CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador del Grupo Informática Forense y Seguridad Digital.	Nombre: Jaroslav Marlen López Chávez. 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: 2024-04-10

1 OBJETIVO

Establecer las directrices generales para realizar las configuraciones de software requeridas a nivel de seguridad de la información, con el fin de prevenir y proteger las herramientas tecnológicas de la Superintendencia de Industria y Comercio; a través del desarrollo de las actividades descritas en este documento, las cuáles serán gestionadas por los servidores públicos o contratistas asignados en la Oficina de Tecnología e Informática.

2 DESTINATARIOS

Este instructivo está dirigido a los servidores públicos, contratistas y terceros directos o indirectos de la Superintendencia de Industria y Comercio, que participen con la gestión de seguridad de la información.

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 GENERALIDADES

Este instructivo se realiza con el fin de verificar y asegurar los elementos de seguridad de la información de las plataformas tecnológicas y sistemas de información de la SIC, con el propósito de tomar las acciones respectivas para la mitigación de posibles vulnerabilidades, a fin de ser gestionadas por la Oficina de Tecnología e Informática.

5 DESCRIPCION DE ACTIVIDADES

La Oficina de Tecnología e Informática, con el propósito de prevenir y proteger las plataformas tecnológicas y los sistemas de información de la entidad en seguridad de la información, considera necesario que se tengan en cuenta las siguientes actividades:

- Diligenciamiento el formato SC05-F04 lista de lineamientos de seguridad de la información y plataformas tecnológicas, con el fin de dar cumplimiento de las configuraciones de seguridad y (Hardening).
- Ejecución de las actividades mismas para la detención de posibles vulnerabilidades en las plataformas tecnológicas de la entidad y los sistemas de información.
- Como segunda línea de defensa hacer seguimiento a las actividades realizadas para la identificación y mitigación de las posibles amenazas y vulnerabilidades de las plataformas tecnológicas y sistemas de información de la entidad.

5.1 HACER LA VERIFICACIÓN DE LA APLICACIÓN DE LA LISTA DE LINEAMIENTOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN Y PLATAFORMAS TECNOLÓGICAS

5.1.1 Reconocimiento general del sistema de información o plataforma tecnológica.

Los servidores públicos o contratistas designados por la OTI, deben aplicar la lista de chequeo descrita en el formato SC05-F04 lista de lineamientos de seguridad de la información y plataformas tecnológicas, la cual incluye temas relacionados con arquitectura, contingencia, autenticación, trazabilidad, seguridad perimetral, comunicaciones, actualizaciones, entre otros y con las evidencias que se consideren necesarias a fin de verificar la implementación de controles o identificar aspectos 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.

5.1.2 Guía de hardening

Teniendo en cuenta lo anterior, con el apoyo de los grupos de trabajo de la Oficina de Tecnología e Informática, y en base en la arquitectura del sistema de información o elementos de la plataforma tecnológica, se deben seleccionar de forma apropiada las guías de referencia de seguridad (NIST, CIS, SANS o incluso propias construidas por el Fabricante), que apoyen las configuraciones de los elementos más importantes del sistema de información o plataforma tecnológica, tales como: sistemas operativos, servidores web, bases de datos, entre otros.

El formato SC05-F04 lista de lineamientos de seguridad de la información y plataformas tecnológicas, se debe enviar al grupo de Informática Forense y Seguridad Digital, con el fin de revisar los controles de seguridad aplicados a la plataforma tecnológica o sistemas de información.

5.2 EJECUTAR LAS ACTIVIDADES PARA LA DETECCIÓN DE POSIBLES VULNERABILIDADES.

De acuerdo con la actividad anterior y con el apoyo de las actividades definidas en los procesos y procedimientos liderados por la Oficina de Tecnología e Informática, (Procedimiento Ciclo de vida de construcción de software GS03-P03, Procedimiento Requisitos y pruebas de seguridad en el desarrollo de sistemas de información GS03-P05, Procedimiento gestión de vulnerabilidades técnicas GS01-P10), se deben realizar las siguientes actividades:

5.2.1 Escaneo de vulnerabilidades a la infraestructura de la Superintendencia de Industria y Comercio.

El Centro de Servicios Integrados de TI – CSIT, de acuerdo con las actividades definidas en el Procedimiento gestión de vulnerabilidades técnicas GS01-P10, se realiza la identificación, clasificación y remediación las posibles vulnerabilidades detectadas en la infraestructura tecnológica de la entidad.

5.2.2 Escaneo de vulnerabilidades a los diferentes sistemas de información de la entidad previo al paso a producción.

En las etapas de los procedimientos se define "*…7.5.4 Efectuar análisis de vulnerabilidades…"* del procedimiento de Ciclo de vida de construcción de software GS03-P03 y "*…7.2.2 Identificar y analizar vulnerabilidades del sistema de información, previo al paso a producción…*" en el procedimiento de Requisitos y pruebas de seguridad en el desarrollo de sistemas de información GS03-P05.

5.2.3 Análisis de código estático a los sistemas de información de la entidad.

Asimismo, en los procedimientos se define el análisis de código estático en los numerales "*…7.4.6 Someter los componentes de software a análisis de vulnerabilidades…"* Procedimiento Ciclo de vida de construcción de software GS03-P03 y "*…7.2.1 Identificar y corregir vulnerabilidades en etapas tempranas del desarrollo del sistema de información…*", Procedimiento de Requisitos y pruebas de seguridad en el desarrollo de sistemas de información GS03-P05.

De acuerdo con lo anterior, para el ítem 5.2.2 y 5.2.3 y con el apoyo de los grupos de trabajo suscritos a la OTI, se gestiona el desarrollo de las actividades y respectivos entregables según lo establecido en los procedimientos.

5.3 REALIZAR EL SEGUIMIENTO DE LAS ACTIVIDADES REALIZADAS PARA LA DETECCIÓN DE POSIBLES VULNERABILIDADES.

Una vez realizada la respectiva identificación de las posibles amenazas y vulnerabilidades de las plataformas tecnológicas y sistemas de información de la entidad, la Oficina de Tecnología e Informática con el apoyo del Grupo de Trabajo de Informática Forense y Seguridad Digital, deberá gestionar con los grupos de trabajo de la OTI involucrados, las vulnerabilidades detectadas para su revisión y mitigación, según lo establecido en los procedimientos anteriormente nombrados.

Nota: Los insumos que se tendrán en cuenta son:

- Análisis de Código Estático en la herramienta aprovisionada por la entidad.

- Escaneo de Vulnerabilidades (GS01-F23 Informe de análisis de vulnerabilidades) de los sistemas de información, generado por el Grupo de Informática Forense y Seguridad Digital.
- Escaneo de Vulnerabilidades Cuatrimestral a la infraestructura de la SIC, teniendo en cuenta los informes técnicos con los resultados y remediaciones, generados por el Centro de Servicios Integrados de TI.

6 DOCUMENTOS RELACIONADOS

SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información - SGSI.
SC05-F04 Lista de lineamientos de seguridad en sistemas de información y plataformas tecnológicas.
GS03-P03 Ciclo de vida de construcción de software.
GS03-P05 Requisitos y pruebas de seguridad en el desarrollo de sistemas de información.
GS01-F23 Informe de análisis de vulnerabilidades.
GS01-P10 Procedimiento gestión de vulnerabilidades técnicas

6.1 DOCUMENTOS EXTERNOS

Guías de referencia de seguridad (NIST, CIS, SANS o incluso propias construidas por Fabricante).

7 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Actualización de los ítems en general y versionamiento del formato del instructivo publicado en el SIGI.

_____

Fin documento