Contenido

1. OBJETIVO

Realizar análisis de vulnerabilidades para la identificación de riesgos de seguridad, sobre la infraestructura tecnológica (equipos de cómputo, servidores, dispositivos de red), de aplicaciones y otros que soporten los servicios de la Entidad.

2. ALCANCE

Se inicia con el levantamiento de información para definir el plan de pruebas de vulnerabilidades, continua 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 remediación y el resultado de las remediaciones aplicadas.

3. DEFINICIONES

- **Administrador de componentes informáticos:** Persona responsable de administrar cada elemento (hardware, software y aplicaciones de la Entidad) del parque informático del Icetex y de remediar vulnerabilidad(es) que será(n) escalada(s) por el asesor de seguridad.
- **Analizador de Vulnerabilidades:** Es una herramienta de seguridad informática que se utiliza para detectar fallos de seguridad en los distintos elementos tecnológicos del parque microinformático 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 asignadas al rol.
- **Coordinador de Infraestructura:** Es la persona responsable de liderar la gestión de la infraestructura tecnológica del instituto tales como seguridad informática, telecomunicaciones, microinformática, administración de los servidores, en la organización.
- **Comité 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.
- **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 físicos, software y la relación entre incidencias, problemas, cambios y otros datos del servicio de tecnologías de la información.
- **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.
- **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 bases de datos presenta una falla de seguridad, cuando en realidad ésta no existe.
- **Retest:** Consiste en realizar nuevamente un test para verificar si las vulnerabilidades detectadas en un análisis aplicado con anterioridad, fueron solucionadas.
- **Remediación:** Consiste en actualizar, desinstalar o configurar el software para corregir vulnerabilidades informáticas.
- **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

- Se debe contar con un Asesor de Seguridad Informática o un recurso similar, para que brinde apoyo en la gestión del procedimiento de pruebas de vulnerabilidades.
- Se deberá realizar en el primer trimestre del año una primera socialización, por parte del Asesor de Seguridad Informática al comité de vulnerabilidades y a todos los involucrados, sobre los resultados de la gestión de vulnerabilidades del año anterior, el cronograma anual de las pruebas para el año en curso y los resultados obtenidos en la ejecución de las pruebas realizadas en el primer trimestre.
- Se debe programar trimestralmente las reuniones del comité de vulnerabilidades y a partir del segundo comité se debe mostrar las actividades propuestas del plan de tratamiento/remediación para su respectiva verificación o ajuste.
- Se deberá realizar trimestralmente las pruebas de vulnerabilidades, las cuales deben estar planteadas en el cronograma.
- Se deberá brindar gestión de remediación a las vulnerabilidades catalogadas como críticas, altas y medias. Para las bajas e informativas se puede o no tratar teniendo en cuenta la disponibilidad de recursos para la solución.
- Se debe enviar una notificación de manera urgente, en caso de que se detecte una vulnerabilidad crítica o alta para que se le brinde la respectiva gestión de remediación, a los responsables o administradores de los activos relacionados... Esta notificación deberá ser enviada por el asesor de seguridad informática o quien haga sus veces.

- Se debe trabajar conjuntamente con todos los actores internos y externos (administradores de aplicaciones, administradores de dispositivos, Entidades de seguridad estatales, usuarios funcionales, jefes de área, coordinadores, y demás proveedores involucrados) para brindar solución a las vulnerabilidades halladas.
- Después de realizar el escaneo de vulnerabilidades el Asesor de Seguridad tiene un tiempo de 3 a 5 días para notificar los resultados mediante la herramienta de gestión a los administradores para la remediación de los mismos.
- En dado caso que el administrador de la plataforma lo considere apropiado, se pasará por "Procedimiento de Control de Cambios y despliegue" A7-1-11 la modificación que sea necesaria para la remediación de la vulnerabilidad. Dado caso de realizarse análisis de vulnerabilidades por entes externos, estos deben incluirse en el plan de remediación.
- Se debe consignar en el sitio dispuesto toda la documentación de las pruebas de vulnerabilidades.
- Se debe realizar reunión del comité de vulnerabilidades para informar el resultado de la mitigación de las vulnerabilidades del acta anterior, los resultados de las vulnerabilidades del periodo actual, las conclusiones y compromisos del escaneo actual y escaneo del próximo periodo según programación. Dicho comité debe estar conformado por:

  Integrantes del comité de vulnerabilidades:
  Director de Tecnología
  Coordinador de Infraestructura
  Líder Técnico de Operaciones o quien haga sus veces
  Asesor de seguridad
  Analista de la Oficina de Riesgos o quien haga sus veces.
  Los demás interesados que se convoquen a la reunión.

