
Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Aplicaciones

Introducción

La seguridad de las aplicaciones no solo debe enfocarse en el desarrollo de las mismas, sino hasta su implementación.

En este tema se darán a conocer herramientas para proteger las aplicaciones con las que cuenta una empresa, las cuales van desde bloquear cambios de codificación hasta evaluar amenazas de codificación inadvertidas, evaluar opciones de cifrado y auditar permisos y derechos de acceso.

Explicación

Importancia de la seguridad de aplicaciones

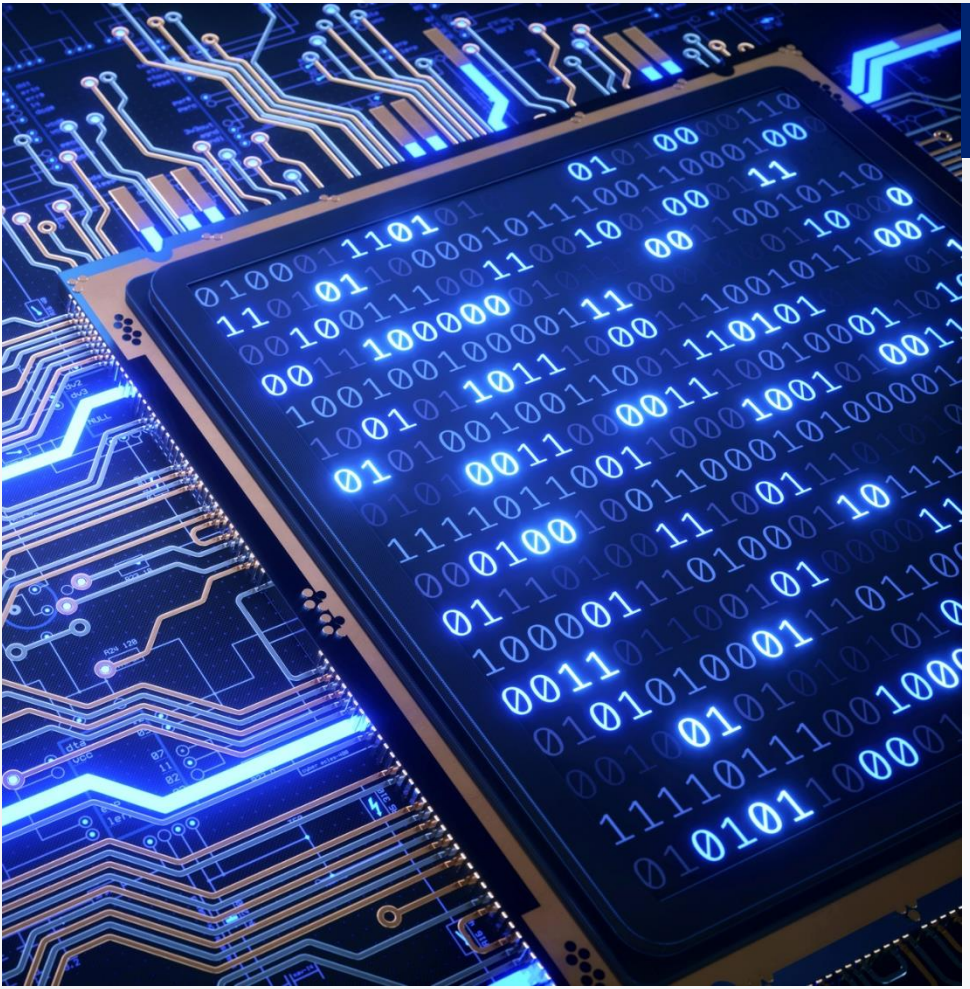
El State of Software Security informó que el 83% de 85,000 aplicaciones presentan al menos una falla.

El desarrollo de software debe ser rápido y pronto.

Las herramientas de seguridad tienen que funcionar con las nuevas técnicas de desarrollo.

