DGTIC

Jornadas de visibilidad Web unam 2019

Visibilidad Web UNAM

Consideraciones para evaluar la seguridad de aplicaciones Web

Rubén Aquino Luna

Mnemo Evolution & Integration Services

Ciberseguridad – Relevancia Global

Reporte de Riesgo Global 2019[3]

Incidentes de ciberseguridad

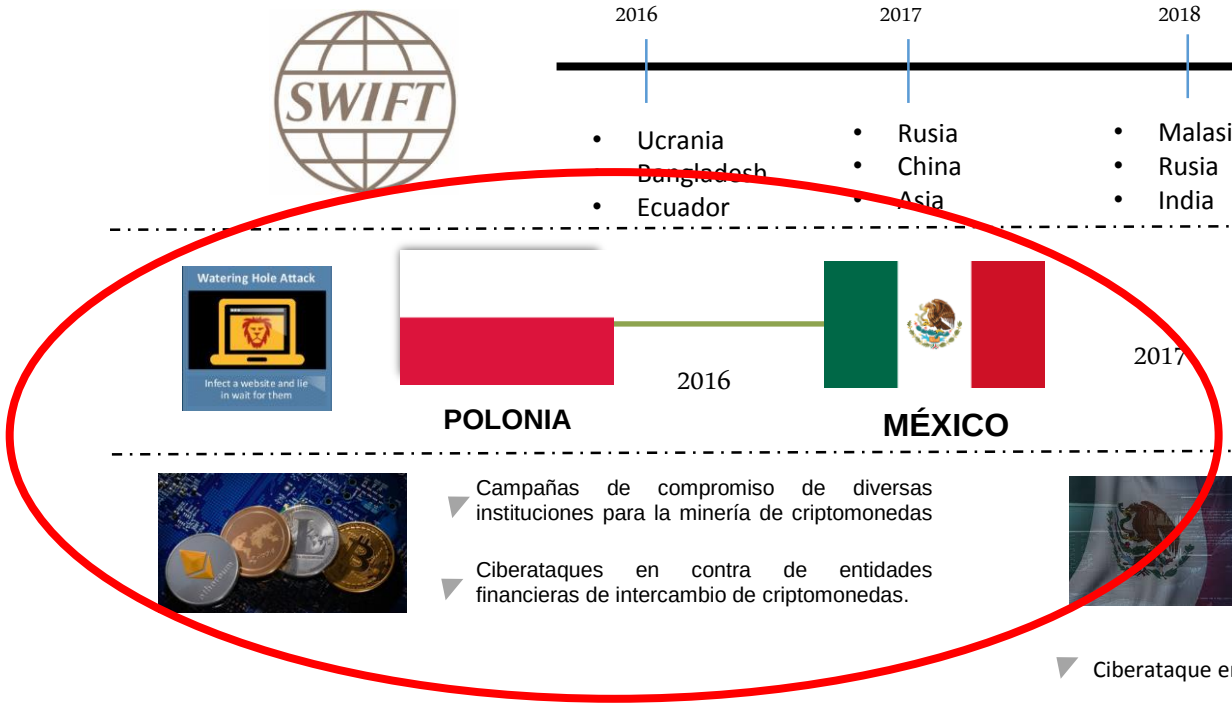
- Hay dos tipos de organizaciones:
  - Las que ya han sido *hackeadas*.
  - Las que aún no lo saben.

"La ausencia de evidencia no es evidencia de ausencia"

¿Tiene algún valor mi sitio web?

