
Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Gobernanza de la SI

Introducción

La gobernanza de la seguridad de la información se define como un subconjunto de la gobernanza empresarial que proporciona dirección estratégica y que garantiza que se alcancen los objetivos.

Su propósito es garantizar que las actividades de la organización estén alineadas de manera que respalden los objetivos comerciales de la organización.

Explicación

La seguridad de la información deberá realizarse apegada a la norma NIST SP 800-59.

Se deben aplicar los conceptos de confidencialidad, integridad y disponibilidad (tríada CIA, por sus siglas en inglés).

Confidencialidad

Proteger los datos de las vistas no autorizadas

Integridad

Proteger los datos de modificaciones no autorizadas

Disponibilidad

Garantizar que se puede acceder a los datos de la manera autorizada

Explicación

Los términos básicos de seguridad son los siguientes:

- Necesidad de saber
- Privilegio mínimo
- Separación de funciones
- Rotación de trabajo
- Atención debida
- Debida diligencia

Explicación

Actividad

Muchas de las organizaciones no realizan apropiadamente la fase de destruir la información cuando esta ya no es útil o por norma se debe eliminar.

Investiga técnicas de borrado seguro para conocerlas y aplicarlas cuando sea necesario en tu ámbito laboral.

Cierre

La gobernanza de seguridad son procesos, roles y políticas específicas que establece una organización a efecto de mejorar los esfuerzos en materia de seguridad.

Es importante determinar el impacto que un daño puede causar derivado de una amenaza que se detona en una o más vulnerabilidades en los activos de TI.

El ciclo de vida de los datos es parte de la gobernanza de seguridad junto con las funciones y responsabilidades de seguridad.


Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Riesgos de SI

Introducción

Es importante comprender y, sobre todo, no ignorar los riesgos que existen en las organizaciones, ya que en caso de algún incidente este puede provocar pérdidas monetarias, de activos e incluso de personas.

Por ello, es crucial tener un inventario de todos los activos de TI y determinar las vulnerabilidades que pueden tener ante las diversas amenazas en cada uno de ellos.

La administración de riesgos es una función imprescindible del Administrador de Seguridad de la Información.

Explicación

Riesgos:

- Financiero
- Económico
- Competitivo
- Ti

01

Identificación
¿Dónde y cuándo?

02

Análisis
¿Qué tan grave?

03

Evaluación
¿Nivel aceptable?

04

Tratamiento
¿Qué hacer?

Explicación

Marco de gestión de riesgos

Explicación

Marco de gestión del riesgo

Desarrollo de prioridades y objetivos
Establecer metas y objetivos

Definición de la tolerancia al riesgo
Establecer nivel de riesgo a aceptar

Definir el apetito por el riesgo de la organización
Documentar el apetito

Explicación

Proceso de gestión del riesgo

Actividad

Identifica las principales amenazas que hay en tu centro actual de trabajo, de cada uno de los activos de TI con los que cuenta la empresa.

Posteriormente, revisa los controles que hay para mitigar esas amenazas y, de no existir, propón aquellos que puedan reducir los posibles riesgos que se lleguen a presentar.

Cierre

La gestión de riesgos identifica, documenta y examina los activos de TI de la organización para establecer las estrategias de seguridad y realizar la evaluación del riesgo para decidir su tratamiento: aceptar, ignorar, delegar o mitigar el riesgo.