CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Yeison Humberto Latorre Ruiz Cargo: Coordinador del Grupo de Trabajo de Servicios Tecnológicos	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: 2020-08-xx

1 OBJETIVO

Identificar, clasificar y remediar las vulnerabilidades en la infraestructura tecnológica, para salvaguardar la información de la entidad frente a posibles brechas de seguridad existentes, a través de lineamientos específicos para gestionar vulnerabilidades técnicas, los cuales se detallan en este procedimiento.

2 DESTINATARIOS

Este documento aplica para los servidores públicos y/o contratistas de la Oficina de Tecnología e Informática - OTI.

3 GLOSARIO

AMENAZA: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

CSIT: Centro de Servicios de Tecnología de Información.

CVE: Common Vulnerabilitis and Exposures, es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación, descripción de la vulnerabilidad, versiones del software afectadas, posible solución al fallo (si existe) y referencias.

RIESGO: posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

SOC: Centro de Operaciones de Seguridad.

VULNERABILIDAD: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos de Información.

4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Decreto	1008 del 14 de junio de 2018	Política de Gobierno Digital	Artículo 2.2.9.1.1.1 al 2.2.9.1.4.2	Aplicación total
NTC-ISO-IEC	27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos	Aplicación Total	Aplicación total

5 GENERALIDADES

La gestión de vulnerabilidades técnicas es un control tecnológico que tiene como finalidad minimizar los vectores de ataque a la infraestructura tecnológica y disminuir la probabilidad de afectación de la información de la Entidad.

A través de este documento se da a conocer una serie de pasos que abarcan temas de planeación, ejecución, reporte y remediación de las vulnerabilidades, mediante la administración y ejecución de escaneos con herramientas especializadas.

5.1 POLITICAS DEL PROCEDIMIENTO

5.1.1. La identificación de vulnerabilidades no debe interrumpir el cumplimiento de las actividades misionales de la entidad.

5.1.2. El CSIT debe realizar escaneos de vulnerabilidades a la plataforma tecnológica (3) tres veces al año (1 test principal y 2 re-test), o por solicitud del Coordinador del Grupo de Trabajo de Servicios Tecnológicos o el Oficial de seguridad de la información en el momento que se requiera.

5.1.3. El Coordinador del Grupo de Trabajo de Servicios Tecnológicos debe asegurarse que el CSIT mantenga un listado actualizado de vulnerabilidades de la plataforma tecnológica de la entidad, incluyendo el plan de remediación.

5.1.4. Todas las vulnerabilidades críticas y altas deben remediarse, a menos que haya una razón técnica que lo impida, la justificación cual debe ser conocida y aprobada por

el Oficial de seguridad de la información y ser tenida en cuenta en el mapa de riesgos institucional. Para las vulnerabilidades de nivel media o bajo, será el Oficial de seguridad de la información quien defina si requiere o no remediación.

5.1.5. El Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue deberá presentar un resumen ejecutivo del resultado de la gestión de vulnerabilidades de TI al comité técnico de la OTI.

5.1.6. El Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue realiza el seguimiento y verificación de que el CSIT hayan corregido las vulnerabilidades técnicas, mediante los informes mensuales presentados en por el SOC.

5.1.7. Toda acción tomada para la remediación de una vulnerabilidad técnica en el ambiente productivo, deberá surtir el procedimiento de gestión de cambio tecnológico.

5.2 ROLES Y RESPONSABILIDADES

Dueño del Servicio: Jefe de la Oficina de Tecnología e Informática o quién este delegue.

- Conocer el estado de la plataforma tecnológica en relación a las vulnerabilidades técnicas.
- Proporcionar los recursos para remediar las vulnerabilidades técnicas, de ser requerido.
- Aprobar los cambios realizados al presente procedimiento.

Oficial de Seguridad de la Información: Profesional de la Oficina de Tecnología e Informática- OTI.

- Revisa que las políticas del presente procedimiento se encuentren alineadas con el documento SC05-I01 Políticas del sistema de gestión de seguridad de la información – SGSI.
- Revisar y emitir observaciones al plan de trabajo para la ejecución de los escaneos de vulnerabilidades de la plataforma de tecnológica de la SIC.
- Revisar los planes de remediación de vulnerabilidades de la plataforma de Tecnológica.

Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue: Profesional de la Oficina de Tecnología e Informática- OTI.

- Asegurar que el procedimiento fue definido y documentado.

- Responsable de la supervisión del escaneo durante la ejecución de las pruebas, debe aprobar los planes de trabajo conjuntamente con el Oficial de Seguridad y asegurar el cumplimiento de los prerrequisitos para su ejecución.
- Su participación es requerida en la evaluación de los resultados del escaneo y la aprobación del plan de trabajo para la remediación.
- Monitorear la ejecución de los planes de remediación de las vulnerabilidades.