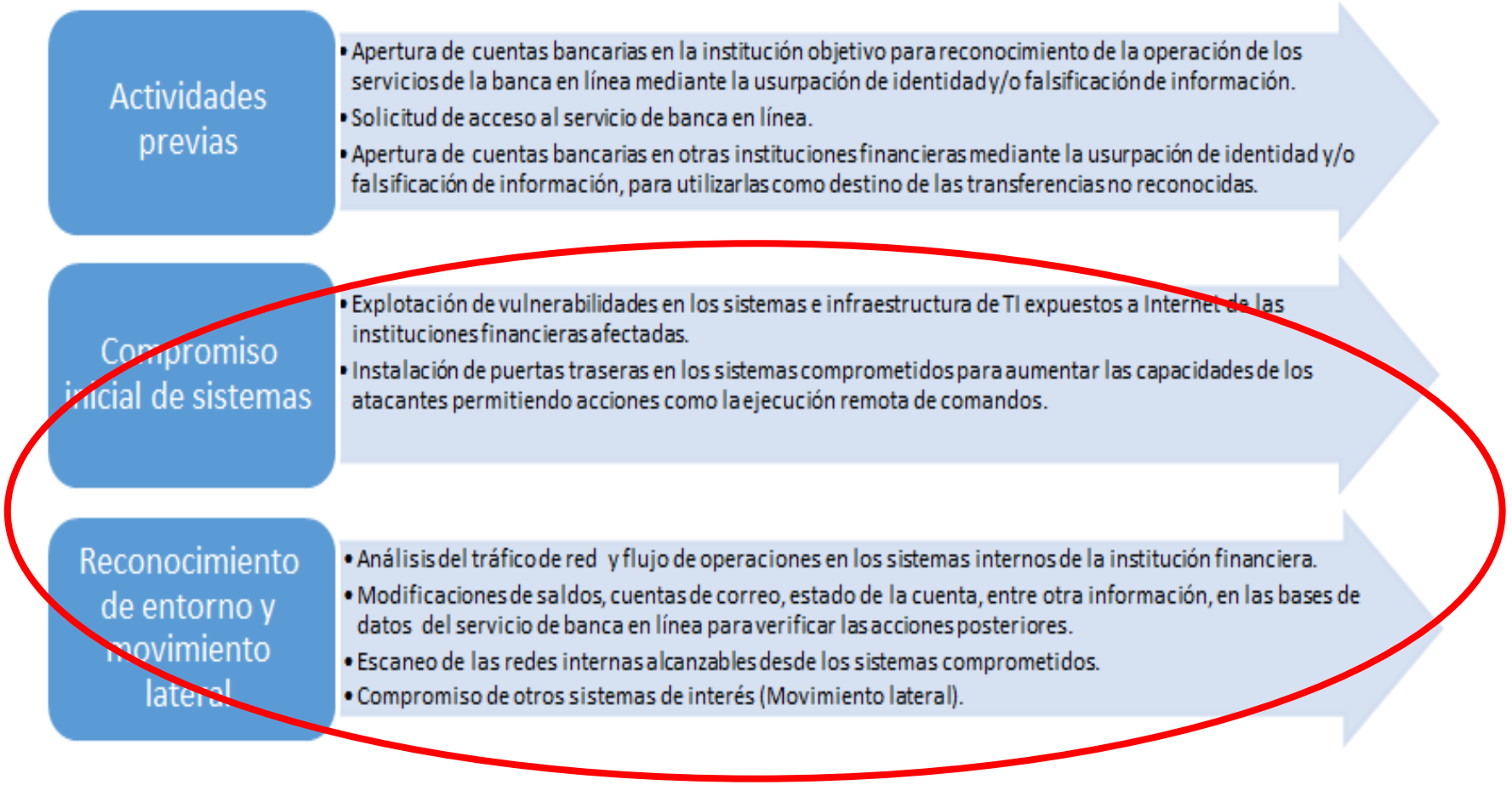
- Reputación
- Visibilidad
- Datos personales
- Capacidades de procesamiento

Ciberataques – Sector financiero global



Ciberataques – Sector financiero México

Mnemo-CERT identificó una campaña de ciberataques en contra de instituciones financieras (2017).



