Ethical Hacking

Evaluaciones de seguridad

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar

La evaluaciones de la seguridad

- Permiten conocer el nivel de seguridad de una organización
  - Procesos, sistemas y redes
- No representan una solución integral a problemas de seguridad
  - Son una herramienta
  - Requieren ser combinados con otros procesos
- Deben ser parte del proceso continuo de gestión
  - Considerar periodicidad
  - Considerar autorización

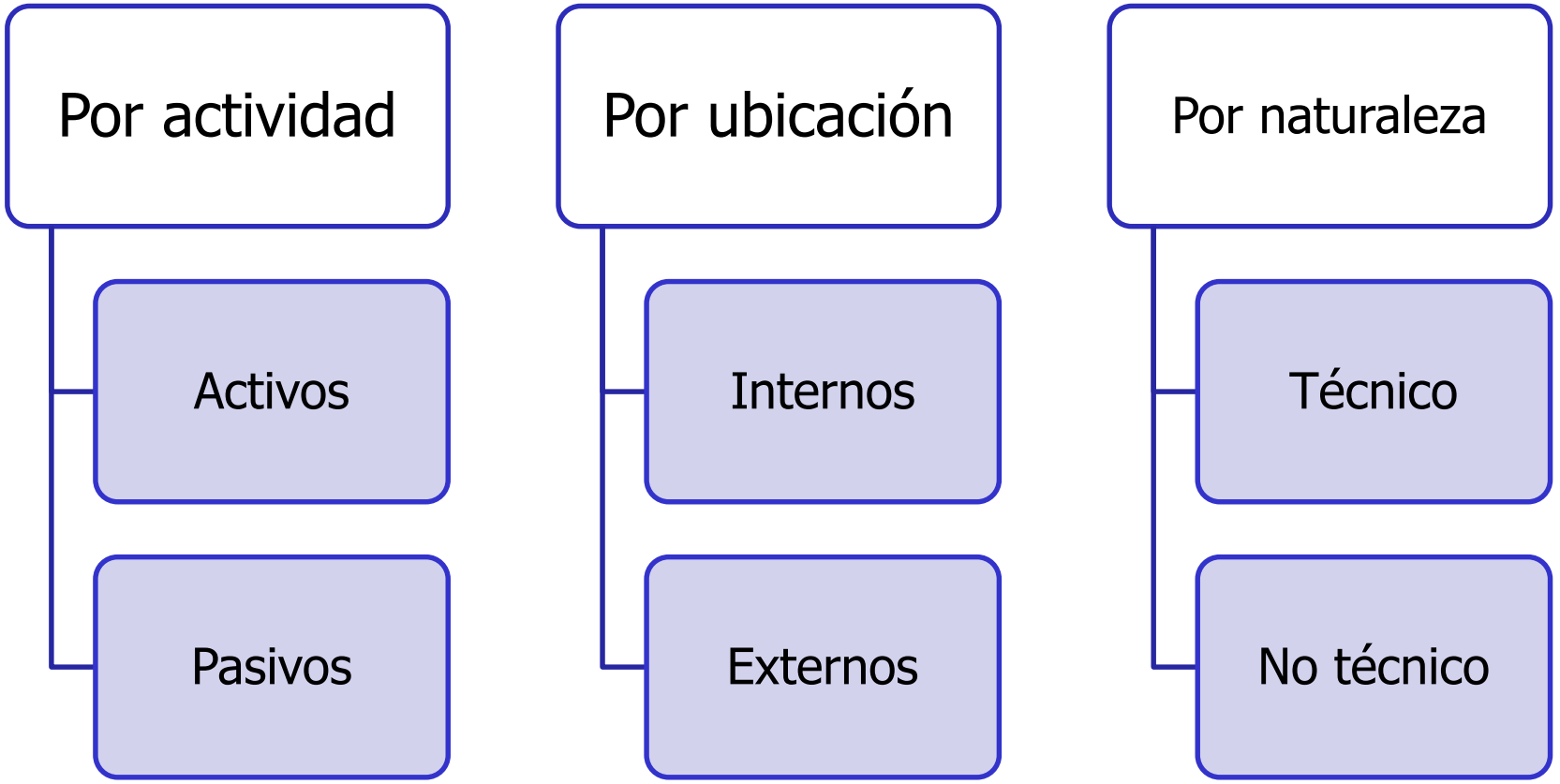
Motivaciones

- Cumplimiento de leyes, regulaciones y normativas
- Identificación de puntos débiles y vulnerabilidades
- Obtención de información para la gestión de la seguridad

