Pruebas de vulnerabilidad

MacroProceso	Gestión tecnológica	Proceso	Gestión de servicios tecnológicos	Estado	Vigente

Contenido

1. OBJETIVO	2. ALCANCE
Asegurar los activos de información tecnológicos mediante la identificación, análisis, evaluación, priorización, remediación y seguimiento de las vulnerabilidades presentes en la infraestructura tecnológica, con el fin de reducir la exposición y superficie a riesgos de ciberseguridad, fortalecer la confidencialidad, integridad y disponibilidad de la información, y contribuir a la continuidad, mejora continua y confiabilidad de los servicios tecnológicos.	Inicia con el levantamiento de información para definir el plan de pruebas de vulnerabilidades, continúa con la elaboración y validación del plan, la ejecución de las pruebas de vulnerabilidades y finaliza con la entrega de los informes de resultados, propuesta del plan de tratamiento y el resultado.

3. DEFINICIONES

- **Activos Tecnológicos:** son los recursos de hardware, software, servicios y componentes de infraestructura que soportan el procesamiento, almacenamiento, transmisión y acceso a la información institucional. Entre ellos se encuentran:
  - Equipo de cómputo: Dispositivo electrónico destinado al procesamiento de información y ejecución de aplicaciones, como computadores de escritorio y portátiles.
  - Servidor: Equipo físico o virtual diseñado para proporcionar servicios, recursos o aplicaciones a otros dispositivos conectados a una red.
  - Dispositivo móvil: Equipo portátil con capacidad de procesamiento y conectividad, como teléfonos inteligentes, tabletas o dispositivos similares.
  - URL (Uniform Resource Locator): Dirección única que permite localizar y acceder a recursos o servicios disponibles en una red, especialmente en Internet.
  - Aplicación: Programa o conjunto de programas informáticos desarrollados para ejecutar funciones específicas y apoyar los procesos institucionales.
  - Impresora: Dispositivo periférico que permite reproducir información digital en formato físico.
  - Router (Enrutador): Equipo de red encargado de dirigir el tráfico de datos entre diferentes redes, permitiendo la comunicación entre ellas.
  - Gateway (Puerta de enlace): Dispositivo o sistema que facilita la interoperabilidad y comunicación entre redes o sistemas con características distintas.
  - Switch (Conmutador): Dispositivo de red que conecta equipos dentro de una misma red local y administra el tráfico de datos entre ellos.
  - Access Point (Punto de acceso): Dispositivo que proporciona conectividad inalámbrica a una red, permitiendo la conexión de equipos mediante tecnología Wi-Fi.
  - Nube (Cloud Computing): Modelo de prestación de servicios tecnológicos que permite acceder, a través de internet, a recursos de procesamiento, almacenamiento, redes y aplicaciones gestionados por terceros o por la misma organización.
- **Administrador de componentes informáticos:** Persona responsable de administrar cada elemento (hardware, software y aplicaciones de la Entidad) del inventario de activos del Icetex y de remediar vulnerabilidad(es) que será(n) escalada(s) por el asesor de seguridad.
- **Análisis y Clasificación:** Las vulnerabilidades serán clasificadas como:
  - **Crítica:** Vulnerabilidad que puede ser explotada de forma remota o automática y que tiene un impacto muy alto sobre los activos institucionales, pudiendo comprometer la confidencialidad, integridad o disponibilidad de la información. Su explotación permite un control total del sistema o la interrupción grave de los servicios.
  - **Alta:** Vulnerabilidad que puede ser explotada con relativa facilidad y que afecta de manera significativa los activos institucionales. Su explotación puede permitir acceso no autorizado, modificación de información o afectación relevante a la disponibilidad de los servicios, aunque pueda requerir interacción del usuario o algún nivel de acceso previo.
  - **Media:** Vulnerabilidad que requiere condiciones específicas para ser explotada o cuyo impacto es moderado. Puede permitir exposición limitada de información, alteraciones menores o afectaciones parciales a la operación, generalmente sin comprometer directamente los activos críticos.
  - **Baja:** Vulnerabilidad con bajo impacto y dificultad de explotación alta. Su materialización no afecta de manera significativa la confidencialidad, integridad o disponibilidad de la información institucional.
- **Analizador de vulnerabilidades:** Es una herramienta de seguridad informática que se utiliza para detectar fallos de seguridad en los distintos elementos tecnológicos del inventario de la entidad, incluye hardware y software.
- **Asesor de Seguridad Informática:** Es la persona responsable de asesorar proyectos de seguridad informática, asignados por la Dirección de Tecnología, implementar y administrar plataformas de seguridad informática, entre otras actividades que sean acordes al rol.
- **CMDB (Base de datos de la gestión de configuración):** Es una base de datos que contiene detalles relevantes de cada componente informático y de la relación entre ellos, incluyendo equipos híbridos, software y la interdependencia entre incidencias, problemas, cambios y otros datos del servicio de tecnologías de la información.
- **Coordinador de Infraestructura:** Es la persona responsable de liderar la gestión de la infraestructura tecnológica del instituto tal como seguridad informática, telecomunicaciones, microinformática, administración de los servidores, en la organización.