Ciberataques – Sector financiero México

Modificación de registros y evasión del método de autenticación	• Sustitución de la dirección de correo electrónico registrada por otra de uso temporal controlada por el atacante, para evitar que los usuarios legítimos recibieran las notificaciones de las transacciones realizadas. • Modificación del código fuente del aplicativo de banca en línea para la evasión de controles de autenticación (contraseñas de usuario y segundo factor de autenticación "token").
Acciones	• Modificación de saldos de usuarios a nivel de base de datos o selección de cuentas de usuario en función del saldo disponible. • Ejecución de transferencias no reconocidas de fondos a las cuentas destino aperturadas previamente, aprovechando la evasión de los métodos de autenticación.
Retiro de efectivo	• Uso de mulas para el retiro en efectivo de los montos enviados a las cuentas destino en las transacciones no reconocidas.

Mnemo-CERT

Aviso de seguridad MVN-2017-1030

Evaluación de riesgo tecnológico

- La falta de entendimiento del impacto que pueden tener las amenazas de ciberseguridad puede derivar en el compromiso de los procesos de negocio.

- La ciberseguridad debe ser un elemento habilitador de procesos de negocio.

- El desconocimiento de las amenazas y la falta de evaluaciones efectivas de ciberseguridad ha influido de manera adversa en la Gestión del Riesgo.

¿Cómo debo abordar la seguridad de mi sitio web?

- Hacer una evaluación de riesgos.

- Es necesario realizar una revisión y mejora de procesos de seguridad más elementales que podrían robustecer los entornos tecnológicos.

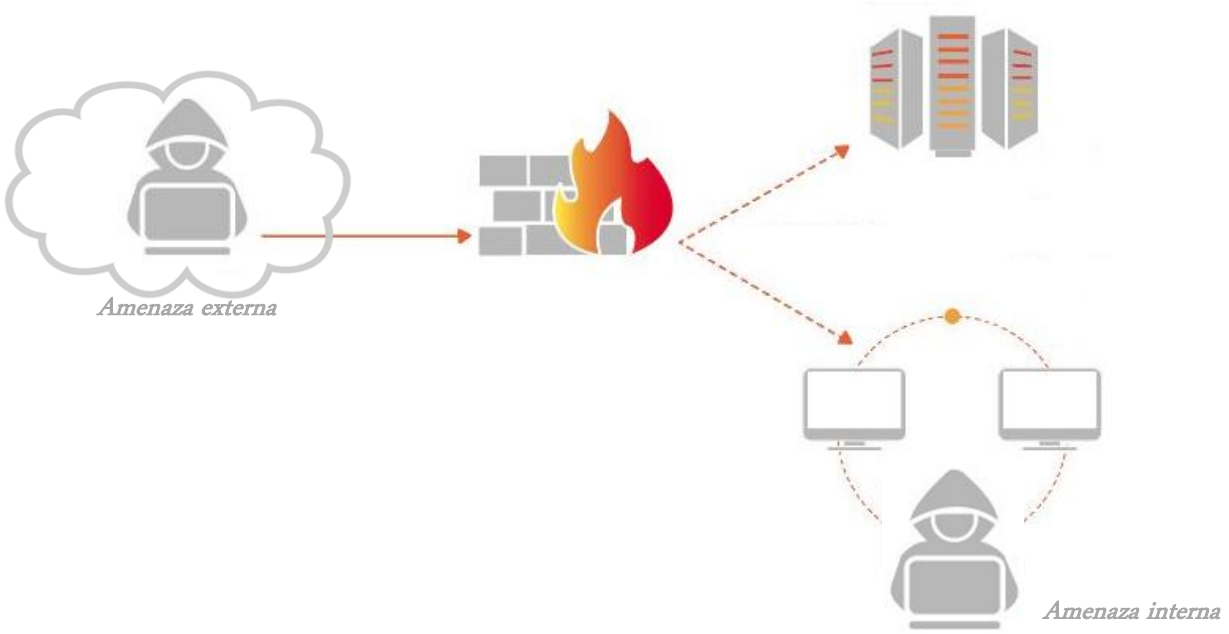
- La protección en ciberseguridad reside en la efectividad de los controles implementados, más que en la cantidad y nivel de sofisticación de los mismos.

