

REALTIME
CONSULTING & SERVICES

Procedimiento de Gestión Vulnerabilidades

Security operations center (SOC)
REALTIME CONSULTING & SERVICES
https://www.rt.com.co/
soc@rt.com.co

COMPAÑÍA
ISO/IEC 27001:2013
CERTIFICADA

Tabla de contenido

Tabla de contenido 2
Glosario de términos 3
Objeto 4
Alcance 4
Descripción del proceso 4



Glosario de términos

- **Pentesting:** Intento de vulnerar un sistema informático para determinar su nivel de seguridad conociendo parte del entorno del objetivo.

- **Ethical hacking:** Intento de vulnerar un sistema informático para determinar su nivel de seguridad desconociendo del entorno del objetivo.

- **Ingeniería Social:** Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

- **Vulnerabilidad:** Debilidad de un sistema o elemento.

- **Confidencialidad:** Característica o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Integridad:** Característica o propiedad de salvaguardar la exactitud y completitud de los activos de información.

- **Disponibilidad:** Característica o propiedad por lo que la información permanece accesible y disponible para su uso cuando lo requiera una entidad autorizada.

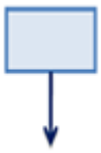
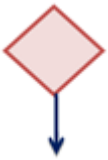
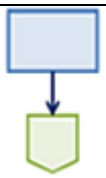
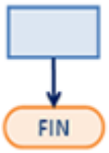
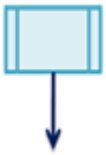
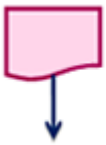
Objeto

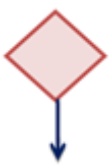
Realizar control de las vulnerabilidades técnicas en los sistemas de información, los componentes de infraestructura asociados, las estaciones de trabajo, servidores conectados a la red de datos de las compañías, empleados y vinculados

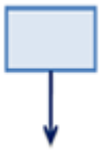
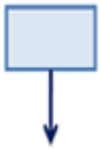
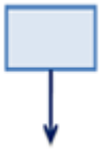
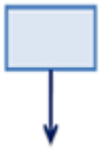
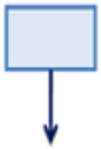
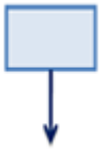
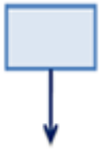
Alcance

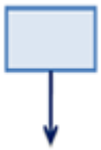
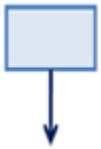
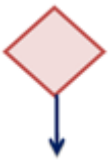
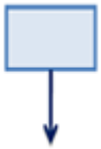
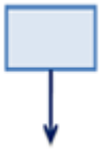
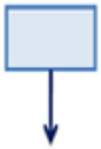
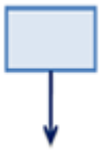
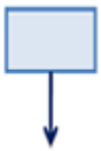
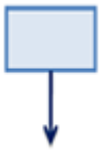
Este procedimiento cubre los sistemas de información, los componentes de infraestructura asociados, las estaciones de trabajo, servidores conectados a la red de datos empleados y vinculados de la compañía.

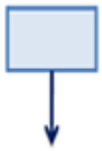
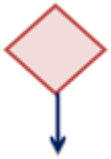
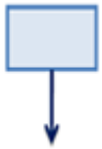
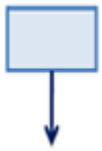
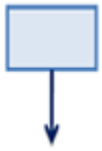
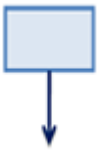
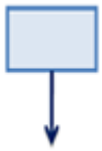
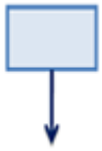
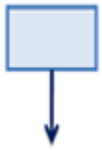
Descripción del proceso

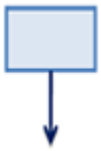
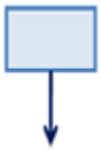
Operación	Decisión	Conector	Inicio con operación	Fin con operación	Procedimiento	Documento	Fin
							

PASO	DESCRIPCIÓN ACTIVIDAD	FLUJO
1	Inicio del procedimiento	
2	¿Es un análisis de vulnerabilidades?, entonces continuar en el paso 3. ¿Son pruebas de hacking ético y/o Pentesting?, entonces continuar en el paso 13 ¿pruebas de ingeniería social? continuar en paso número 21.	

3	Seleccionar los dispositivos que van a ser cubiertos dentro del análisis	
4	Definir a que componentes de los dispositivos se va a realizar el análisis.	
5	Definir alcance y tipo de análisis a realizar sobre los componentes seleccionados.	
6	Definir el nivel de exploración de las vulnerabilidades (profundidad)	
7	Determinar qué implicaciones se deben tener en cuenta antes durante y después del análisis.	
8	Ejecutar el análisis de vulnerabilidades	
9	Generar reporte de las vulnera-bilidades, (reporte estándar y diferencial).	
10	10.1 Identificar y seleccionar las remediaciones pertinentes que se tienen que aplicar para corre-gir las vulnerabilidades detecta-das. 10.2 Identificar y documentar las vulnerabilidades que no se pueden corregir ya sea porque no existe remediación o porque la aplicación de esta puede o causaría un gran impacto en el dispositivo, afectando la operación del negocio.	

11	Documentar y elaborar el plan de remediación.	
12	Elaborar el control de cambios para las remediaciones o capacitaciones para ser presentado en comité. Continuar en el paso 29.	 Paso 29
13	¿Es una solicitud interna o de una consultoría?, entonces ir a paso 14. ¿Es una solicitud de las compañías hacia un ente externo?, entonces ir a paso 17	
14	Se realiza la solicitud de aprobación al propietario del activo de información	
15	El propietario del activo de información analiza la solicitud	
16	¿El propietario del activo de información acepta la solicitud?, se continua en el paso 17 ¿El propietario del activo de información rechaza la solicitud?, se continua en el paso 29	
17	Definir los elementos objetivo de las pruebas	
18	Ejecutar las pruebas de Ethical Hacking y/o Pentesting	
19	Elaborar el informe de Ethical Hacking y/o Pentesting	
20	Presentar el informe de Ethical Hacking y Pentesting	

	Ir a paso 10	 Paso 10
21	¿Es una solicitud interna o de una consultoría?, entonces ir a paso 22. ¿Es una solicitud de las compañías hacia un ente externo?, entonces ir a paso 25	
22	Se realiza la solicitud al área escogida para hacer la prueba	
23	El área escogida para hacer la prueba analiza la solicitud	
24	¿El área escogida para hacer la prueba acepta la solicitud?, se continua en el paso 17 ¿El área escogida para hacer la prueba rechaza la solicitud?, se continua en el paso 29	
25	Identificar y seleccionar las personas a los cuales se les va a realizar las pruebas de ingeniería social.	
26	15.1. Definir las pruebas de ingeniería social. 15.2. Ejecución de las pruebas de ingeniería social	
27	Generar informe con los hallazgos.	
28	Identificar y seleccionar las capacitaciones pertinentes que se tienen impartir para corregir las falencias detectadas.	

29	Documentar y elaborar el plan de capacitación. Continuar en el paso 10.	 Paso 11
29	Realizar seguimiento periódico a las remediaciones de vulnerabilidades y/o capacitaciones	
30	Finaliza el proceso	