

Ingeniería en Sistemas de Información

Ciberseguridad

Docente: Ing. Gabriela Nicolao

Ayudantes: Ing. Luciano Sebastianelli, Matías
Baghdassarian



Auditoría



Introducción Auditoría

- ▶ Es un control selectivo.
- ▶ Lo compone un grupo independiente del proceso a auditar.
- ▶ Busca lograr los objetivos propuestos.
- ▶ Debe evaluar la eficiencia y eficacia de los sectores.
- ▶ Se obtienen evidencias para para el respaldo de las afirmaciones.
- ▶ Proponen cursos de acción alternativos.



- ▶ Es la revisión y evaluación de los controles, sistemas y procedimientos de la informática.
- ▶ Participa del procesamiento de datos, con el fin de establecer cursos alternativos de acción que permitan obtener información en forma segura, confiable y eficiente para la toma de decisiones.
- ▶ Se basa sobre la integridad y la confidencialidad de la información.



Consideraciones para el auditor

- ▶ El informe del auditor no es asegurador y no es garantía.
- ▶ El auditor debe tener en cuenta que pueden existir errores o irregularidades en el sistema de control. Es por eso que el auditor debe analizar, evaluar y considerar los riesgos de auditoría.
 - Los riesgos de auditoría representan la posibilidad de emitir un informe de auditoría incorrecto por no haber detectado errores o irregularidades. Los riesgos de auditoría disminuyen a medida que obtengo evidencias.

Clasificación de los riesgos de Auditoría



Riesgos Inherentes

- ▶ Son errores o irregularidades significativos antes de considerar los sistemas de control.
- ▶ Son riesgos por fuera del control del por parte del auditor.



Riesgos de Control

- ▶ Se refieren a la incapacidad de detectar errores o irregularidades significativos por parte de los sistemas de control.



Riesgos de Detección

- ▶ Es el riesgo que los procesos de auditoría seleccionados no detecten errores o irregularidades.



1. Identificar las afirmaciones a ser evaluadas.
2. Evaluar la importancia de las afirmaciones.
3. Reunir la información o evidencia necesaria.
4. Analizar y Evaluar la evidencia.
5. Formular un informe.

Tipos de Auditoría

Externa

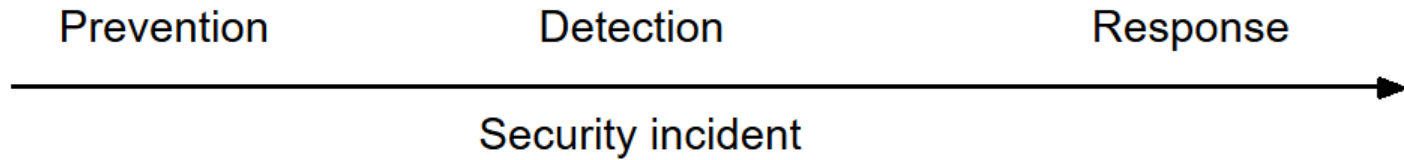
Interna



SOX – Sarbanes Oxley



Sarbanes Oxley



- Hay distintos tipos de fraudes que sucedieron en los años 2000 y que pueden ser prevenidos con SOX, por ejemplo modificación de informes financieros como:
 - Obtener aumentos de sueldos o bonos.
 - Obtener aprobaciones de bancos para financiamiento.
 - Cumplir las expectativas de accionistas.



El organismo Security and Exchange Commission (SEC) detectó ganancias inapropiadas, valuaciones de activos inapropiadas, entradas fraudulentas, etc. y tomó acciones en contra de esas organizaciones.

Enron Corporation, Tyco International plc, Adelphia, WorldCom.

Controles internos de la auditoría SOX

Accesos: Se refiere a los controles físicos y lógicos que previenen el acceso no autorizado a usuarios de información sensible.

Seguridad: Significa estar seguro de aplicar los controles para prevenir ataques y contar con las herramientas para solucionar los incidentes que hayan ocurrido.

Administración del cambio: Involucra el agregado de nuevos usuarios, equipos, sistemas y cualquier cambio en otros componentes donde esta almacenada la información.

Procedimientos de Backup: Los sistemas de backup deben ser realizados y probados periódicamente.





GDPR General Data Protection Regulation



Introducción GDPR

¿Quién?

Union Europea.

¿Qué?

Protege los datos de los ciudadanos y residentes Europeos.

¿Dónde?

En cualquier lugar donde haya datos de personas pertenecientes a la Unión Europea.

¿Cuándo?

Aplicable a partir del 25 de mayo del 2018.

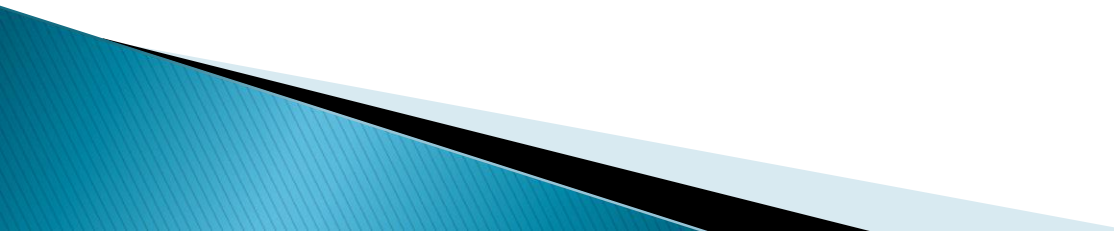


Alcance

Cualquier información que pueda ser usada para identificar un individuo de manera directa o indirecta. Esto puede ser datos de clientes, proveedores, empleados, stakeholders, etc.

Personal	Identificadores	Financiera	Salud
Nombre Edad Email Afiliación religiosa Datos biométricos	Cuentas bancarias Numero de tarjeta de créditos Identificador del país (DNI, SSN, etc.) Número de licencia de conducir	Balances contables Información de salario Pago de impuestos	Información de salud Características físicas Resultados de exámenes médicos Evaluaciones de salud mental Pago por cuidados de la salud

Requerimientos de GDPR

- Evidencia y cumplimiento.
 - Seguridad Integral.
 - Pseudonimización y cifrado de datos personales.
 - Protección de datos por diseño y por defecto.
 - Control de acceso a usuarios.
 - Registros de auditoría.
- 

PREGUNTAS?