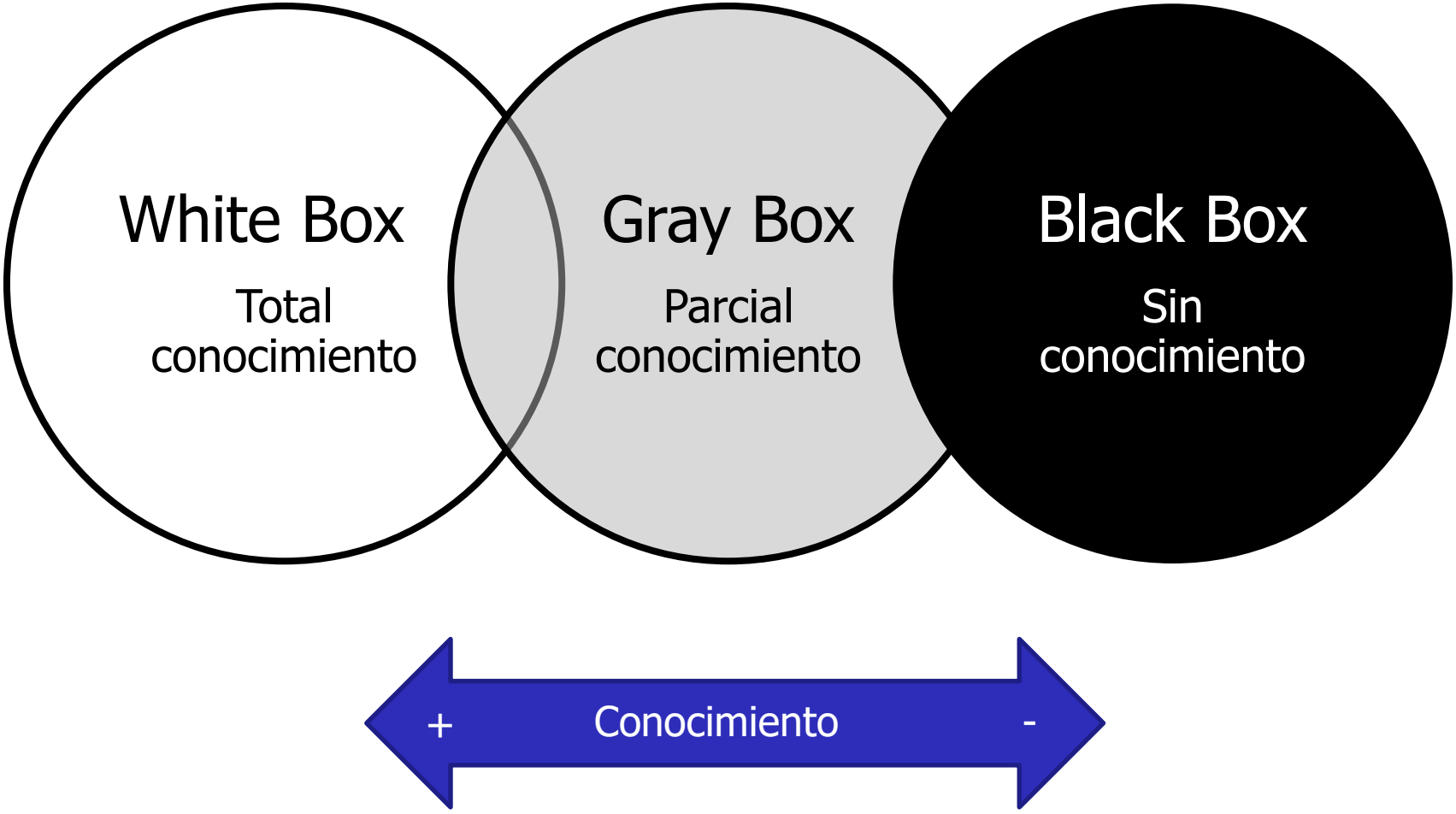
Ejecución

- Profesionales de seguridad
  - Necesidad de confianza
- Forma de contratación
  - Personal interno especializado
  - Consultoras externas
  - Profesionales independientes

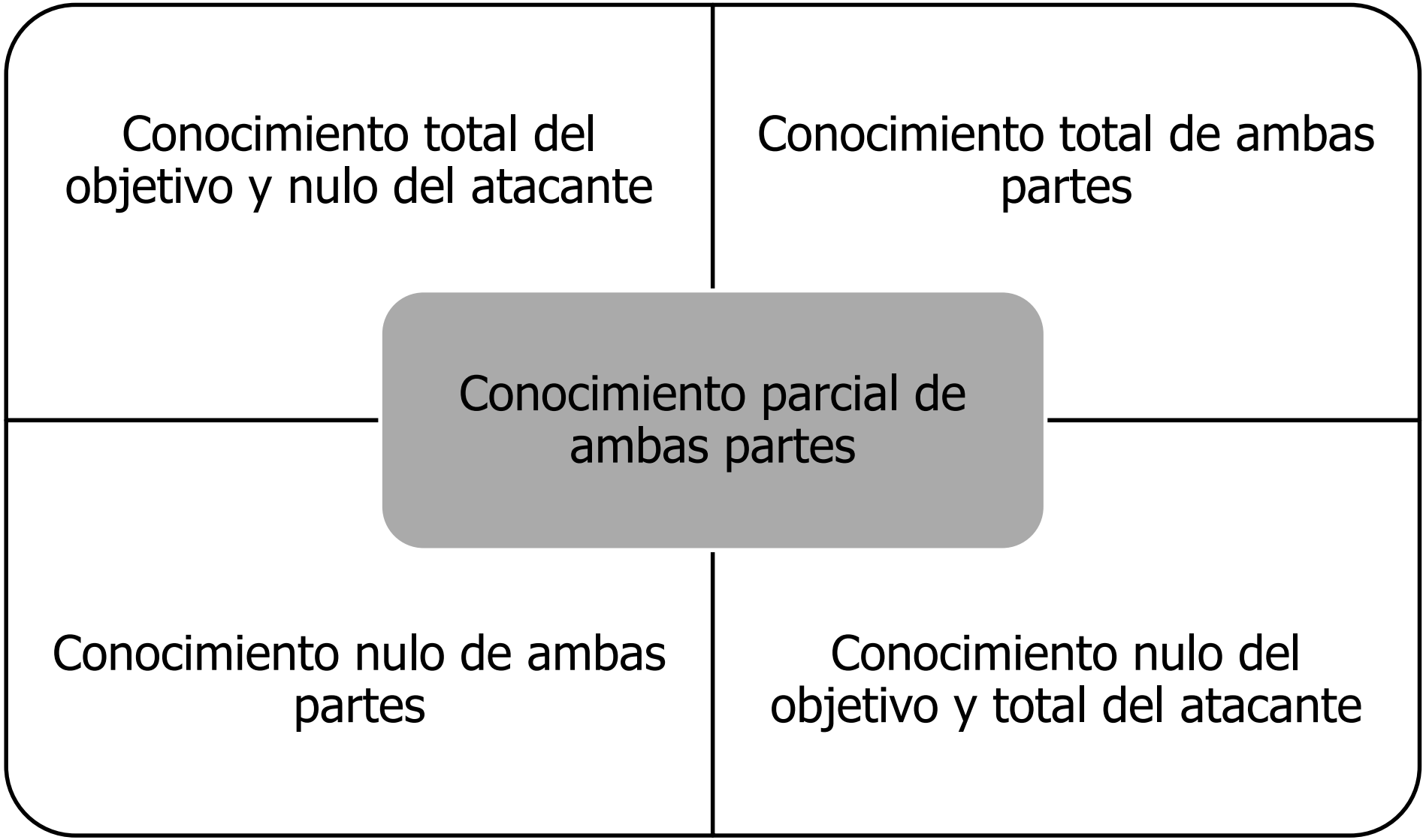
Clasificaciones



Conocimiento del evaluador sobre el objetivo



Situaciones según conocimiento de cada parte



Ámbitos de aplicación de la evaluaciones

- Sistemas y redes
- Software
- Procesos y procedimientos
- Entorno físico

Evaluaciones sobre sistemas y redes

- Análisis de vulnerabilidades
- Penetration test
- Auditoría de seguridad
- Análisis de redes
- Test de plataformas específicas

Análisis de vulnerabilidades

- Identificación de vulnerabilidades en sistemas
  - Solo conocidas
- Puede automatizarse en gran medida
  - Muchos falsos positivos
- Existen distintas áreas de explotación
  - Sistemas Operativos
  - Aplicaciones
  - Configuraciones

Penetration test = Ethical Hacking

- Orientado a penetración y logro de objetivos
  - Incluye el análisis de vulnerabilidades
  - Puede incluir distintas formas de ataque
- Excede al aspecto puramente técnico
  - Puede incluir debilidades en procesos
  - Puede utilizar ingeniería social
  - Puede incluir pruebas físicas
- Requieren el uso de una metodología
- Ejecutado por Pentesters o Ethical Hackers

Auditoria de seguridad

- Proceso de verificación de aspectos de seguridad predefinidos
  - Crystal Box approach
- Puede referirse a procesos, sistemas o productos específicos
- Verificar la alineación respecto a la política
- Basados en guías, checklist, scripts y best practices

Auditoria de seguridad

Action	Description	Severity Level	O/S	Oracle Version	Default Install
0.	Planning and Risk assessment				
0.1	Identify and patch known and reported Vulnerabilities	1	ALL	ALL	YES
0.2	Identify and record software (Oracle and OS and Applications) versions and patch levels on the System	1	ALL	ALL	YES
0.3	Install only the database features that are needed	1	ALL	ALL	YES
0.4	Record database configuration and store securely	2	ALL	ALL	YES
0.5	Record database security configuration and store securely	2	ALL	ALL	YES
0.6	Review database security procedures and policies	2	ALL	ALL	YES
0.7	Store copies of the media used to build Oracle database off site	3	ALL	ALL	YES
0.8	Consider physical location of servers	2	ALL	ALL	YES
0.9	Define secure database / application architecture	3	ALL	ALL	YES
1.	Host Operating System security Issues				
1.1.1	Check owner of Oracle software owns all files in $ORACLE_HOME/bin	1	ALL	ALL	YES
1.1.2	Lock Oracle software owner account	1	ALL	ALL	YES
1.1.3	Do not name Oracle software owner account *oracle*	2	ALL	ALL	YES
1.1.4	Limit access to software owner account				
1.1.5	Use separate owners for different components of Orac				
1.2.1	Check file permissions in $ORACLE_HOME/bin				
1.2.2	Check *umask* value				

Windows

Why Windows Apps+games PCs+tablets Downloads **How-to**

Get started **Get help**

Security checklist for Windows

4.7.2	Use VPD, RLS and label security for full data protec				
4.8.1	Be aware of possible failure to be alerted of suspici				
4.9.1	Be aware of possible failure to audit the security pro				
4.10.1	Audit and review the Oracle generated log files				
5.	Networking				
5.1.1	Prevent set commands on the listener				
5.1.2	Prevent remote dba access on sql*net v1				
5.1.3	Audit the *listener.ora* file				
5.1.4	Enable shared sockets				
5.1.5	Force the MTS dispatcher to use specific ports				
5.1.6	Do not use the standard listener ports 1521, 1526	2	ALL	ALL	YES
5.1.7	Do not use known SID or service names such as ORCL	2	ALL	ALL	YES
5.1.8	In small environments do not use hostnames in *listener.ora.*	2	ALL	ALL	
5.1.9	Use a personal firewall on database administrator computers	2	ALL	ALL	YES
5.1.10	Secure *listener.ora* at the O/S level	2	ALL	ALL	YES
5.1.11	Ensure that listener logging is enabled	2	ALL	ALL	YES
5.2.1	Restrict sources of database connections	3	ALL	ALL	
5.2.2	Use connection manager and Oracle names to restrict connections by source	2	ALL	ALL	
5.3.1	Set the listener password	1	ALL	ALL	YES
5.4.1	Restrict listener banner information	3	ALL	ALL	
5.5.1	Use a firewall to protect the Oracle server.	2	ALL	ALL	
5.6.1	Audit Oracle client file permissions	4	ALL	ALL	
5.6.2	Audit client configuration file contents	5	ALL	ALL	
5.6.3	Audit the listener	2	ALL	ALL	YES

