

Seguridad en el Desarrollo de Aplicaciones

¿Qué es la seguridad de la Información?

“La seguridad de la información se podría definir como aquellos **procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada**. Esta definición básicamente significa que debemos proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos”

ISO/IEC (International Organization for Standardization & International Electrotechnical Commission) 2016



Objetivos a garantizar

🕒 Integridad

La información debe ser la correcta acorde a su manejo dentro de la organización

🕒 Confidencialidad

La información debe ser accedida únicamente por las personas o instituciones autorizadas

🕒 Disponibilidad

La información debe poder ser accedida en todo momento por las personas autorizadas



Riesgos y afectaciones en México



En el 2022 se tuvo a nivel mundial un total de 1.802 millones de ataques a nivel mundial. En lo que refiere a américa latina como principales países bajo ataque se encuentran Brasil en primer lugar y en segundo a México con un total de 14.000 millones de ataques



Hasta agosto de 2023, se reportaron afectaciones a instituciones bancarias, de acuerdo con información del Banco de México (Banxico), por más de 67.61 millones de pesos. Tres de estos incidentes fueron sufridos por instituciones bancarias y uno por la sociedad Cooperativa de Ahorro y Préstamo (Socap) Caja Popular Mexicana.

Conceptos de seguridad:

Autenticación

Autorización

Registro de logs

Pruebas de seguridad



Conceptos de seguridad: Autenticación

Autenticación

Es el proceso mediante el cual un sistema confirmar que la persona y/o aplicativo de software tiene acceso a los recursos privados del sistema. La autenticación tiene tres pasos:

- **Identificar los usuarios**, esto lo realiza mediante el nombre de usuario que esté tratando de acceder.
- **Autenticación**, que quiere decir que el usuario debe confirmar quien dice ser, esto regularmente es manejado mediante una contraseña.
- **Autorización**, esto implica que aún si el usuario pudo acceder al sistema , este tenga únicamente acceso a la información y acciones que el administrador le ha concedido



Conceptos de seguridad: Autorización de los datos

Autorización de los datos

Aún si el usuario ha sido autorizado para acceder al sistema, es necesario que en todo momento se estén validando las acciones que puede o no realizar dentro del mismo. Regularmente estas restricciones y permisos están basados en roles

- Restricciones de acceso a pantallas y menús
- Restricciones de acceso a recursos (información, imágenes, archivos, etc)
- Restricciones de acceso a funciones específicas como registros, modificación o eliminaciones dentro del sistema.
- Restricciones de uso, como podrían ser horarios para el uso de la aplicación, días inhábiles, acceso desde otros países o redes locales, etc.



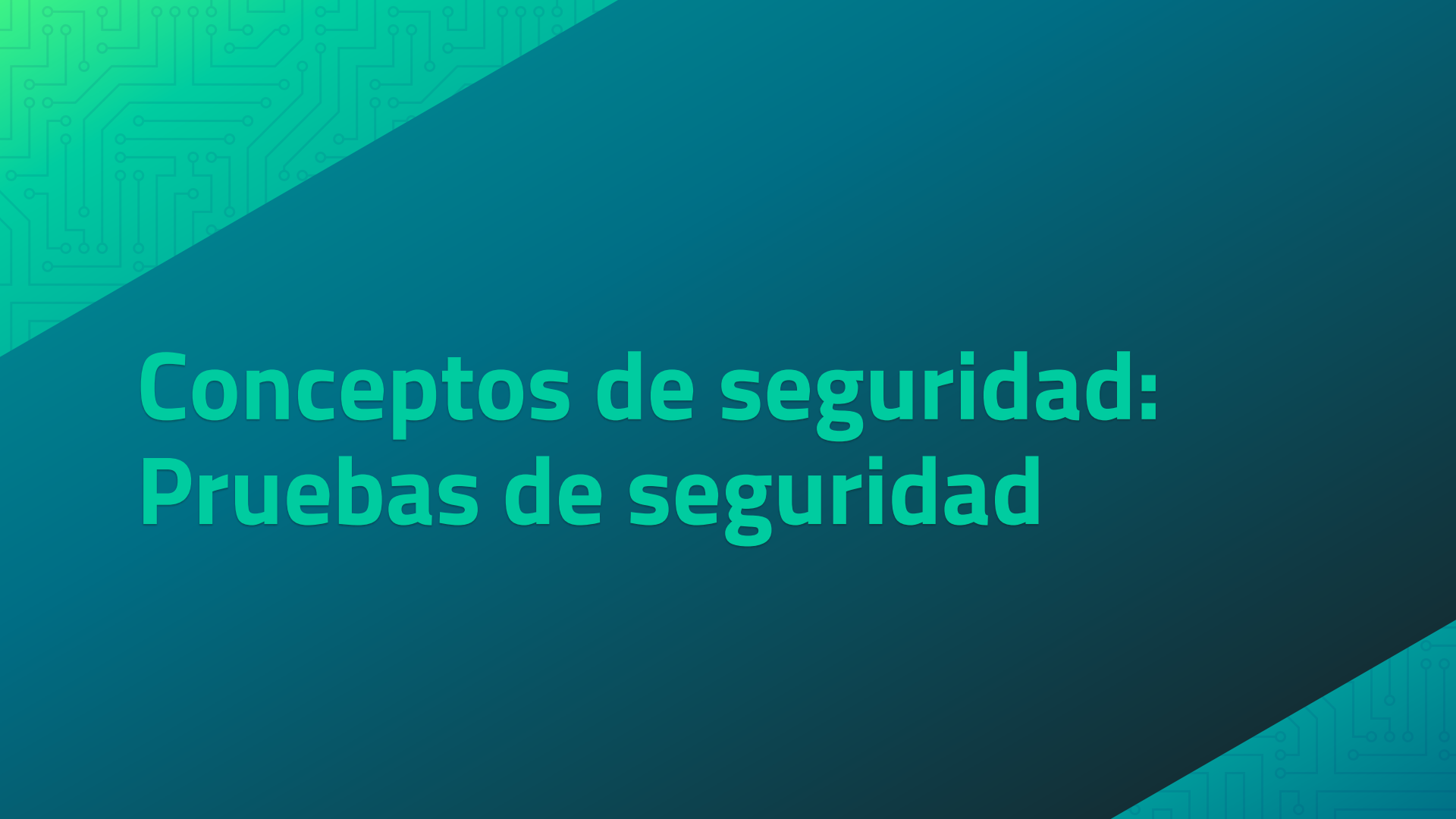
Conceptos de seguridad:

Registro de logs

Registro de logs

El registro de logs implica el seguimiento a las acciones que un usuario realiza, incluso desde antes de acceder al sistema. Esto permite poder detectar tanto vulnerabilidades como responsabilidades de uso del sistema.

- **Logs de inicios de sesión y su resultado (exitoso o fallido)**
- **Bitácoras de cambios dentro del sistema (registro, modificación o eliminación de elementos)**
- **Errores de la aplicación, pueden ser tanto errores por datos del usuario como errores de la aplicación en sí.**



Conceptos de seguridad: **Pruebas de seguridad**

Pruebas de seguridad

Las pruebas de seguridad (AST Application Security Testing), tienen como finalidad recopilar, identificar y cuantificar los fallos de seguridad dentro de un sistema para su posterior corrección.

- ◉ **Static application security testing (SAST).** Son pruebas y herramientas que permiten identificar las vulnerabilidades de un sistema desde el Código Fuente.
- ◉ **Dynamic application security testing (DAST).** Son pruebas y herramientas que permiten identificar las vulnerabilidades de un sistema en tiempo de ejecución.