- **Escaneo de vulnerabilidades (test):** Es una actividad que permite realizar un análisis, verificación y reporte de las vulnerabilidades de seguridad en los componentes de la infraestructura tecnológica.

- **Evaluación del Riesgo:** Análisis que permite determinar el nivel de riesgo de una vulnerabilidad con base en su probabilidad de explotación, el impacto institucional y los controles implementados. Se realizará análisis de riesgo considerando:

  o **Probabilidad de explotación:** Probabilidad de que una amenaza o vulnerabilidad sea aprovechada y genere un evento de riesgo.
  o **Impacto institucional:** Consecuencias que la materialización del riesgo podría ocasionar sobre la operación, los activos, la información, los servicios o el cumplimiento de los objetivos institucionales.
  o **Controles existentes:** Medidas y/o mecanismos implementados para prevenir, detectar o reducir la probabilidad de ocurrencia y/o el impacto del riesgo.
  El resultado determinará el tipo de tratamiento.

- **Falso Negativo:** Es un error mediante el cual un software de análisis de vulnerabilidades falla en detectar vulnerabilidades existentes en un sistema, aplicación o bases de datos.

- **Falso Positivo:** Es un error por el cual un software de análisis de vulnerabilidades reporta que un sistema, aplicación o base de datos presenta una falla de seguridad, cuando en realidad ésta no existe.

- **Inventario de activos tecnológicos:** Registro actualizado, completo y controlado de los activos tecnológicos (hardware, software, sistemas operativos, aplicaciones, servicios, dispositivos de red, máquinas virtuales, bases de datos y demás componentes tecnológicos) que hacen parte del alcance del proceso de gestión de vulnerabilidades. Este inventario constituye la base para la identificación, evaluación, priorización, tratamiento y seguimiento de las vulnerabilidades de seguridad.

- **Mesa Técnica de Vulnerabilidades:** Es un órgano interno, donde se presentan los planes, las vulnerabilidades, los resultados del análisis de vulnerabilidades y el tratamiento dado a cada una de ellas.

- **Nube:** Infraestructura y servicios tecnológicos alojados en entornos externos y accesibles mediante internet.

- **Retest:** Consiste en realizar nuevamente un test para verificar si las vulnerabilidades detectadas en un análisis aplicado con anterioridad fueron solucionadas.

- **SOC:** Unidad especializada encargada de la monitorización continua, detección, análisis y respuesta ante incidentes de seguridad con el fin de proteger la confidencialidad, integridad y disponibilidad de la información institucional.