> Deben ir más allá de identificar errores comunes de seguridad en el desarrollo de aplicaciones y protegerse contra técnicas de ataque comunes“ (Garner, 2020)

Explicación



Debilidades de software más comunes

10 vulnerabilidades CWE en el top 25 de CWE 2020 de MITRE

1. Script entre sitios
2. Escritura fuera de límites
3. Validación de entrada incorrecta
4. Lectura fuera de límites
5. Restricción inadecuada de operaciones dentro de los límites de un búfer de memoria
6. Inyección SQL
7. Exposición de información sensible a un actor no autorizado
8. Usar después de gratis
9. Falsificación de solicitudes entre sitios (CSRF)
10. Inyección de comandos del sistema operativo

Explicación

Actividad

Universidad Tecmilenio

Investiga a que área de las 10 vulnerabilidades más comunes y completa la siguiente tabla (se indican tres ejemplos para mayor claridad de lo solicitado).

Vulnerabilidad	Área
Script entre sitios	Servidores web
Escritura fuera de límites	
Validación de entrada incorrecta	
Lectura fuera de límites	
Restricción inadecuada de operaciones dentro de los límites de un búfer de memoria	
Inyección SQL	Base de datos
Exposición de información sensible a un actor no autorizado	
Usar después de gratis	
Falsificación de solicitudes entre sitios (CSRF)	Servidores web
Inyección de comandos del sistema operativo	

Cierre

Hoy en día, las aplicaciones enfocadas a la comunicación social, como las redes sociales y las compras por Internet, son el blanco preferido por los ciberdelincuentes para realizar fraudes o, en su defecto, obtener información.

De aquí la importancia de conocer las 10 vulnerabilidades más comunes en las aplicaciones para tomar medidas preventivas y, de ser necesario, correctivas, para generar el documento de “lecciones aprendidas” y que no se vuelvan a presentar.


Universidad
Tecmilenio®

Universidad Tecmilenio

Seguridad de Bases de Datos

Seguridad en la nube/dispositivos móviles y redes sociales

Introducción

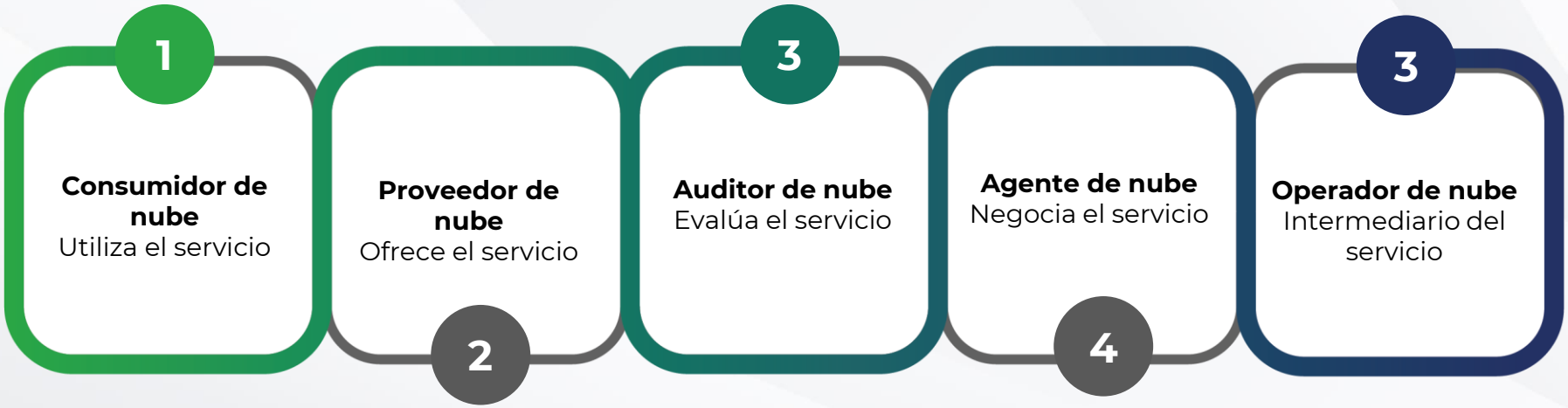
Gracias a la versatilidad del Internet y a las redes de servidores remotos, podemos contar con un servicio potente, cómodo y muy accesible: el servicio en la nube.

El servicio en la nube no es ajeno a sufrir problemas de seguridad, por lo tanto, se deben considerar las preocupaciones de seguridad para mejorar la garantía de la seguridad requerida para los clientes de la nube.

Explicación

Seguridad de cómputo en la nube

NIST define cinco actores principales:



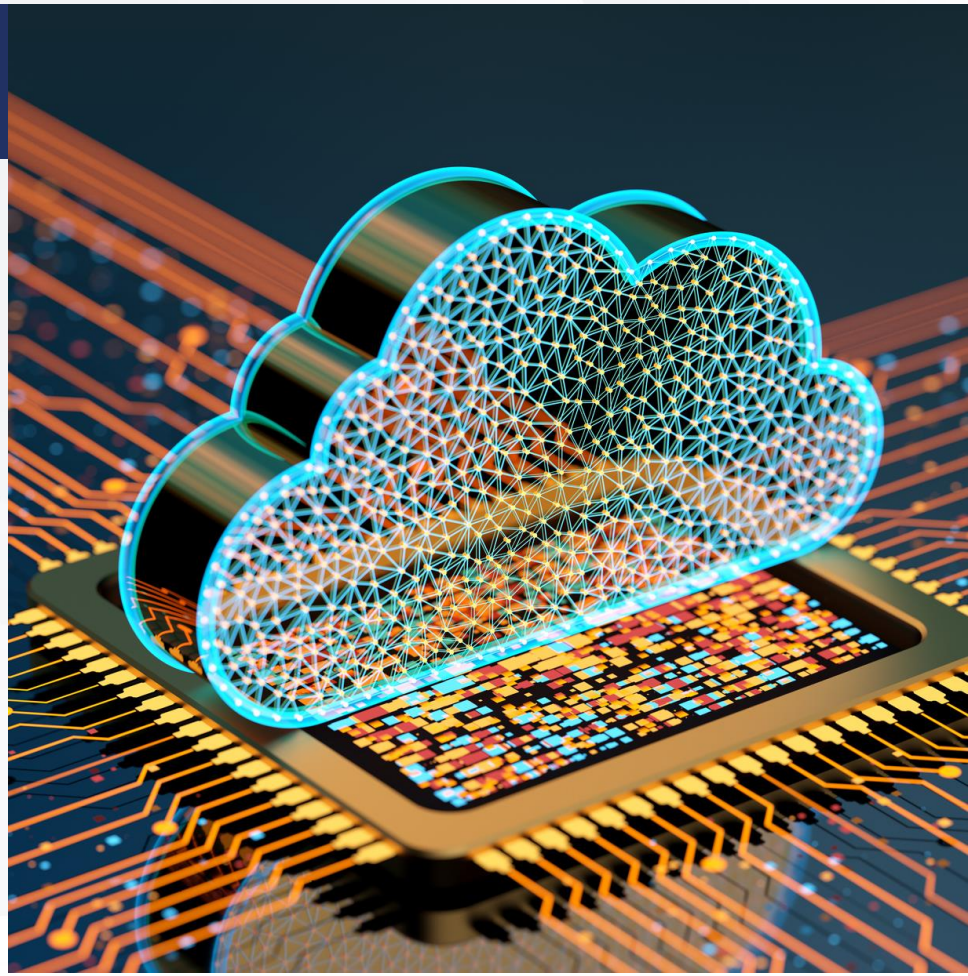
Explicación

Modelos de implementación

Nube pública
La organización ofrece varios servicios al público

Nube privada
Dedicada totalmente a los usuarios de la organización

Nube híbrida
Combinación de pública y privada



Explicación

Las empresas pueden tener políticas sobre cómo permitir que las personas usen sus propios dispositivos en las redes empresariales.

Ataques a dispositivos móviles

- Procesador diferente
- Los ataques de phishing
- El malware
- El software malicioso
- La mala programación
- Utilizar mecanismos de cifrado incorrectos
- Manejo inadecuado de los datos

Solo necesita estar cerca de la víctima

Bluetooth

Le permite trabajar en el aire en lugar de hacer algo físicamente.

BYOD

Es importante tener en cuenta que un dispositivo móvil:

- Puede actuar como vector de transmisión de virus.
- Puede usarse para eliminar material sensible fuera del sitio.
- Puede usarse como parte de un ataque Bluetooth.

Explicación

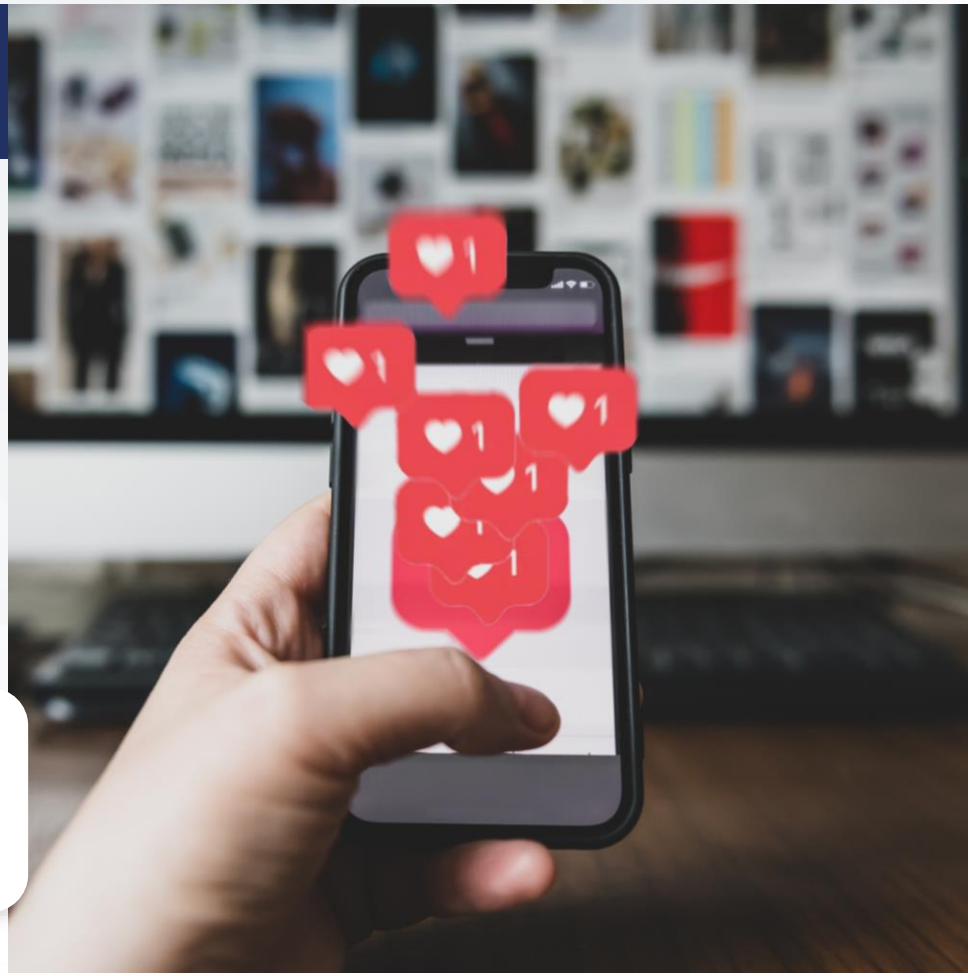
Reducir el impacto de la ingeniería social:

01 Empleados educados en los conceptos básicos de un entorno seguro.

02 Desarrollar una política de seguridad y una política de uso de la computadora.

03 Hacer cumplir una política estricta para los procedimientos de apoyo técnico interno y externo.

Prohibir que los empleados compartan fotos en sus redes sociales que comprometan el interior de las oficinas, áreas operativas y de infraestructura de TI.



Actividad

Busca en Internet proveedores de nube en la ciudad donde vives o en una zona metropolitana cercana.

De acuerdo a lo investigado, clasifica si el servicio que ofrecen es del tipo Iaas, PaaS o Saas.

Cierre

Para la seguridad del cómputo en la nube se deben involucrar a los cinco actores principales:

- Consumidor
- Proveedor
- Auditor
- Agente
- Operador.

Los dispositivos móviles son muy prácticos, pero también son muy vulnerables, entre ellos, se presenta el robo de datos confidenciales y el ataque interno entre dispositivos de la misma red.

La técnica de engaño más utilizada en las redes sociales es la ingeniería social, con la que obtienen acceso a los recursos de TI.