
Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Diseño e implementación de controles y políticas de seguridad

Introducción

Es importante no ignorar y, sobre todo, comprender que los riesgos que existen en las organizaciones pueden detonarse ocasionando algún incidente que provoque 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 que existan.

La administración de riesgos es una función imprescindible del administrador de seguridad de la información.

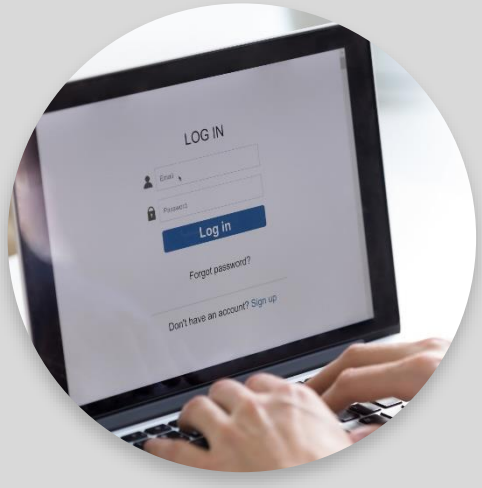
Explicación

Control de acceso

Explicación

Tipos de controles de acceso

Físicos
Controlan el acceso a los recursos físicos (edificios, estacionamientos y áreas protegidas, entre otros)



Lógicos
Controlan el acceso a los intangibles de TI (red, sistema informático, mediante usuario y contraseña)

Explicación

Control de acceso	Autorización	Contraseña
Identificación	Privilegios por usuario	Requisitos claros
Autenticación	Membresía de grupos	Complejidad
Autorización	Grados de autoridad	Mejores prácticas
Responsabilidad		

Actividad

Revisa la lista de requisitos de contraseña sugeridos y verifica si se aplican en cada una de las contraseñas que manejas.

Realiza una matriz binaria que distinga fácilmente si se aplica o no cada requisito.

Requisito	Contraseña 1	Contraseña 2	Contraseña 3
Al menos ocho caracteres alfanuméricos	✗	✓	✗
Combinación de letras mayúsculas y minúsculas y números	✓	✓	✗
Al menos un carácter especial dentro de los primeros siete caracteres	✗	✓	✓
Una letra o símbolo no numérico en el primer y último carácter	✗	✗	✓
No deben contener el nombre de usuario	✗	✓	✗

Cierre

El administrador de seguridad de la información debe garantizar que existan controles de acceso, así como políticas para el mismo; de la misma manera, debe monitorear que existan, funcionen y sean útiles.


Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Modelos de seguridad de información

Introducción

El uso de mejores prácticas ayuda a obtener mejores resultados, reduce los posibles errores que puedan presentarse y se entregan mejores productos y/o servicios a los clientes, fortaleciendo así a las empresas que deciden aplicarlas.

En este módulo conocerás un marco de referencia que modela la seguridad de la información y la privacidad, e involucra la gestión del riesgo de la ciberseguridad.

Explicación

Marco de referencia NIST de ciberseguridad 1.1

- Creado en 2014 en los Estados Unidos.
- Es neutral.
- Contiene variedad de estándares, directrices y prácticas.
- Proporciona una taxonomía y un mecanismo común.

Explicación

Descripción general del Marco NIST

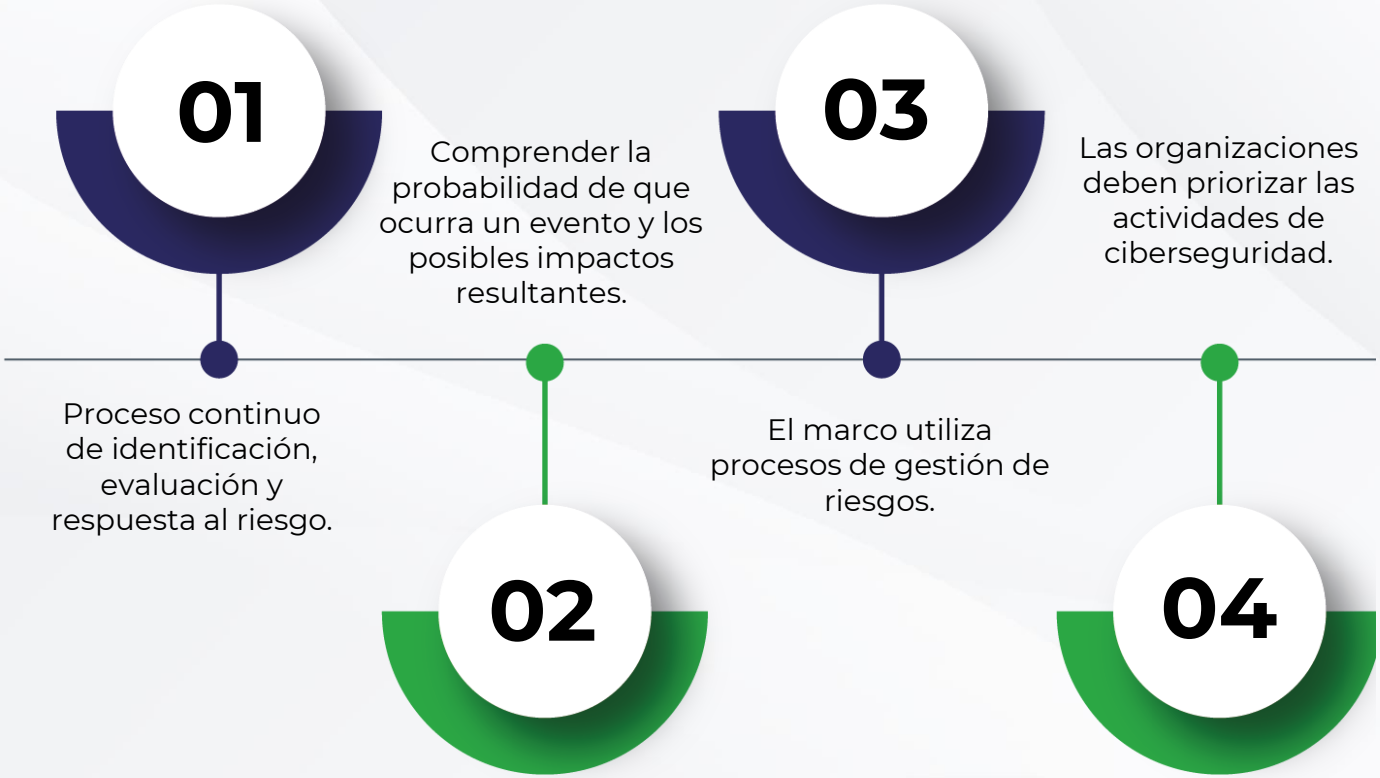
- El Framework Core: conjunto de actividades de ciberseguridad.
- Los niveles: contexto sobre cómo una organización ve el riesgo de ciberseguridad.
- El perfil: representa los resultados basados en las necesidades comerciales de una organización.

NIST Cybersecurity Framework				
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security & Continuous Monitoring	Communications	Improvements
Governace	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Processes &Procedures		Mitigation	
	Maintenance		Improvements	

Functions Categories

Explicación

Gestión de riesgos y marco de ciberseguridad



Actividad

Realiza un breve cuadro sinóptico del marco de referencia NIST que considere las funciones y las categorías, incluyendo una descripción resumida de cada una de ellas.

Cierre

La gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo.

El marco de referencia de NIST es adaptable para proporcionar una implementación flexible y basada en riesgos.

El marco gestiona el riesgo de ciberseguridad y se compone de tres partes: