UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA Y CONTROL DE SISTEMAS

UNIVERSIDAD DE LIMA

FACULTAD DE INGENIERÍA Y ARQUITECTURA
CARRERA DE INGENIERÍA DE SISTEMAS

AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD DE DATOS, CIBERSEGURIDAD Y AFINES

AUDITORÍA Y CONTROL DE SISTEMAS

AGENDA

- Conceptos generales
- Auditoría de seguridad
- Auditoría de privacidad
- Auditoría de ciberseguridad
- Ejecución de auditorías
- Referencias

UNIVERSIDAD DE LIMA

60 años

CONCEPTOS GENERALES

Introducción

- ✓ Es indispensable no confundir términos
  - Seguridad de la información no es igual al Gobierno de seguridad de la información
  - Seguridad y ciberseguridad no son lo mismo
  - Privacidad de datos implica un tipo de datos en particular
- ✓ El auditor tiene que saber diferenciar estos conceptos para no confundir el alcance respectivo de las auditorías.

Introducción

- ✓ Conocer la regulación en estos tipos de auditorías también es vital porque muchos de los criterios de la auditoría van a estar basados en verificar que se esté cumpliendo dicha regulación:
  - ✓ Sobre privacidad de datos personales
  - ✓ Delitos informáticos
  - ✓ Sistemas de gestión de seguridad de la información, etc.

Definiciones

- **Seguridad de la información:**

✓ Proceso mediante el cual se buscar proteger de peligros y daños, accidentales o provocados a todos los **activos de información de la organización procurando salvaguardar la confidencialidad, integridad y disponibilidad de los mismos(ISACA, 2019).**

✓ **Activo de información:** todo aquel activo que cree, manipule o contenga información en cualquier formato (físico o digital)

✓ **Ciberseguridad:**

❑ Cuando se hace referencia exclusiva a los activos e información **en formato digital** y cuando **el ataque es de naturaleza digital.**

Definiciones

- **Privacidad de datos**

✓ Procedimientos que permitan proteger toda información que identifique, **de manera inequívoca,** a una persona natural (ISO, 2019).

UNIVERSIDAD DE LIMA | 60 años

AUDITORÍA DE SEGURIDAD, PRIVACIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN

Auditoría de Seguridad, Privacidad y Ciberseguridad.

Definición

- Este proceso **recolecta y evalúa la evidencia para determinar**:
  - ✓ **Si los activos de información y la información misma, se encuentra convenientemente protegidos.**
  - ✓ **Si la información personal se encuentra conveniente protegida, de acuerdo a la regulación vigente.**
  - ✓ **Si la infraestructura de TI se encuentra suficientemente preparada para hacer frente a un ciberataque.**
- Considerar **que pueden ser 3 auditorías diferentes y que no necesariamente tienen que realizarse juntas.**

Criterios comúnmente utilizados

- **SI = Seguridad de la información**
- Controles (todos o algunos en particular) de seguridad de la información funcionan de manera adecuada a nivel de:
  - Procesos
  - Información
  - Sistemas e infraestructura de TI
- Segregación de funciones del personal a todo nivel para preservar la SI
- Protección de los datos personales que maneje la organización.
- Regulación relacionada con SI que afecte a la empresa a nivel de:
  - Leyes
  - Contratos con clientes y proveedores

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:

- Políticas, procedimientos y demás documentación relativa a seguridad de la información.
  - ✓ Organización de la Seguridad de la Información.
  - ✓ Seguridad de los Recursos Humanos
  - ✓ Gestión de los Activos.
  - ✓ Control de Accesos.
  - ✓ Cifrado.
  - ✓ Seguridad Física y Ambiental.
  - ✓ Seguridad de las Operaciones.
  - ✓ Seguridad de las Comunicaciones.
  - ✓ Adquisición de sistemas, desarrollo y mantenimiento
  - ✓ Relaciones y obligaciones de seguridad con los Proveedores.
  - ✓ Gestión de Incidencias

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:
- Controles específicos de seguridad sobre:
  - ✓ Organización de la Seguridad de la Información.
  - ✓ Seguridad de los Recursos Humanos
  - ✓ Gestión de los Activos.
  - ✓ Accesos.
  - ✓ Cifrado.
  - ✓ Seguridad Física y Ambiental.
  - ✓ Seguridad de las Operaciones.
  - ✓ Seguridad de las Comunicaciones.
  - ✓ Adquisición de sistemas, desarrollo y mantenimiento
  - ✓ Relaciones y obligaciones de seguridad con los Proveedores.
  - ✓ Gestión de Incidencias
  - ✓ Privacidad de datos personales

Fuentes de evidencia

- El equipo auditor encontrará evidencias revisando:

- Cumplimiento regulatorio
  - ✓ Contratos
  - ✓ Leyes relacionadas y a las que está sujeta la organización.
- Exámenes particulares tipo
  - ✓ Ethical hacking
  - ✓ Penetration test
  - ✓ Análisis de vulnerabilidades
  - ✓ Análisis de puertos

Resultados esperados habituales

- La organización que conduce una auditoría de seguridad normalmente pretende encontrar como resultados lo siguiente:

- Correcto / incorrecto funcionamiento de los controles de seguridad
- Cumplimiento / incumplimiento de alguna regulación relacionada con seguridad de la información.
- Calidad del desempeño del proveedor en aspectos relacionados con seguridad.

Referencias bibliográficas

- [ISACA, 2018] ISACA International. Certified Information Systems Auditor (CISA) Exam Preparation Guide. ISACA Publishing, USA (2018).
- ISACA, 2019] ISACA International. COBIT 2019 Framework. ISACA Publishing, USA (2019).
- [ISO, 2019] ISO International. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. ISO Publishing, Suiza (2019)

¿Consultas?

UNIVERSIDAD DE LIMA | 60 años

AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN, PRIVACIDAD DE DATOS, CIBERSEGURIDAD Y AFINES