Análisis de redes

- Escaneo de sistemas de telecomunicaciones y redes de datos
  - Protocolos
  - Dispositivos
  - Servicios

- Se analizan principalmente vulnerabilidades conocidas
  - Normalmente su alcance es puramente técnico

- Puede destinarse a tipos de redes específicas
  - Wi-Fi
  - Bluetooth
  - VoIP

Test de plataformas específicas

- Evaluaciones sobre productos comerciales
  - En general de gran magnitud o despliegue masivo
- Se profundiza en aspectos muy detallados
  - Implementación
  - Configuraciones
  - Niveles y permisos de acceso
  - Vulnerabilidades estándar
- Normalmente lo realizan consultoras especializadas
  - Algunas también testean hardware
  - Suele relacionarse a la investigación de vulnerabilidades

Evaluaciones sobre software

- Software testing tradicional
- Security testing
- Auditoría de código fuente

Software Testing Tradicional

- Busca determinar el cumplimiento de requerimientos funcionales y caso de uso
  - Debe hacer lo que se supone que debería hacer, y de la forma que debe hacerlo
- Los testers construyen casos de uso y escenarios
  - Basados en los requerimientos funcionales
  - Verificar metódicamente que cada punto funciona correctamente
- También se pueden incluir otros aspectos
  - Performance, stress, backup, recuperación, cuestiones operativas
- No suelen incluir requerimientos de seguridad
  - Si los hay, se testean

Security Testing

- Busca determinar el nivel de seguridad del software desde su exterior (black box)
  - Además de verificar los requerimientos de seguridad
- Enfoque "Negative Testing" (verificar que cosas malas no puedan suceder)
  - Hace el producto lo que NO se supone que hace
  - Se asume que si se implementa bien podría continuar siendo inseguro
  - Se asume que un usuario puede no usar el producto como en los escenarios evaluados
- Se construyen patrones de ataque en vez de casos de uso
  - Se simula el comportamiento de un atacante, no de un tester (QA)
- Varía si es software binario o aplicaciones web
  - Puede incluirse ingeniería reversa y técnicas específicas

Auditoría de código fuente

- Análisis del código estático en busca de fallas

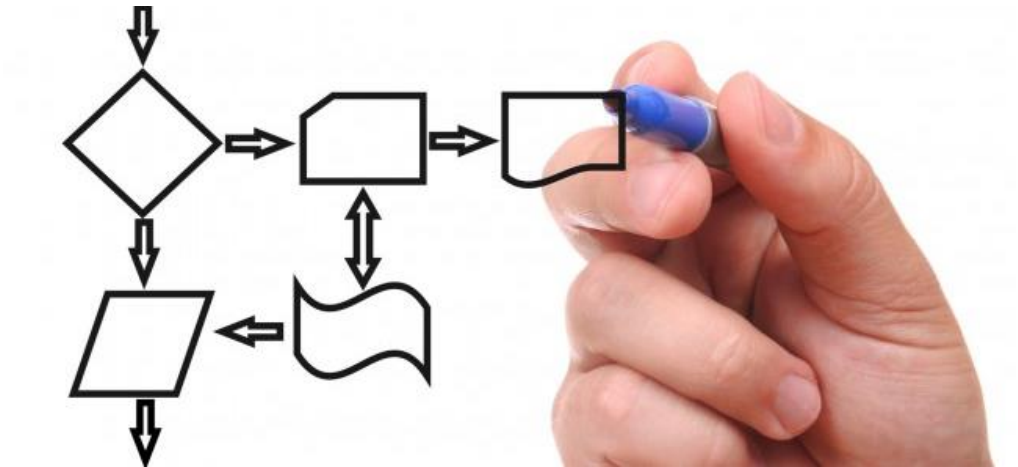
- Técnicas
  - Revisión manual lineal
  - Seguimiento de flujos
  - Funciones peligrosas
  - Revisión automatizada