- **Tratamiento:** Consiste en actualizar, desinstalar o configurar el software para mitigar, aceptar, transferir y compensar vulnerabilidades informáticas mediante los tratamientos aplicados.

- **Vulnerabilidad:** Debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso o consistencia del sistema, de sus datos o aplicaciones.

4. CONDICIONES GENERALES

4.1. Se deberá contar con un profesional con el rol de Asesor de Seguridad Informática o quien haga sus veces de la Dirección de Tecnología, quien será el encargado de brindar apoyo en la gestión del procedimiento de pruebas de vulnerabilidades.

4.2. La gestión de vulnerabilidades comprende las vulnerabilidades técnicas presentes en la infraestructura tecnológica de la Entidad, incluyendo equipos de cómputo, servidores, dispositivos de red, servicios en la nube, sistemas de información, aplicaciones y demás componentes tecnológicos que soportan la prestación de los servicios institucionales. Deben estar actualizados por los respectivos responsables, cada vez que se realice una adición, actualización y/o eliminación de las vulnerabilidades.

4.3. En caso de identificar una vulnerabilidad técnica la cual no pueda ser subsanada por la Dirección de Tecnología, ya sea por ser compartida con otro grupo o área de la entidad o con un fabricante, y con este último no se tenga soporte contratado, se deben evaluar los riesgos relacionados con la vulnerabilidad y notificar a la Oficina de Riesgos para tomar las acciones pertinentes que conlleven a mitigar la vulnerabilidad técnica identificada o evaluar los medios de aceptación del riesgo cuando aplique, con su respectivo sustento técnico.

4.4. Las evidencias de un análisis de vulnerabilidades y el respectivo informe, será información considerada como confidencial y, por ende, así se tratarán estos documentos. Se utilizará cifrado de documentos. No se harán entregas en medios magnéticos extraíbles y/o digitales de almacenamiento. Toda la documentación relacionada con las pruebas de vulnerabilidades deberá ser consignada y almacenada en el sitio designado para tal fin; de acuerdo con el inventario de activos de información de la Dirección de Tecnología.

4.5. En el primer trimestre de cada año, el profesional con el rol de asesor de Seguridad Informática o quien haga sus veces de la Dirección de Tecnología, deberá realizar una socialización inicial a la Mesa Técnica de Vulnerabilidades y todos los involucrados. Esta presentación incluirá los resultados de la gestión de vulnerabilidades del año anterior, el cronograma anual de pruebas para el año en curso, así como los resultados obtenidos de las pruebas ejecutadas durante el primer trimestre. Las pruebas de vulnerabilidades deberán realizarse trimestralmente, siguiendo el cronograma establecido.

4.6. Las reuniones de la mesa técnica de vulnerabilidades se programarán trimestralmente. A partir de la segunda sesión, se presentarán las actividades propuestas en el plan de tratamiento y remediación para su revisión, verificación y ajuste. En cada reunión, se informarán los avances en la mitigación de las vulnerabilidades reportadas en el acta anterior, los hallazgos correspondientes al periodo actual, las conclusiones y compromisos derivados del escaneo realizado, así como la programación del siguiente ciclo de pruebas.

4.7. Se gestionará el tratamiento inmediato para las vulnerabilidades clasificadas como críticas, altas y medias. Para las vulnerabilidades catalogadas como bajas o informativas, su tratamiento será opcional y dependerá de la disponibilidad de recursos.

4.8. La gestión de la solución a las vulnerabilidades deberá realizarse en conjunto con todos los actores internos y externos involucrados, tales como administradores de

aplicaciones y dispositivos, entidades de seguridad estatales, usuarios funcionales, jefes de área, coordinadores, proveedores y/o relacionados.

4.9. En caso de que el administrador de la plataforma lo considere pertinente, cualquier modificación necesaria para la remediación deberá gestionarse bajo el "Procedimiento de Control de Cambios y despliegue" (A7-1-12) Cuando el análisis de vulnerabilidades sea realizado por entes externos, sus resultados deberán incorporarse en el plan de tratamiento.