CSIT: Equipo de Seguridad (SOC).

- Responsable de la ejecución operativa del procedimiento de gestión de vulnerabilidades.
- Gestionar la correcta funcionalidad de las herramientas de análisis de vulnerabilidades definidas.
- Velar por la correcta funcionalidad o actualización de las herramientas de análisis de vulnerabilidades definidas por la SIC.
- Definir el plan de trabajo para la ejecución de los escaneos de vulnerabilidades.
- Notificar las vulnerabilidades encontradas.
- Subsanar las vulnerabilidades encontradas según el plan de remediación aprobado.

5.3 INTEGRACION CON OTROS PROCEDIMIENTOS

- GS01-P08 Procedimiento de gestión de cambios: La remedición de vulnerabilidades puede requerir realizar cambios tecnológicos en el ambiente productivo.

- SC05-P01 Procedimiento de gestión de incidentes de seguridad de la información: cuando una vulnerabilidad es explotada el evento será crítico y posiblemente se presente una caída del servicio, en este caso el evento se debe convertir a un incidente.

- SC05-I06 Instructivo para la inspección de seguridad en sistemas de información: el conjunto de actividades descritas en el instructivo son un control enfocado en labores de auditoría técnica o inspección de un elemento puntual de la plataforma de tecnológica y se complementa con el presente procedimiento para obtener un nivel de seguridad robusto.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	**PLANEAR EL ESCANEO DE VULNERABILI-DADES**	Inventario de infraestructura Tecnológica.	Teniendo en cuenta el Inventario de infraestructura Tecnológica el CSIT define y presenta para aprobación el plan de trabajo para escanear la infraestructura Tecnológica de la SIC En esta etapa se desarrollan las siguientes actividades: - Definir y presentar el plan de trabajo - Revisar y aprobar el plan de trabajo.	CSIT Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue. Oficial de Seguridad de la información.	Plan de trabajo aprobado.
2	**EJECUTAR EL ESCANEO Y PRIORIZAR VULNERABILI-DADES**	Plan de Trabajo aprobado	Según el plan de trabajo aprobado, se ejecuta, revisa y presenta los resultados del escaneo de vulnerabilidades sobre los servidores, equipos de cómputo, almacenamiento, elementos de red y demás componentes de infraestructura tecnológica. En esta etapa se desarrollan las siguientes actividades: - Ejecutar el escaneo de vulnerabilidades. - Revisar el resultado del escaneo. - Presentar informe con los resultados priorizados.	CSIT Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue. Oficial de Seguridad de la información	Informe técnico y ejecutivo con los resultados del escaneo de vulnerabilidades.
3	**REMEDIAR LAS VULNERABILI-DADES**	Informe técnico con el resultado del escaneo de vulnerabilidades.	Con el informe de resultados del escaneo de vulnerabilidades se diseña, aprueba y ejecuta el plan de remedición, teniendo en cuenta el nivel de priorización de las vulnerabilidades. En esta etapa se desarrollan las siguientes actividades:	CSIT Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue.	Plan de remediación de vulnerabilidades Informe mensual de seguimiento.

No.	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
			- Diseñar y aprobar el plan de remediación de vulnerabilidades. - Ejecutar el plan de remediación aprobado.	Oficial de Seguridad de la información	
4	**VALIDAR LA REMEDIACIÓN DE VULNERABILI-DADES**	Plan de remediación de vulnerabilidades.	Se valida la subsanación las vulnerabilidades mediante los re-test aprobados en el plan de trabajo. En esta etapa se desarrollan las siguientes actividades: - Solicitar autorización para la ejecución de re-test. - Presentar y revisar los resultados del re-test.	CSIT Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue. Oficial de Seguridad de la información	Informe con el resultado del re-test de vulnerabilidades. Plan de remediación de vulnerabilidades actualizado.

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

A continuación se describen las etapas que hacen parte del procedimiento

7.1 PLANEAR EL ESCANEO DE VULNERABILIDADES

7.1.1 Definir y presentar el plan de trabajo

El CSIT debe diseñar el plan de trabajo para la ejecución del escaneo de vulnerabilidades, remedición y re-test, el cual incluya, objetivos, alcance, metodología, el listado de elementos de la infraestructura tecnológica, cronograma de actividades, fecha de re-test, descripción de las herramientas a utilizar, responsables, riesgos y acciones de mitigación a implementar.

El plan de trabajo debe ser remitido a través de correo electrónico al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o quien él delegue y al Oficial de seguridad de la información.

7.1.2 Revisar y aprobar el plan de trabajo.

Una vez recibido el plan de trabajo, el Coordinador del Grupo de Trabajo de Servicios Tecnológicos se debe revisar su completitud y coherencia de documento para ser socializado al comité técnico de la OTI para su conocimiento y observaciones pertinentes. En la revisión también participa el Oficial de seguridad

de la información quien debe emitir sus observaciones principalmente enfocadas en los riesgos identificados en el plan de trabajo.

