CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Eduar Enrique Navarro Morales Cargo: Coordinador Grupo de Trabajo Informática Forense y Seguridad Digital.	Nombre: Francisco Andrés Rodríguez Eraso Cargo: Jefe Oficina de Tecnología e Informática.	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad. Fecha: 2019-05-31

1 OBJETIVO

Establecer los lineamientos necesarios para llevar a cabo la inspección de seguridad en los sistemas de información de la Superintendencia de Industria y Comercio, con referencia en las mejores prácticas de configuraciones de seguridad (Hardening), actividad que será realizada por la Oficina de Tecnología e Informática - OTI.

2 DESTINATARIOS

Colaboradores de la OTI.

3 GLOSARIO

AMENAZA: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

ANTIVIRUS: Programa informático que previene o detecta la presencia de software malicioso principalmente en los equipos de cómputo y servidores.

BENCHMARK: Es un punto de referencia o comparador de las mejores prácticas sobre el área de interés, utilizado para transferir el conocimiento de las mejores prácticas y su organización.

FIREWALL: Sistema de seguridad informática cuya función es de controlar el tráfico de datos, es decir, permitir el paso o impedirlo de acuerdo a los criterios o políticas de seguridad determinadas.

HARDENING: Proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

IPS: Sistema de Prevención de Intrusos, dispositivo de seguridad informática que monitorea el tráfico de red en busca de actividad maliciosa.

SISTEMAS DE INFORMACIÓN: Es un conjunto de procedimientos interrelacionados que forman un todo, es decir, obtiene, procesa, almacena y

distribuye información para apoyar la toma de decisiones y el control en una organización.

VULNERABILIDAD: Debilidad de un activo de información o control que puede ser explotada por una o más amenazas.

WAF: Firewall de Aplicaciones Web es un dispositivo hardware o software que permite proteger los servidores de aplicaciones web de determinados ataques informáticos originados desde la red de internet.

4 DESCRIPCIÓN DE ACTIVIDADES

4.1 DEFINIR EL ALCANCE Y PROGRAMACIÓN

Los colaboradores del Grupo de Trabajo de Informática Forense y Seguridad Digital anualmente definen los sistemas de información de la Entidad o elementos de la plataforma tecnológica que serán objeto de la inspección de seguridad, para lo cual deben presentar la propuesta con el detalle de las actividades al Comité Técnico de la OTI. Esta actividad se debe realizar con observancia en las siguientes directrices:

- El alcance de las pruebas de inspección se debe acordar y controlar.
- Los requisitos de la inspección para el acceso a sistemas y a datos se deben identificar y acordar con la coordinación de la OTI apropiada.
- Las pruebas de inspección se deben limitar a acceso a software y datos únicamente para lectura.
- De requerirse acceso diferente al de solo lectura, únicamente se debe proveer en copias aisladas de los archivos del sistema, que se deben borrar de forma segura una vez que la revisión haya finalizado, y se debe proporcionar la protección apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de la inspección.
- Las pruebas de inspección que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.
- Se debe hacer seguimiento de todos los accesos y registrarlos para producir un rastro de referencia.

4.2 IDENTIFICAR LOS COMPONENTES DE LA INSPECCIÓN

Una vez definido el alcance y el(los) sistema(s) de información o el (los) elemento(s) de la plataforma tecnológica sujeto(s) de la inspección, el Coordinador

del grupo de trabajo custodio debe informar al Grupo de Trabajo de Informática Forense y Seguridad Digital, el listado de los colaboradores asignados para atender la inspección y la arquitectura del sistema, la cual debe incluir al menos el diagrama de arquitectura, servidores, elementos de red de datos, sistemas operativos y bases de datos.

4.3 EJECUTAR LA INSPECCIÓN

Previa citación a los colaboradores de la OTI y especialistas de la mesa de servicios involucrados en la gestión del sistema de información o elementos de la plataforma tecnológica, el Grupo de Trabajo de Informática Forense y Seguridad Digital desarrolla en la fecha programada la inspección de seguridad, teniendo en cuenta las siguientes fases:

4.3.1 Realizar inspección general del sistema de información o elementos de la plataforma tecnológica

En esta fase debe aplicar la lista de chequeo descrita en el formato SC05-F04 Inspección de aspectos generales de seguridad en sistemas de información. La cual incluye temas relacionados con arquitectura, contingencia, autenticación, trazabilidad, seguridad perimetral, comunicaciones, actualizaciones, entre otros. Es de anotar que el Grupo de Trabajo de Informática Forense y Seguridad Digital puede solicitar las evidencias que consideren necesarias a fin de verificar la implementación del control o identificar puntos de mejora, en este sentido, los grupos de trabajo de la OTI, según su competencia, deben aportar las evidencias o la debida justificación para los casos que no aplique su verificación.

