1. OBJETO:

Definir las actividades para realizar las pruebas de penetración en entornos controlados a los sistemas y redes de datos de la Entidad, con el fin de descubrir, reparar amenazas y vulnerabilidades.

2. ALCANCE:

El presente documento aplica para los sistemas de información, redes de datos, bases de datos, aplicaciones que procesen, almacenen o trasmitan información de la Entidad.

El procedimiento contempla la periodicidad, roles, responsabilidades y metodología para la realización de las pruebas controladas de penetración, que sirven de insumo para la solución anticipada de posibles problemas de seguridad.

3. DEFINICIONES:

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización y por lo tanto debe proteger.

AD Active Directory – Directorio activo: son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO/IEC Guía 73:2002].

Backend: el back end del sitio o aplicación web consiste en un servidor, una aplicación y una base de datos. Se toman los datos, se procesa la información y se envía al usuario.

CVE: es una base de datos de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID.

Exploit: palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Frontend: consiste en la conversión de datos en una interfaz gráfica para que el usuario pueda ver e interactuar con la información de forma digital usando HTML, CSS, PHP y JavaScript.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]

IDS – Intrusion Detection System - sistema de detección de intrusiones: es un programa de detección de accesos no autorizados a un computador o a una red.

IPS – Intrusion Prevention System - sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones

LDAP - Lightweight Directory Access Protocol: El protocolo ligero de acceso a directorios hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

MITRE: Es una corporación no gubernamental fundada en 1958 cuya misión es intentar resolver problemas que contribuyan a un mundo más seguro, por lo que en esta oportunidad analizaremos su framework MITRE ATT&CK (por sus siglas en inglés, Tácticas, Técnicas y Conocimiento Común de Adversarios)

NIST – National Institute of Standards and Technology: El Instituto Nacional de Estándares y Tecnología, llamada entre 1901 y 1988 Oficina Nacional de Normas, es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

OWASP: Proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.

Penetration Testing (Pentesting) / PENTEST: Prueba de penetración, es un ataque controlado a un sistema informático con la intención de encontrar las debilidades o vulnerabilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002].

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

Tratamiento del Riesgo: Proceso de selección e implementación de medidas a para modificar el riesgo. [ISO/IEC Guía 73:2002].

4. NORMATIVA:

NUMERO	DESCRIPCIÓN
Ley 1581 del 18 octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1078 del 26 de mayo de 2015	(Artículo 2.2.9.1.1.1) – Por el cual se expide el decreto único reglamentario del sector de las tecnologías de la información de las comunicaciones.
Conpes 3995 del 1 de julio de 2020	Política Nacional de Confianza y Seguridad Digital.
Resolución 500 del 9 marzo de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución 1126 del 14 de mayo 2021	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

5. LINEAMIENTOS DE OPERACIÓN:

5.1 Para la elaboración del plan de auditoría, resuelva las siguientes preguntas:

- ¿Cuáles son los activos de información a evaluar?
- ¿Qué pruebas se van a realizar?
- ¿Objetivo que se busca alcanzar con estas pruebas?
- ¿En qué fechas de inicio y finalización de las pruebas?
- ¿En qué horarios se realizarán las pruebas?
- ¿Se realizarán pruebas de ingeniería social – phishing controlado?
- ¿Quiénes serán los encargados de efectuar las pruebas?
- ¿La Entidad contempla contratar los servicios de pentesting (pruebas de penetración) a compañías externas?

Adicional, tenga en cuenta los siguientes elementos:

- Definir los entregables: manual ejecutivo, técnico, recomendaciones e informe.
- Establecer comunicación con los encargados de los sistemas a evaluar.
- Recolección de evidencia de cada una de las fases.
- Identificar los sistemas de monitoreo o detección para evaluar su efectividad.
- Si la auditoría es realizada por una compañía externa se debe cumplir o exceder los requisitos establecidos en este documento.

5.2 Para realizar el reconocimiento de la información pueden utilizarse uno de los siguientes tres (3) métodos:

- Activo: Método de búsqueda mediante en el cual una aplicación contiene varias herramientas incluidas.
- Pasivo: Método manual que utiliza herramientas de manera individual o desarrolladas por el equipo auditor.
- Semi – pasivo: Combina las dos técnicas aumentando la efectividad.