- Herramientas
  - Editores de código
  - Checklist
  - Expresiones regulares
  - Herramientas específicas

Evaluaciones sobre procesos y procedimientos

Análisis funcional específico

Análisis diferencial



Análisis funcional específico

- Basado en el estudio exhaustivo de un proceso
- Se utilizan técnicas de seguridad para intentar vulnerarlo
- Cada análisis es muy particular de cada organización
- No está basado en aspectos técnicos

Análisis diferencial (Gap Analysis)

- Comparación del estado actual con un estado ideal propuesto
  - Puede basarse en una norma o estándar

- Se realiza por medio de reuniones con responsables de procesos

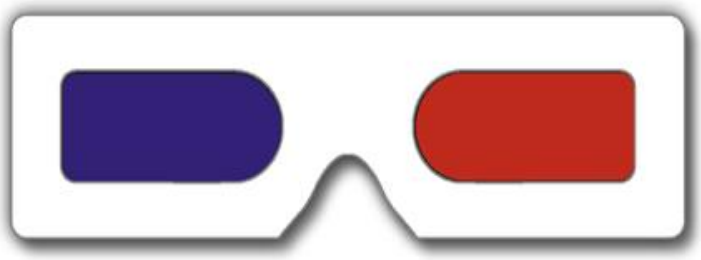
(ISO 27001)	
POLÍTICAS DE SEGURIDAD	
•Existen documento(s) de políticas de seguridad de SI	☑ VERDADERO
•Existe normativa relativa a la seguridad de los SI	☐ FALSO
•Existen procedimientos relativos a la seguridad de SI	☐ FALSO
•Existe un responsable de las políticas, normas y procedimientos	☐ FALSO
•Existen mecanismos para la comunicación a los usuarios de las normas	☐ FALSO
•Existen controles regulares para verificar la efectividad de las políticas	☐ FALSO
ORGANIZACIÓN DE LA SEGURIDAD	
•Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☐ FALSO
•Existe un responsable encargado de evaluar la adquisición y cambios de SI	☐ FALSO
La Dirección y las áreas de la Organización participa en temas de seguridad	☐ FALSO
•Existen condiciones contractuales de seguridad con terceros y outsourcing	☐ FALSO
•Existen criterios de seguridad en el manejo de terceras partes	☐ FALSO
•Existen programas de formación en seguridad para los empleados, clientes y terceros	☐ FALSO
•Existe un acuerdo de confidencialidad de la información que se accesa.	☐ FALSO
•Se revisa la organización de la seguridad periódicamente por una empresa externa	☐ FALSO
ADMINISTRACIÓN DE ACTIVOS	
•Existen un inventario de activos actualizado	☑ VERDADERO
•El Inventario contiene activos de datos, software, equipos y servicios	☐ FALSO
•Se dispone de una clasificación de la información según la criticidad de la misma	☐ FALSO
• Existe un responsable de los activos	☐ FALSO
•Existen procedimientos para clasificar la información	☐ FALSO
•Existen procedimientos de etiquetado de la información	☑ VERDADERO

Evaluaciones al entorno físico

- Busca determinar vulnerabilidades físicas y ambientales
  - Usualmente llamados Red Team Test
  - Muchas veces encarado como Pentest (limitación: no ejecutado en forma real)

- Ejecutado por un Red Team
  - Equipo multidisciplinario
  - Personal propio o externo

- Características
  - Prueban la efectividad del Blue Team (equipo defensivo)
  - Realizan ataques reales o simulados
  - Incluye equipamiento electrónico
  - Normalmente se realiza sin previo aviso



¿Preguntas?

Federico Pacheco

 @FedeQuark

 www.federicopacheco.com.ar

 info@federicopacheco.com.ar