Riesgos

- Amenaza
- Impacto
- Probabilidad de ocurrencia

Ejercicios ofensivos

Acciones enfocadas en simular las actividades realizadas por los atacantes.

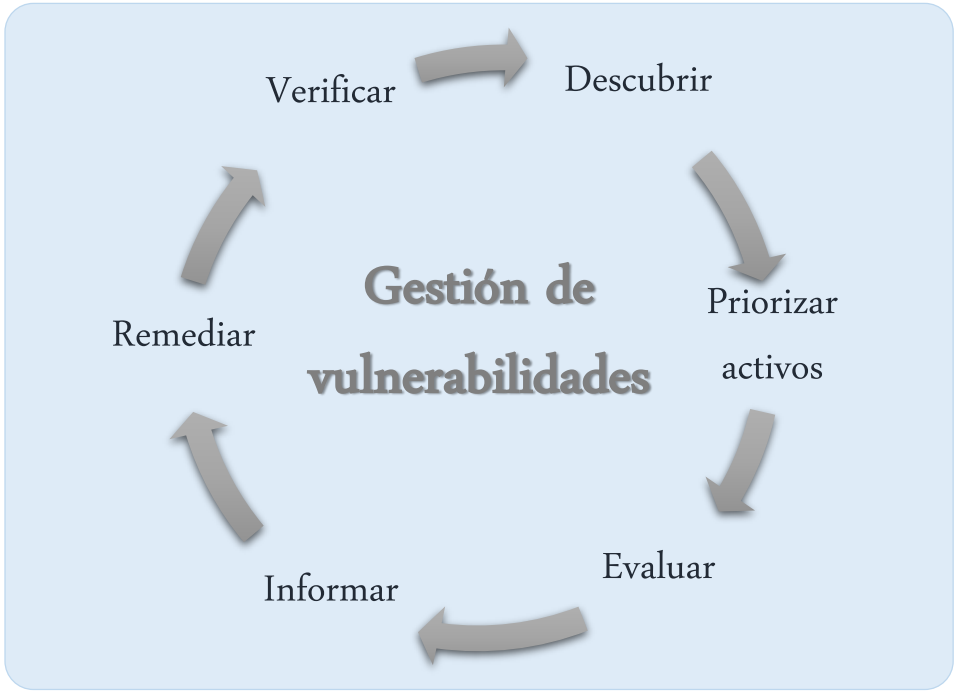


Ejercicios ofensivos

Análisis/gestión de vulnerabilidades

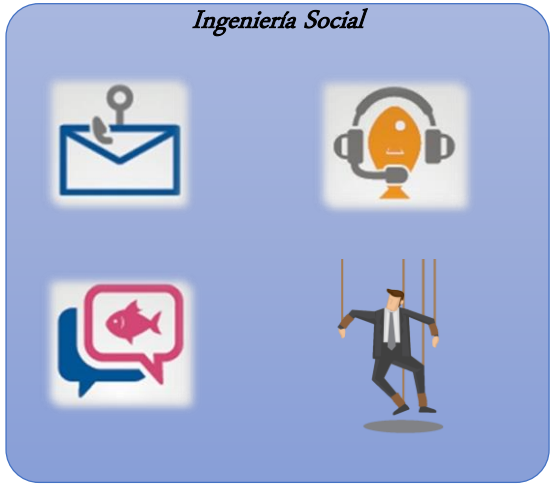
Actividades orientadas en la identificación, evaluación y corrección de vulnerabilidades **conocidas** en la infraestructura tecnológica de la organización.

