



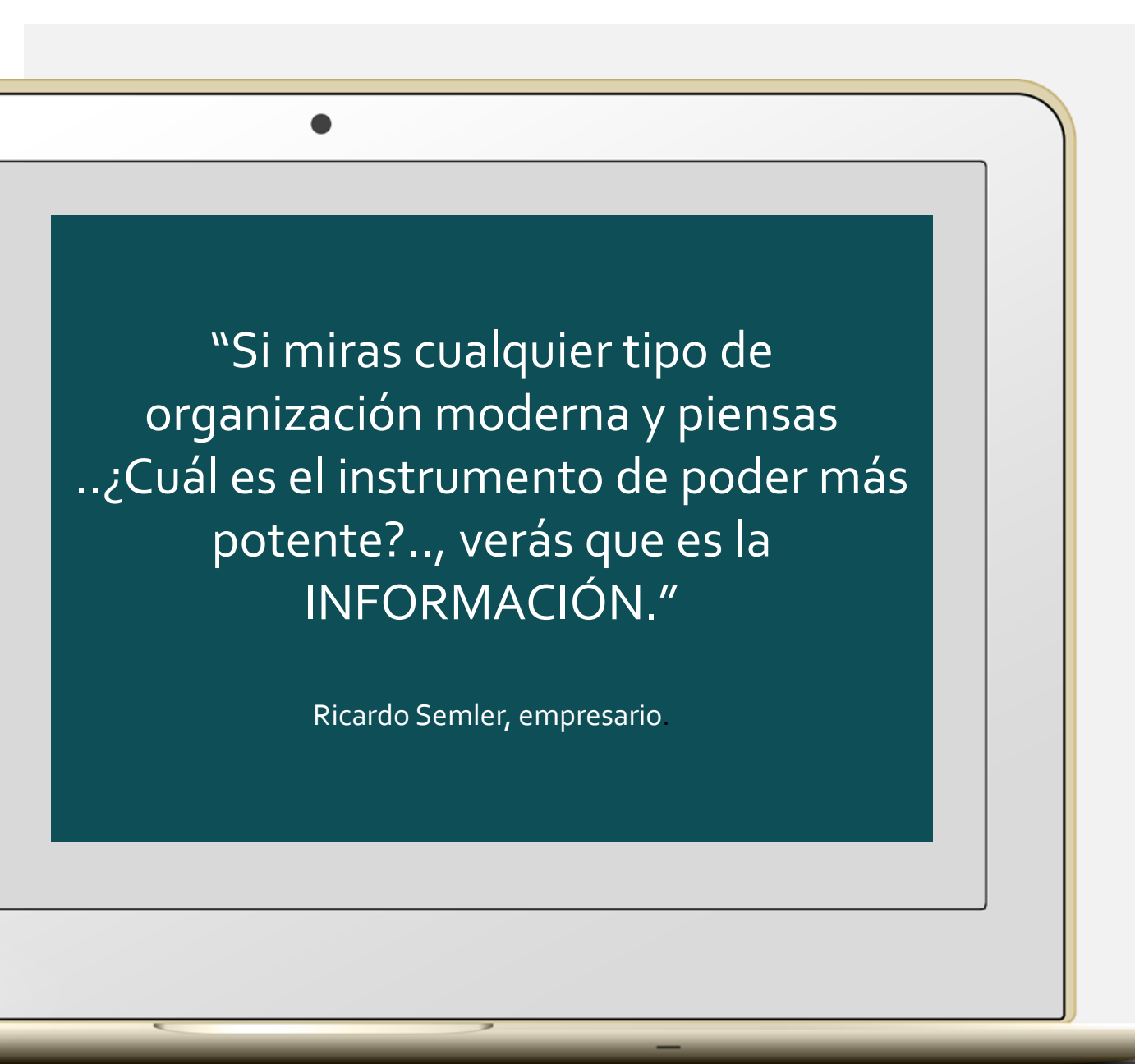
Auditoría de Sistemas Informáticos

La tecnología informática se ha convertido en una FUENTE generadora de valor y ventajas competitivas



Educación(e-leaming),
Gobierno (e-goverment),
Comercio (e-commerce),
Servicios financieros (e-banking),
Salud (e-health), etc.



A laptop with a gold-colored bezel is shown from a slightly elevated angle. The screen displays a quote on a dark teal background. The quote is in white text and reads: "Si miras cualquier tipo de organización moderna y piensas ..¿Cuál es el instrumento de poder más potente?.., verás que es la INFORMACIÓN." Below the quote, in a smaller font, is the attribution "Ricardo Semler, empresario.".

