoo en agosto de 2013, cuando sufrió un hackeo masivo, según reconoció a finales del año pasado.

¿Cómo protegerte?

- Los especialistas de seguridad de Google dicen que existen **nuevas alertas** para avisar de prácticas peligrosas para evitar que los usuarios hagan clic enlaces sospechosos.
- Préstales atención.
- También monitorean los intentos sospechosos de accesos a la cuenta desde otros dispositivos o ubicaciones diferentes de las habituales. Cuando eso ocurre, envían un mensaje para "verifiques" si eres tú. Esto permite la **"verificación en dos pasos"**, que reforzaría la seguridad.
- Otra opción es **denunciar** las cuentas sospechosas a través de Gmail para prevenir más daños.
- Puedes usar una herramienta de Chrome llamada **Smart Lock** para gestionar las contraseñas.