1. Diagnóstico de seguridad
2. Revisión de políticas de seguridad
3. Revisión de procesos que comprometan la seguridad
4. Generación de documento con recomendaciones



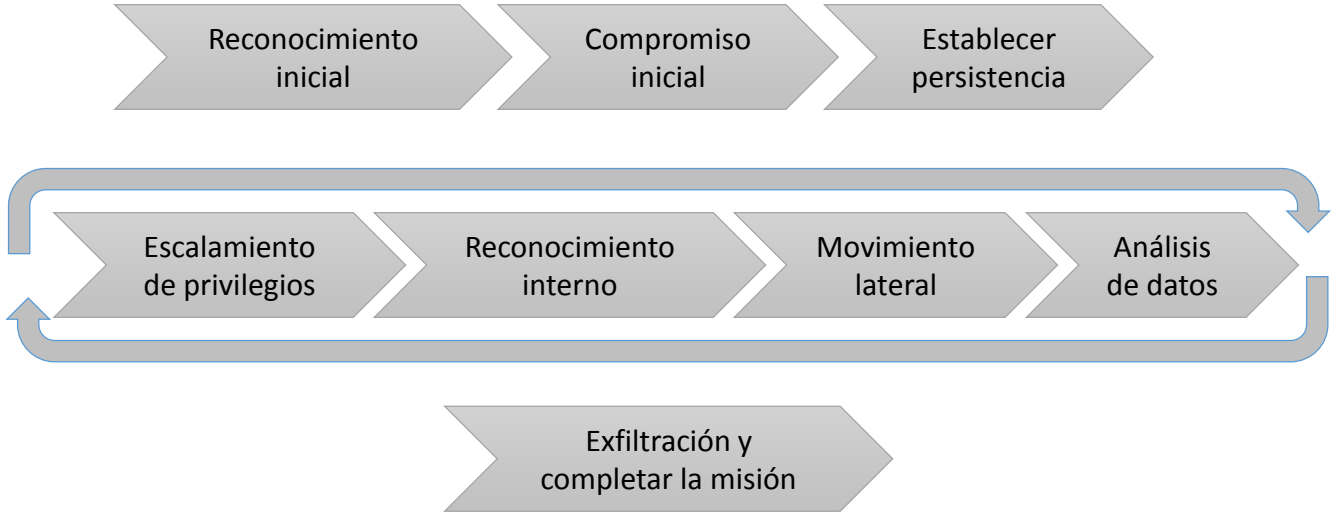
Ejercicios ofensivos-Pruebas de penetración

Ejecución de ataques simulados enfocados en la identificación y aprovechamiento de vulnerabilidades en la infraestructura tecnológica de la organización.