- El comité de Vulnerabilidades debe ser notificado de los resultados de las vulnerabilidades detectadas en los escaneos y retest realizados a los activos.
- El comité de Vulnerabilidades deber realizar el seguimiento a los planes de trabajo para la gestión de la remediación de las vulnerabilidades
- De presentarse situaciones que generen alto impacto en la gestión de vulnerabilidades, estas deben notificarse a la Vicepresidencia de Operaciones y Tecnología, para determinar las acciones a seguir y toma de decisiones

5. DESCRIPCIÓN

5.1. DIAGRAMA DE FLUJO

(Ver anexo)

5.2. ACTIVIDADES

Asesor de Seguridad Informática / Dirección de Tecnología

Inicio

5.2.1 Se identifica los activos de información a analizar: El asesor de seguridad, debe apoyarse en la CMDB para la identificación de la muestra de los activos a analizar. Pueden ser equipos de cómputo, servidores, dispositivos móviles, URLs, aplicaciones, dispositivos (impresoras, routers, gateways, switch, acces point) entre otros, que se determine incluir en el plan de pruebas de vulnerabilidades para su respectivo análisis.

5.2.2 Se elabora / ajusta el plan de pruebas de vulnerabilidades: Se construye el plan de las pruebas de vulnerabilidades el cual debe contener como mínimo el objetivo, alcance, recursos a utilizar y cronograma.

5.2.3 Se debe socializar el plan a la Coordinación de infraestructura para su revisión.

Coordinador de infraestructura / Dirección de Tecnología

5.2.4 Se realiza la verificación al Plan de vulnerabilidad:
¿Requiere ajustes?

Si: Si requiere ajuste continúe en actividad 5.2.2 Elaborar/ajustar el plan de pruebas de vulnerabilidades
No: No requiere ajustes continúe en actividad 5.2.5 Iniciar la gestión para la ejecución de las pruebas

Asesor de Seguridad Informática / Dirección de Tecnología

5.2.5 Se coordina con los diferentes actores para dar inicio a la ejecución de las pruebas de acuerdo al cronograma.
Además, si se requiere el Asesor de Seguridad Informática configurará 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: Continúe a la actividad 5.2.8 Notificar resultados de las pruebas.
No: Continúe en las actividades 5.2.6 Reprogramar pruebas y 5.2.7. Documentar Novedades

5.2.6 Si durante la ejecución de las pruebas, estas no pudiesen ser realizadas satisfactoriamente, se debe cambiar la programación de horarios o ventana de tiempo y se debe volver a ejecutar esta actividad. La nueva propuesta de programación debe contar con la validación del coordinador de infraestructura.
Si las pruebas fueron realizadas satisfactoriamente el Asesor de Seguridad Informática continúa en el numeral 5.2.8.

5.2.7 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 del Comité de Vulnerabilidades.

5.2.8 Se Notifican 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 y con esto hacer seguimiento y evaluar los tiempos de respuesta para la mitigación de las vulnerabilidades. Además, se debe generar el consolidado de las vulnerabilidades por severidad (criticas, altas y medias) y estado (cerradas, en proceso y atrasadas)

Administrador de componentes informáticos / Dirección de Tecnología

5.2.9 Se analizan las vulnerabilidades encontradas con base en el informe entregado por el Asesor de Seguridad Informática, y determinar si es factible remediarlas o no.
¿Genera acciones de remediación?

Si. Pasa actividad 5.2.11
No. Pasa a 5.2.10

5.2.10. Se reporta los impedimentos por los cuales no se pueden aplicar las acciones de remediación, mediante correo electrónico o herramienta de gestión

5.2.11 Se aplica las acciones de remediación.

Asesor de Seguridad informática / Dirección de Tecnología

5.2.12 Se consolida la información generada por el (los) administrador(es) de elementos informáticos y se elabora el informe de resultados de las remediaciones a las vulnerabilidades reportadas.

5.2.13 Se debe presentar ante el comité de vulnerabilidades y debe quedar consignado en acta lo siguiente:

- Revisión de los compromisos del acta anterior.
- Revisión del resultado de los escaneos del periodo actual.
- Conclusiones y compromisos.
- Plan de escaneo del próximo periodo.

El acta debe realizarse en el formato de acta general de reuniones dispuesto en el sistema de gestión de calidad.

5.2.14. Se debe verificar la eliminación de vulnerabilidades encontradas anteriormente. Se realiza el Retest que consiste en ejecutar nuevamente las pruebas de vulnerabilidades en los activos analizados y que se establecieron en el plan de remediación, si no son remediadas, se dejan en seguimiento para su futura remediación y si son remediadas se deben incluir en el informe

5.2.15. Se debe validar las actividades efectuadas por el (los) administrador(es) de elementos informáticos, se deben verificar los resultados finales de las remediaciones y efectuar recomendaciones finales para futuros ejercicios.

5.2.16. Se debe revisar los resultados del escaneo del último periodo.

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Ejecución de las pruebas de vulnerabilidad	Revisión de las pruebas de vulnerabilidad	Registro en la Informe de escaneo de vulnerabilidades	Coordinador de Infraestructura

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Acta general de reuniones	F05
Procedimiento de Control de Cambios y despliegue 11	A7-1-11

Anexos:
A7-1-11 Pruebas de Vulnerabilidad.pdf
Editado por Elda Yolanda Castellanos Monroy, jul 09 2020 16:20 p.m.

Modificaciones

Descripción de cambios

- 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

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
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	-