4.3.2 Realizar inspecciones específicas de seguridad

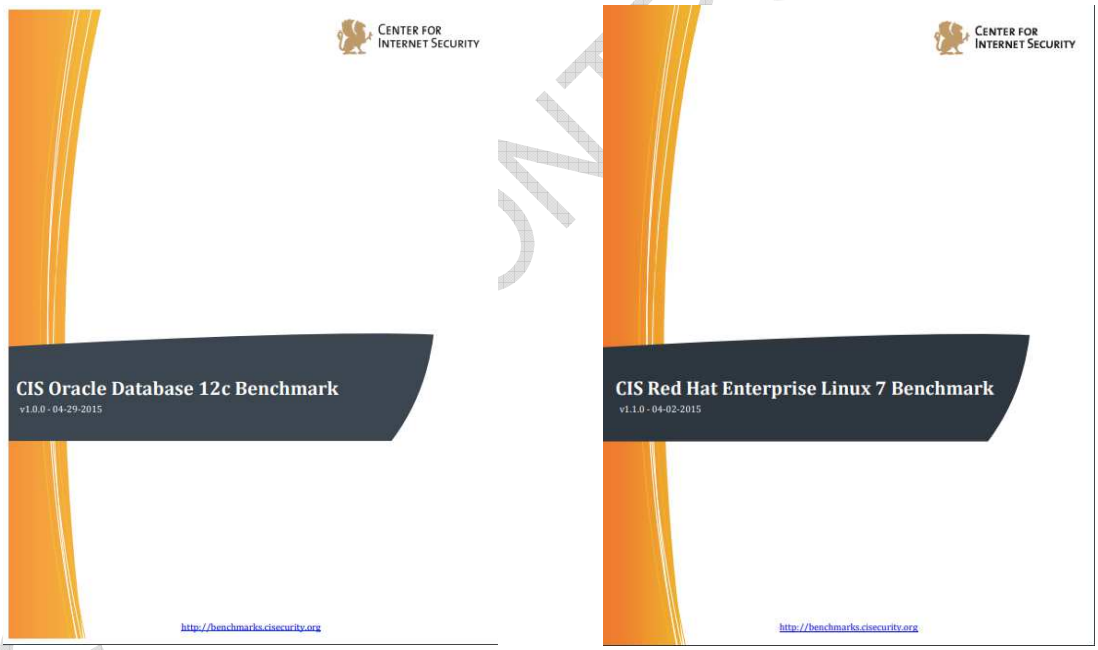
Con base en la arquitectura del sistema de información o elementos de la plataforma tecnológica a inspeccionar, el Grupo de Trabajo de Informática Forense y Seguridad Digital debe seleccionar de forma apropiada las guías de referencia de seguridad (benchmark) que apoyen la inspección de los elementos más importantes del sistema de información o elementos de la plataforma tecnológica, tales como: sistemas operativos, servidores web, bases de datos, entre otros. Se recomienda utilizar las guías proporcionadas por el Centro para la Seguridad de Internet (CIS)[1], entre las cuales se encuentras las siguientes:

[1] Los benchmark del CIS se distribuyen de forma gratuita para propagar su uso y adopción en todo el mundo, son las únicas guías de configuración de seguridad basadas las mejores prácticas, desarrolladas y aceptadas por sectores de gobierno, empresas, industria y la academia. Disponibles en: https://www.cisecurity.org/cis-benchmarks/

- Navegadores web.
- Dispositivos móviles.
- Dispositivos de red.
- Sistemas operativos.
- Servidores y servicios.
- Plataformas de virtualización y nube.
- Herramientas ofimáticas.

La inspección de sistemas de información o elementos de la plataforma tecnológica puede apoyarse de la utilización de scripts o herramientas especializadas, siempre y cuando se sigan las directrices expuestas en el apartado 4.1 de este documento.

A manera ilustrativa se presentan las carátulas de los benchmark de Oracle Database 12c y Red Hat Enterprise Linux 7.



Fuente: https://www.cisecurity.org/cis-benchmarks/

4.4 PRESENTAR LOS RESULTADOS

Una vez realizada la respectiva inspección e identificadas las posibles amenazas y vulnerabilidades del sistema de información, el Grupo de Trabajo de Informática Forense y Seguridad Digital deberá consolidar los resultados, presentarlos en

primera instancia a las coordinaciones de todos los grupos de trabajo de la OTI involucrados para su revisión. En caso de no haber observaciones se presentan los hallazgos a la jefatura del OTI para la respectiva toma de decisiones. El informe debe contener al menos los siguientes ítems:

a) Objetivo: Describir la finalidad de la inspección.
b) Alcance: Describir el alcance definido.
c) Desarrollo: Describir la metodología seguida para la inspección.
d) Hallazgos: Describir las vulnerabilidades y amenazas encontradas.
e) Recomendaciones: Describir el concepto desde el punto de vista de seguridad y las recomendaciones derivadas de la inspección.

5 DOCUMENTOS RELACIONADOS

SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información - SGSI.
SC05-F04 Inspección de aspectos generales de seguridad en sistemas de información.

6 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

N/A - Creación del documento.

Fin documento