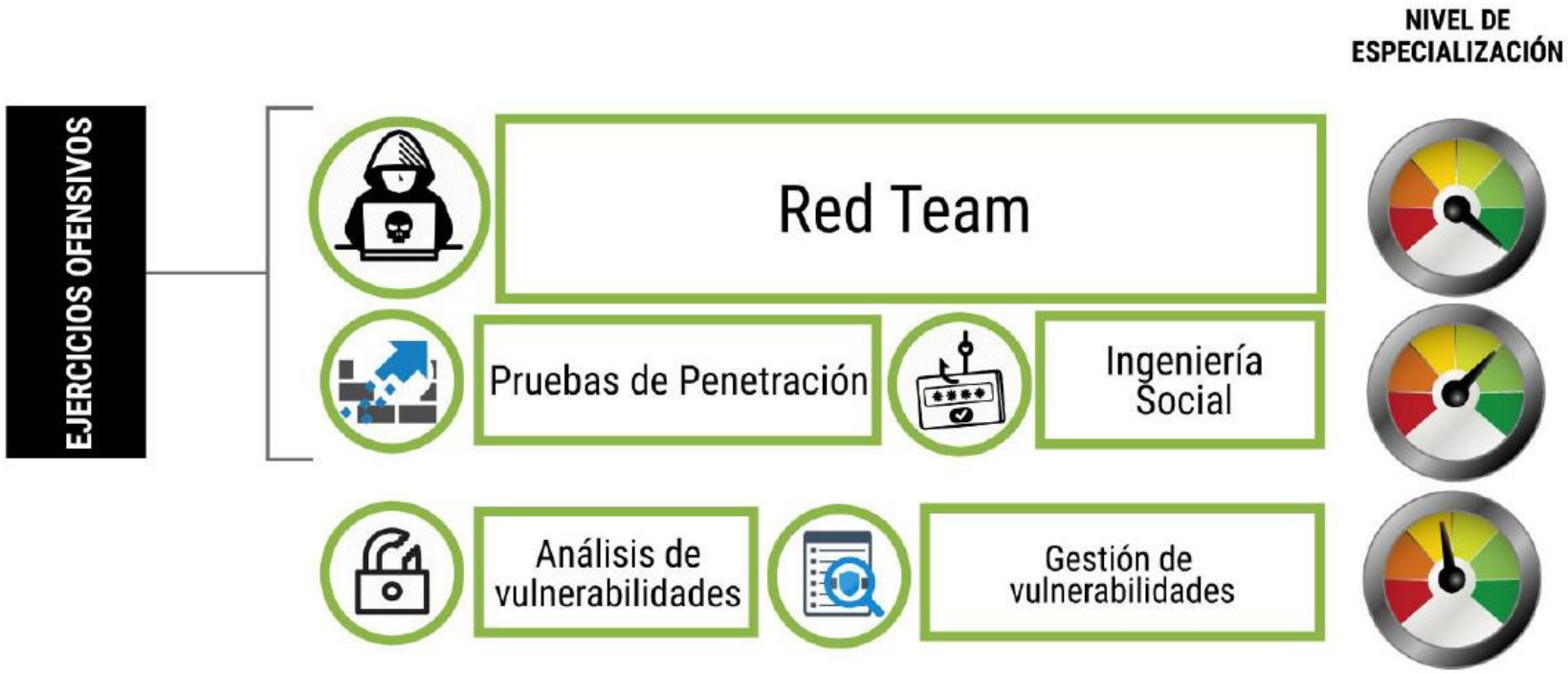


Ejercicios ofensivos-Red Team

Actividades ofensivas con alto nivel de intrusión al estar apegadas a escenarios de ataques en los que se recrean TTPs utilizadas por atacantes sofisticados.



Ejercicios ofensivos-Nivel de especialización



Prácticas que no permiten una evaluación eficaz

- Alcance restringido.
- Análisis basados en la ejecución de herramientas automáticas.
- Habilidades técnicas limitadas por parte de los consultores.
- Consultores con enfoque exclusivamente técnico.
- Contratación de ejercicios ofensivos con base en el menor precio.
- Postura o enfoque de cumplimiento.

Riesgos de no ejecutar ejercicios ofensivos adecuados

- Falsa sensación de seguridad
- Evaluación equivocada del riesgo
- Susceptibilidad ante ataques
- Responsabilidad en caso de incidentes
- Afectaciones a la reputación
- Pérdidas económicas

Ejercicios ofensivos y evaluación de riesgos

- La falta de ejercicios ofensivos efectivos invalida el análisis de riesgos de ciberseguridad.
- La ejecución de ejercicios ofensivos no implica que los elementos evaluados sean seguros.
- Una acción derivada de estos ejercicios debe ser la remediación oportuna de las vulnerabilidades detectadas.
- El impacto inherente a pequeñas fallas es el que a menudo causa que los sistemas colapsen, al ser aprovechadas por los atacantes.

¿Quiénes deben asegurar sus servicios y aplicaciones Web?