De existir observaciones deben ser remitidas al CSIT para su ajuste o aclaración. Surtido este flujo, el Coordinador del Grupo de Trabajo de Servicios Tecnológicos remite la aprobación del plan de trabajo. Con esta aprobación la Mesa de servicios procede a crear el caso en la herramienta de gestión.

7.2 EJECUTAR EL ESCANEO Y PRIORIZAR VULNERABILIDADES

7.2.1 Ejecutar el escaneo de vulnerabilidades.

De acuerdo con el cronograma y una vez aplicados las acciones de mitigación de los riesgos documentados en el plan de trabajo aprobado, el CSIT inicia el escaneo de vulnerabilidades sobre la plataforma tecnológica de la SIC.

El CSIT reporta al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue, todas las novedades que surjan durante la actividad, incluyendo: inicio, afectaciones no previstas y finalización de la actividad. Lo anterior con el fin de tomar acciones oportunas, según sea la situación, llegando inclusive a autorizar la cancelación de la actividad.

7.2.2 Revisar el resultado del escaneo.

Una vez finalizado el escaneo de vulnerabilidades, el CSIT organiza los resultados emitidos por las herramientas, incluyendo: lista de las vulnerabilidades según el nivel de criticidad, asociar los elementos afectados, CVE, sistema de información asociado, descartar falsos positivos.

7.2.3 Presentar informe con los resultados priorizados.

Una vez revisados los resultados del escaneo, el CSIT construye un informe ejecutivo y un informe técnico con los resultados priorizados y las recomendaciones para la subsanación, el cual se remite al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue y al Oficial de seguridad de la información.

7.3 REMEDIAR LAS VULNERABILIDADES

7.3.1 Diseñar y aprobar el plan de remediación de vulnerabilidades.

Una vez remitido el informe con el resultado del escaneo de vulnerabilidades, el CSIT procede a diseñar el plan de remediación, para lo cual se tiene en cuenta que

se debe dar prioridad a las vulnerabilidades de nivel crítico y alto, así como a aquellos elementos de la infraestructura tecnológica que soporten aplicaciones críticas de la SIC, según el análisis BIA con el que cuente la OTI.

Adicionalmente, para la definición del cronograma se debe tener en cuenta que se realizarán 2 re-test.

Construido el plan de remediación, éste se remite al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue y al Oficial de seguridad de la información, quienes emitirán su aprobación, previa socialización tanto del informe ejecutivo como del plan de remediación al comité técnico de la OTI.

7.3.2 Ejecutar el plan de remediación aprobado.

El CSIT ejecuta el plan de remediación aprobado, teniendo en cuenta que puede requerirse realizar cambios tecnológicos en el ambiente productivo, los cuales deben surtir las etapas del procedimiento GS01-P08 Procedimiento de gestión de cambios.

Si los ajustes no cumplen con los criterios para ser considerado un cambio tecnológico, únicamente se procede a crear el caso en la herramienta de gestión y ejecutar la actividad definida.

El CSIT mantiene informado al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue, sobre el estado de las actividades del plan de remediación y consolida los avances de la subsanación de las vulnerabilidades en el informe mensual de seguimiento.

7.4 VALIDAR LA REMEDIACIÓN DE VULNERABILIDADES

7.4.1 Solicitar autorización para la ejecución de re-test.

Según lo previsto en el plan de trabajo aprobado (véase actividad 7.1.2 Revisar y aprobar el plan de trabajo), el CSIT solicita autorización al Coordinador del Grupo de Trabajo de Servicios Tecnológicos o a quien él delegue para ejecutar el re-test, cuyo alcance busca comprobar si las vulnerabilidades fueron subsanadas, según el plan de remediación y encontrar nuevas vulnerabilidades.

7.4.2 Presentar y revisar los resultados del re-test.

El CSIT remite al Coordinador del Grupo de Trabajo de Servicios Tecnológicos y al Oficial de seguridad de la información, el informe de resultados del re-test que

corrobore que las vulnerabilidades fueron subsanadas según lo programado en el plan de remedición.

De encontrarse que las vulnerabilidades persisten o nuevas vulnerabilidades, el CSIT actualiza el informe de vulnerabilidades y el plan de remediación, regresa a la etapa 7.3.

8 DOCUMENTOS RELACIONADOS

GS01-P08 Procedimiento de gestión de cambios.
SC05-P01 Procedimiento de gestión de incidentes de seguridad de la información.
SC05-I01 Políticas del sistema de gestión de seguridad de la información – SGSI.

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

Creación del documento.

Fin documento