5.3 Para el modelado de amenazas considere la siguiente información:

- Enfoque de la Entidad: Información de funcionarios / contratistas - Información de proveedores - Información de la infraestructura - Información financiera - Información del mercado - Políticas, procedimientos y planes - Información sobre infraestructura, bases de datos, arquitectura, configuraciones, cuentas de usuarios - Información sobre los procesos del negocio - Información sobre productos, investigaciones, publicaciones, desarrollos - Información sobre redes sociales.
- Enfoque del atacante: identificar los posibles grupos o agentes, que podrían llegar a lanzar ataques contra la Entidad, con el objetivo de realizar acciones focalizadas, a continuación, se listan los más relevantes:

Internos	Externos
Funcionarios / Contratistas	Ciber delincuentes
Mantenimiento	Proveedores
Administradores de sistemas.	Crimen organizado
Desarrolladores	Hacktivistas

Ingenieros	Crackers
Técnicos	Competencia
Soporte en sitio o remoto	Exfuncionarios / Excontratistas

5.4 Para realizar el análisis de vulnerabilidades:

a) Emplee una de las siguientes metodologías:
   - Análisis activo: Método automatizado o software que interactúa con el objetivo realizando varias pruebas simultáneamente, con poca intervención humana y entregando resultados en corto tiempo.
   - Análisis pasivo: Este método implica el análisis de datos haciendo uso de fuentes externas como aplicaciones online, archivos publicados en Internet que pueden contener información de valor como tipo de servidor, dominios, direccionamiento IP, también incluye el monitoreo de tráfico y recolección de metadatos.

b) Realice una investigación donde verifique las vulnerabilidades evidenciadas y contraste los hallazgos en diferentes fuentes de información para verificar su veracidad y las posibles vías para aprovecharse de las fallas identificadas. Tenga en cuenta las siguientes fuentes de información:
   - Bases de datos de vulnerabilidades CVE.
   - Top ten OWASP.
   - Publicaciones o alertas de los proveedores de las plataformas.
   - Bases de datos de exploits (exploit database, Rapid7, CXSecurity, mitre-attack, NIST,etc.)
   - Diccionarios de contraseñas.
   - Guías de hardering para plataformas.
   - Virtualización de infraestructura.

   Una vez realizada la investigación, se deben confirmar las vulnerabilidades encontradas consolidándolas en un archivo con su respectivo código CVE, su respectiva justificación, explicación y los tipos de ataque que podrían explotarse y sus posibles consecuencias.

5.5 Para la explotación de vulnerabilidades puede emplear una o mas de las siguientes técnicas:

- Exploits comunes: tomando como base el top 10 de OWAPS se pueden explotar las vulnerabilidades más recurrentes en la actualidad.
- - Evasión: utilizando diferentes técnicas se busca evadir los sistemas de seguridad (antivirus, firewall, IPS, IDS, controles criptográficos, etc.)
- - Ataques de precisión: ataques focalizados de acuerdo con la amenaza evidenciada y desarrollando o utilizando exploits dirigidos.
- - Ataques personalizados con base a tecnologías/medios de transmisión: exploits de acuerdo con los medios de transmisión y sus protocolos.
- - Exploits adaptados: técnica que toma exploits existentes y modifica su código de acuerdo con la plataforma o el objetivo.

- - Ataques día zero: si se encuentra una vulnerabilidad nueva, lograr la manera de explotarla.
- - Ataque de SSID (WIFI): técnicas para conseguir acceso a las redes de datos inalámbricas WIFI aprovechándose de las debilidades de los protocolos (WEB, WPA/2, EAP-FAST, etc.)
- - Ingeniería social: de acuerdo con la información recolectada en las fases anteriores, se puede realizar un perfil de los usuarios y lanzar correos phishing para intentar obtener información.
- - Ataque spoofing – Hombre en el medio: ataques como DNS, ARP o WIFI spoofing donde el atacante suplanta un recurso legitimo para interceptar o manipular el tráfico de las comunicaciones.
- - VLAN hopping: técnica que busca engañar a los dispositivos de red con el objetivo de ganar acceso a la red suplantando un dispositivo de confianza.
- - Análisis estático o dinámico de código fuente: mediante diferentes técnicas se realiza el análisis del código para encontrar fallas que puedan ser explotadas.

Teniendo en cuenta que el entorno digital es altamente dinámico, los encargados de realizar las auditorías deben actualizar las técnicas y herramientas de explotación de vulnerabilidades de acuerdo con las buenas prácticas.