4.10. En caso de presentarse situaciones que puedan generar un alto impacto en la gestión de vulnerabilidades, estas deberán ser notificadas a la Vicepresidencia de Operaciones y Tecnología, para que se definan las acciones pertinentes y se tomen las decisiones correspondientes.

4.11. Se cuenta con varias fuentes de información y otros medios que emiten comunicados y/o boletines referentes a vulnerabilidades que pueden llegar a materializarse. Entre ellos, los más relevantes son los siguientes:

- Boletines de Seguridad (CSIRT Policia Nacional, CSIRT Gobierno, ColCERT, DigiCSIRT, CISA, NIST,CVE, Microsoft Defender for Cloud, entre otros)
- Fabricantes sistemas operativos (Microsoft, Linux)
- Componentes de aplicaciones (PHP, Apache, Tomcat)
- Fabricantes bases de datos (Mysql, SQL, Oracle)
- Fabricantes de componentes de seguridad (Fortinet)
- Centro de Seguridad de Operaciones (SOC)

Mesa técnica de vulnerabilidades

4.12. Integrantes de la Mesa Técnica de Vulnerabilidades**:** Harán parte de la mesa los siguientes roles o sus delegados.

Cargo	**Participación**
Director de Tecnología/ Vicepresidencia de Operaciones y Tecnología (VOT)	Obligatorio
Coordinador de Infraestructura/ Dirección de Tecnología (DT)	Obligatorio
Asesor de Seguridad Informática o quien haga sus veces/ VOT	Obligatorio
Oficial de Seguridad de la Información/ Oficina de Riesgos (ODR)	Obligatorio
Coordinador de Sistemas de Información/ DT	Opcional
Coordinador de Datos e Información/ DT	Opcional
Otros interesados que sean convocados a la reunión	Opcional

4.13. Son funciones de los integrantes de la Mesa técnica de vulnerabilidades:

- Realizar seguimiento a los planes de trabajo orientados al tratamiento de las vulnerabilidades.
- Asistir oportunamente a las sesiones de la Mesa Técnica de Vulnerabilidades agendadas.

5. DESCRIPCIÓN DE ACTIVIDADES

Convenciones:

Actividad de control: **Acuerdo de servicio:**

No.	Descripción	Frecuencia / tiempo máximo	Responsable	Registro o evidencia de la actividad	Actividad de control / Acuerdo de servicio
1	Identifica una muestra de los activos de información a analizar, con base en la CMDB. Pueden ser equipos de cómputo, servidores, dispositivos móviles, URLs, aplicaciones, dispositivos (impresoras, routers, gateways, switch, access point, nube) entre otros, que se determine incluir en el plan de pruebas de vulnerabilidades, para su respectivo análisis.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Listado de activos con la muestra identificada	N/A
2	Elabora el plan de pruebas de vulnerabilidades. Se construye el plan de las pruebas de vulnerabilidades de acuerdo con lo indicado en las condiciones generales.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Plan de pruebas de vulnerabilidades	N/A
3	Socializa el plan de pruebas de vulnerabilidades a la Coordinación de infraestructura, para su revisión.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Correo de socialización y/o citación en Calendar y grabación de reunión en Teams	N/A