[1]

Acuerdo por el que se Establecen los Lineamientos para la Protección de Datos Personales en Posesión de la Universidad Nacional Autónoma de México

Capítulo III
De los Deberes

20. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe de los mismos, cada Área Universitaria deberá establecer, mantener y revisar las medidas de seguridad y controles de carácter administrativo, físico y técnico para la protección de los datos personales que los protejan contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garanticen su confidencialidad, integridad y disponibilidad, conforme a las Normas Complementarias que emita el Comité de Transparencia.

Será responsabilidad de la DGTIC proponer al Comité de Transparencia, el proyecto de Normas Complementarias de carácter técnico en materia de seguridad, que resulte viable para la protección de los datos personales que se encuentren en posesión de la Universidad a través de sus Áreas Universitarias.

24. El Área Universitaria elaborará un documento de seguridad de datos personales que contenga lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa específico de capacitación.

25. El Área Universitaria, con el apoyo técnico de la DGTIC, deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:

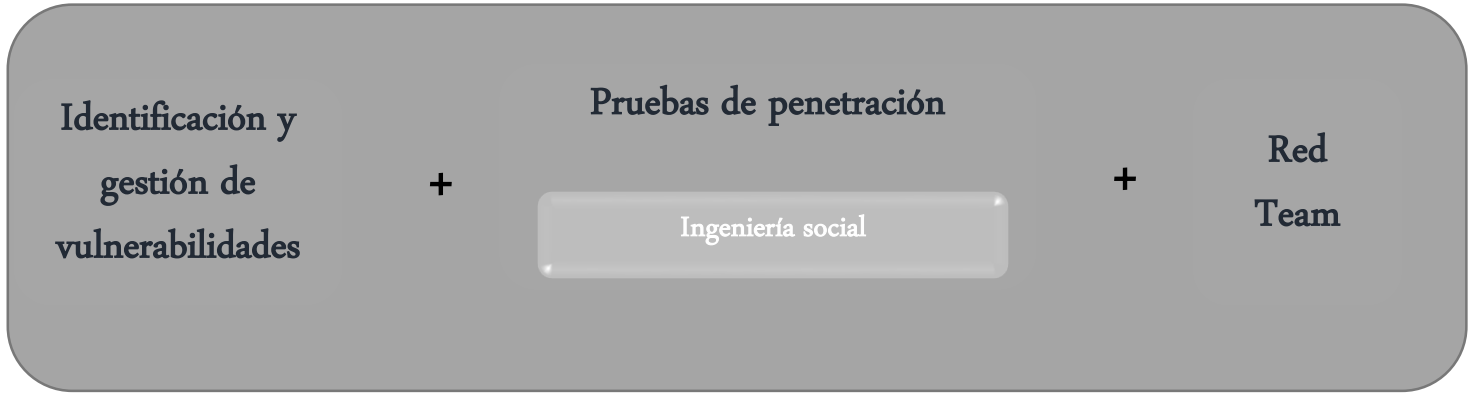
IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, *hardware*, *software*, personal del Área Universitaria, entre otros;
V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en el Área Universitaria;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y
VIII. Las Áreas Universitarias diseñarán y aplicarán diferentes niveles de capacitación del personal bajo su mando, atendiendo los programas generales de capacitación que emita el Comité de Transparencia en términos de lo dispuesto en el Lineamiento 52, fracción VII, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