“Si miras cualquier tipo de
organización moderna y piensas
..¿Cuál es el instrumento de poder más
potente?.., verás que es la
INFORMACIÓN.”

Ricardo Semler, empresario.

A close-up, dark-toned image of a person's hand typing on a laptop keyboard. The laptop screen is visible in the background, showing some text and images. The overall lighting is dim, creating a professional and focused atmosphere.

Importancia de la
INFORMACIÓN



AMENAZAS

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información.

- Las amenazas pueden ser causadas por:
- Usuarios
- Programas maliciosos
- Errores de programación
- Intrusos
- Un siniestro
- Personal técnico interno
- Fallos electrónicos o lógicos de los sistemas informáticos en general.
- Catástrofes naturales





POR EL ORIGEN

INTERNAS

EXTERNAS



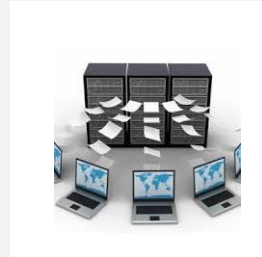
POR EL EFECTO

Robo y/o Destrucción
de información.

Caída del sistema.

Suplantación de la
identidad, publicidad
de datos personales o
confidenciales,

Cambio de
información, venta de
datos personales, etc



POR MEDIOS UTILIZADOS

Virus Informático

Ingeniería Social

Denegación del
Servicio

TIPOS DE AMENAZAS

- Malware o código malicioso: comúnmente conocido como virus informático mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para asaltar dispositivos, configuraciones o componentes específicos de la red.
- Ingeniería social: Utilizan técnicas de persuasión que aprovechan falta de precaución de la víctima para obtener información sensible o confidencial.
- APT o Amenazas Persistentes Avanzadas: son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados.
- Suplantación de identidad: La más conocidas son la suplantación de IP, de ARP, de DNS, suplantación web, de correo electrónico e incluso de redes sociales.

Amenazas por el medio utilizado

Se clasifican con respecto al modus operandi del atacante:



QUE ES UNA AUDITORIA

AUDITORIA DE SISTEMAS
COMPUTACIONALES

AUDITORIA

Es el examen profesional, objetivo e independiente, de las operaciones de una empresa (financieras, administrativas, etc.) mediante procedimientos predefinidos.

Cuyo producto final es un informe conteniendo una opinión sobre la información auditada, así como conclusiones y recomendaciones, que tienden a promover la eficiencia y eficacia de la organización, sin perjuicio de verificar el cumplimiento de las leyes y regulaciones aplicables.



Tipos: financiera, de gestión, administrativa, informática, etc.

AUDITORIA INFORMÁTICA

Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.



OBJETIVOS DE UNA AUDITORIA

El objetivo de la Auditoría a la Seguridad Informática es detectar fisuras o puntos vulnerables en el sistema informático que pongan en riesgo la seguridad de la información y de las tecnologías empleadas para su procesamiento, como base para la elaboración de un diagnóstico.



Funciones de una Auditoría de Sistemas Computacionales



Analizar las políticas de Seguridad Informática adoptadas en la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información que en ella se procesa.



Analizar y comprobar el funcionamiento y eficacia del Sistema de Medidas de Seguridad Informática implantado en la entidad.



Detectar fisuras o puntos vulnerables en el funcionamiento del Sistema Informático y el Sistema de Medidas de Seguridad que puedan propiciar causas y condiciones para la comisión de delitos.

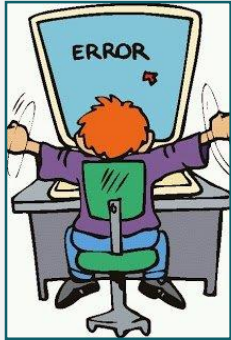


Valorar la factibilidad del Sistema de Medidas de Seguridad, en correspondencia con la caracterización del Sistema Informático.



Destinatarios de la Auditoría

Síntomas de necesidad de Auditoría en una organización



Descoordinación y desorganización:

No coinciden los objetivos de la Informática de la Compañía
Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.



Debilidades económico-financiero:

Incremento desmesurado de costes.
Desviaciones Presupuestarias significativas.
Costes y plazos de nuevos proyectos



Mala imagen e insatisfacción de los usuarios:

No se atienden las peticiones de cambios de los usuarios
No se reparan las averías de Hardware o Software
No se cumplen los plazos de entrega de resultados periódicos.
Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario



Síntomas de Inseguridad:

Seguridad Lógica
Seguridad Física
Confidencialidad Discontinuidad del Servicio.
Centro de Proceso de Datos fuera de control.