4	Realiza la verificación del Plan de pruebas de vulnerabilidades. ¿Requiere ajustes? • Si, regresa a la actividad 2 para realizar los ajustes requeridos. • No, aprueba el plan y continúa con la actividad 5.	Trimestral	Coordinador de infraestructura / Dirección de Tecnología	Plan validado de vulnerabilidades / Aprobación por correo electrónico	
5	Coordina con los diferentes actores para dar inicio a la ejecución de las pruebas, de acuerdo con el cronograma. Además, si se requiere, configura el Analizador de Vulnerabilidades, antes de iniciar la ejecución de las pruebas. Producto de esta configuración se puede ajustar la programación y los objetivos a escanear. ¿Ejecución satisfactoria? • Si, continúa con la actividad 7. • No, continúa con la actividad 6.	Trimestral	Profesional con rol de Asesor de Seguridad Informática / Dirección de Tecnología	Cronograma/ Configuración del Analizador de Vulnerabilidades	N/A
6	Cambia la programación de horarios o ventana de tiempo. Regresa a la actividad 2. La nueva propuesta de programación debe contar con la validación del Coordinador de Infraestructura. Se deben documentar los imprevistos y las causas por las cuales no fue posible realizar las pruebas a través de un informe que será consignado en la siguiente acta de Mesa Técnica de Vulnerabilidades.	Cada vez que se requiera	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Nuevo cronograma / Informe de imprevistos	N/A
7	Genera consolidado de vulnerabilidades y notifica los resultados de las pruebas de vulnerabilidades a los administradores de componentes informáticos. El Asesor de Seguridad Informática, al obtener los reportes de la ejecución de las pruebas de vulnerabilidades, debe notificar a los administradores por medio de la herramienta de gestión, los resultados de las pruebas. Además, debe generar el consolidado de las vulnerabilidades por severidad (criticas, altas y medias) y estado (cerradas, en proceso y atrasadas)	Plazo de 3 a 5 días para notificar los resultados	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Consolidado de vulnerabilidades / Reportes a través de la herramienta de gestión	
8	Analiza las vulnerabilidades encontradas con base en el informe entregado por el Asesor de Seguridad Informática, y determina el tratamiento a seguir. ¿Genera acciones de tratamiento? • Si, continúa con la actividad 10 • No, continúa con la actividad 9.	Trimestral	Administradores de componentes informáticos / Dirección de Tecnología	N/A	N/A
9	Analiza alternativas que permitan aceptar, transferir o mitigar los riesgos asociados. Esta información debe quedar registrada en el acta de la Mesa técnica de vulnerabilidades para su seguimiento. Continúa con la actividad 11.	Trimestral	Administradores de componentes informáticos / Dirección de Tecnología	Correo electrónico/ Herramienta de Gestión	N/A
10	Aplica las acciones de tratamiento y remediación correspondientes. De realizarse adiciones, modificaciones, cualquier cambio a ítems de configuración y/o eliminaciones a los servicios activos de TI, se aplica el "Procedimiento de Control de Cambios y Despliegue" (A7-1-12).	Trimestral	Administradores de componentes informáticos / Dirección de Tecnología	Evidencia de parches, configuraciones, cambios, entre otras, aplicados en el componente	N/A
11	Consolida la información generada por el (los) administrador(es) de elementos informáticos y elabora el informe de resultados de los tratamientos a las vulnerabilidades reportadas. Aplica para todos los casos, exceptuando los informativos.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Informe de resultados de la remediación de vulnerabilidades	N/A
12	Realiza seguimiento a las acciones de mitigación de las vulnerabilidades.	Trimestral	Profesional con rol de Asesor de Seguridad	Correos electrónicos, citaciones y grabaciones	