OWASP Top 10 2017

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

El mejor enfoque

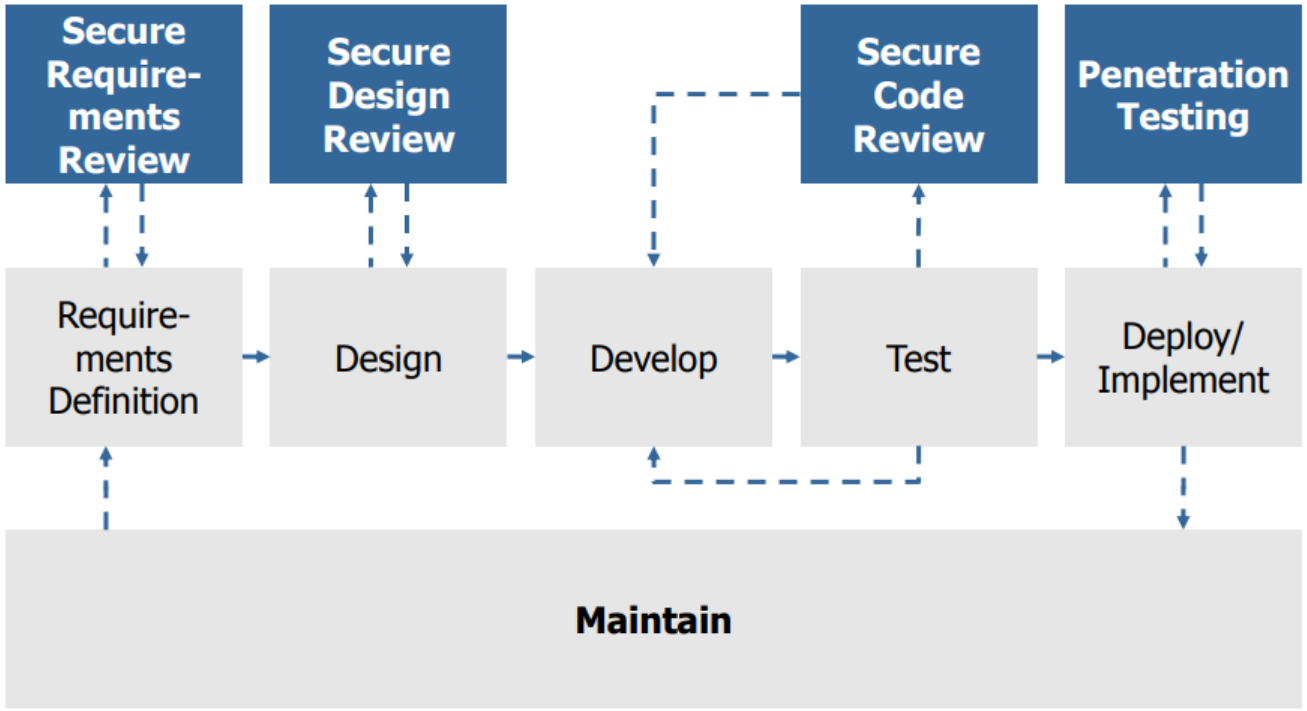
Los diferentes tipos de ejercicios ofensivos no se excluyen entre sí, se complementan entre ellos.



Recomendaciones sobre ejercicios ofensivos

- ✓Ejecución periódica.
- ✓Consultores con las habilidades técnicas adecuadas.
- ✓Pruebas exhaustivas.
- ✓Considerar el entorno tecnológico y el entorno de negocio.
- ✓Los resultados deben ser un insumo para la evaluación de riesgos.

Seguridad en el SDLC



Recomendaciones sobre aplicaciones web

- ✓Requerimientos de seguridad desde el diseño.
- ✓Capacitación sobre aplicación de buenas prácticas de seguridad en el desarrollo.
- ✓Evaluación de seguridad del código mientras se desarrolla
- ✓Aplicación de pruebas de ethical hacking durante el las pruebas, implementación y en producción.
- ✓Aplicación de controles de seguridad en la arquitectura de servidores y aplicaciones.

Referencias

[1] http://www.gaceta.unam.mx/index/wp-content/uploads/2019/02/190225-convocatorias.pdf

[2] https://www.owasp.org/images/7/76/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf

[3] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

¡Gracias!

Rubén Aquino Luna

r.aquino@mnemo.com

@rubenaquino

@mnemocert

DGTIC

Jornadas de visibilidad Web unam 2019

Visibilidad Web UNAM