			Informática o quien haga sus veces/ Dirección de Tecnología	de reuniones de seguimiento	
13	Verifica la eliminación de vulnerabilidades encontradas anteriormente, realizando el Retest. El retest consiste en ejecutar nuevamente las pruebas de vulnerabilidades en los activos analizados y que se establecieron en el plan de tratamiento. También se deben validar los resultados finales de los tratamientos y efectuar recomendaciones finales para futuros ejercicios.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Informe de retest. Informe de validación con recomendaciones	
14	Presenta ante la Mesa Técnica de Vulnerabilidades la información requerida: • Revisión de los compromisos del acta anterior. • Revisión del resultado de los escaneos del trimestre actual. • Métricas de seguimiento de la gestión del procedimiento, tales como: número de vulnerabilidades detectadas, tratadas, pendientes, número de activos escaneados, cumplimiento de plan de pruebas, tiempos estimados de atención, entre otros que se determinen por los integrantes de la Mesa. • Conclusiones y compromisos. • Plan de escaneo del próximo trimestre. • Se deben dejar las alternativas que permitan aceptar, transferir o mitigar los riesgos asociados de las vulnerabilidades que persisten. • Listado de vulnerabilidades que no se pueden remediar junto con la justificación técnica. Toda la información debe quedar registrada en el acta de la Mesa Técnica de Vulnerabilidades.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Acta de Mesa Técnica de Vulnerabilidades en el formato de "Acta general de reuniones" (F05)	
15	Revisa los resultados del escaneo del trimestre anterior, para validar el ajuste del plan de vulnerabilidades a presentar para el siguiente trimestre.	Trimestral	Profesional con rol de Asesor de Seguridad Informática o quien haga sus veces/ Dirección de Tecnología	Informe de escaneo del último trimestre	

6. DOCUMENTOS RELACIONADOS

Nombre del documento	Código
Procedimiento de Control de Cambios y despliegue	A7-1-12

7. ANEXOS

7.1 DIAGRAMA DE FLUJO (Ver Anexo)

7.2 OTROS

No aplica.

Pruebas de vulnerabilidad

MacroProceso	Gestión tecnológica	Proceso	Gestión de servicios tecnológicos	Estado	Vigente

Anexos:

A7-1-11 Pruebas de vulnerablidades V7.png

Editado por Adriana Esperanza Aranguren Prieto, ago 12 2026 04:15 p.m.

Modificaciones

Descripción de cambios

Se modifica la redacción de algunas actividades y se incluyen nuevas condiciones generales. Se cambia al formato F100 en su versión vigente.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2026-08-24	7	Se modifica la redacción de algunas actividades y se incluyen nuevas condiciones generales. Se cambia al formato F100 en su versión vigente.
2020-07-10	6	• se realiza cambios en el objetivo y alcance • En las definiciones se ajustan • Se adicionan reglas generales • Se ajustan las actividades de acuerdo al desarrollo del proceso
2018-7-31	5	Se ajusta la definición de analizador de vulnerabilidades en donde esta es generada por una herramienta dada por el proveedor de servicios. Se agrega la definición de administrador de plataforma. Se agregan las 3 últimas condiciones generales. Se retira de la segunda condición general se clarifica que no se tiene en cuenta "bajas" e "informativas" Se ajusta la actividad #4 en donde se agrega el asesor de seguridad informática. Se ajusta la actividad #6 se retira que el administrador de la plataforma toma los correos generados por el analizador de vulnerabilidades. Se retira de la sección de seguimiento y control el formato de seguimiento de vulnerabilidades y se cambia por el registro en la herramienta de escaneos. ** Los ajustes solicitados no requieren cambiar el diagrama de flujo
2015-07-23	4	• Se ingresa una condición general el cual se verifica el tratamiento en el comité de vulnerabilidades. • En el punto 6 Seguimiento y control en la columna "Evidencia y control" se modificó ingresando "Registro en la Herramienta de Escaneo". No sufre cambios el diagrama de flujo
2014-7-1	3	• Se ingresan nuevos controles modificando todas las actividades, su objetivo y su alcance.
2013-1-15	2	• En el punto 1 objetivo, se suprime "realizar e implementar adecuadamente". • En el punto 2 se modifica totalmente el alcance. • En el punto 3 se ingresan 2 definiciones Coordinador de Infraestructura y Escaneo de vulnerabilidades. • En el punto 5.2 se modificaron todas las actividades, estableciendo nuevas acciones y tareas en las pruebas de vulnerabilidad. • En el punto 6 se ingresa actividad a controlar. • En el punto 7 se ingresan documentos relacionados.
24/6/2010	1.0	-

¿Ha revisado el documento en su totalidad?

SI