5.6 Para la actividad de Post-Explotación no se deben realizar acciones que puedan dañar o desestabilizar los sistemas comprometidos, por esta razón se define el alcance máximo de acciones a ejecutar:

- Solo usar herramientas open source o las adquiridas por la Entidad.
- No se debe usar malware.
- Realizar escalamiento de privilegios.
- Acceso a información específica: repositorios, fileservers, NAS, SAN, FTP, SMB.
- Extracción de hashes o passwords.
- Acceso a logs.
- Ingreso a servidores.
- Acceso a AD – directorio activo o LDAP.
- Sistemas de backup
- Ingreso a entidades certificadoras.
- Identificación de hosts.

El auditor o responsable de la actividad debe extraer copia de la información que evidencie la consecución del objetivo, pero esta debe ser tratada como confidencial y en lo posible debe ser anonimizada, a esta información solo tendrá acceso el jefe de la OTIC, quién deberá verificar su destrucción al finalizar la auditoría.

5.7 Para la elaboración del reporte tenga en cuenta lo siguiente:

- Reporte ejecutivo: reporte dirigido a la dirección y por tratarse de una audiencia que puede no contar con los suficientes conocimientos técnicos, por esta razón es necesario que el lenguaje utilizado sea sencillo y fácil de comprender, este informe debe contener lo siguiente:
    - Introducción.

- Justificación.
- Objetivos alcanzados durante las pruebas.
- Calificación del riesgo.
- Causas de las vulnerabilidades: servidores o sistemas operativos desactualizados, carencia de hardering, servicios o puertos activos sin utilizar y desatendidos, configuraciones débiles o por defecto, firmware desactualizado.
- Plan de remediación: de acuerdo con el procedimiento y el mapa de riesgos se realiza la actualización de los riesgos y se elaboran los respectivos planes de manejo.

- Reporte técnico: este reporte puede incluir la información anterior y adicional se debe tener en cuenta que va dirigido a un público con conocimientos técnicos avanzados, dado que quienes reciben esta información son los que ejecutan las acciones de mejora para cada vulnerabilidad, por esta razón su contendido debe ser lo más específico y contener información detallada de las fases, imágenes, indicadores y otras herramientas que apoyen los resultados. Se debe considerar la siguiente información:
  - Información recolectada.
  - Vulnerabilidades encontradas con su respectivo CVE e información relacionada
  - Vulnerabilidades explotadas, activos comprometidos.
  - Acciones post-explotación aplicadas a los diferentes activos.
  - Plan de mejora.

6. DESCRIPCIÓN DE ACTIVIDADES:

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
1	**Elaborar el plan de auditorías pentest**. Elabora el plan de auditorías pentest, definiendo: contexto, alcance, cronograma, metodología, responsables y reportes.	Informe de análisis de vulnerabilidades – pentest vigencia anterior	Profesional especializado / Profesional universitario / Contratistas / Responsable de Seguridad de la Información Oficina TIC	Plan anual de auditorías pentest elaborado.
2	**Revisa y aprueba el plan de auditorías pentest** Revisa y aprueba del plan de auditorías pentest.		Jefe Oficina TIC.	Correo electrónico
	¿Se aprueba el plan anual de auditorías pentest? Si: Continúa con la actividad N 3.			

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	No: Solicita las correcciones y continúa con la actividad No 1.			
3	**Realizar el reconocimiento del objetivo** Realiza la recolección activa, pasiva o semi-pasiva de la mayor cantidad de información del objetivo, para ser utilizada en las siguientes fases. Nota: Si se contrata los servicios de pruebas de penetración (pentesting) con una empresa externa continúe con la actividad No.9		Profesional especializado / Profesional universitario / Contratista / Responsable de Seguridad de la Información Oficina TIC	Informe de análisis de vulnerabilidades - pentest inicial
4	**Realizar el modelado de amenazas** Define qué beneficios se pueden obtener si se logran los objetivos de penetrar el sistema y modificar, borrar, sustraer o destruir algún activo de información.		Profesional especializado / Profesional universitario / Contratista /Responsable de Seguridad de la Información Oficina TIC	Informe de análisis de vulnerabilidades – pentest vigente actualizado
5	**Realizar el análisis de vulnerabilidades** Identifica las fallas en los sistemas y aplicaciones que pueden ser aprovechadas.		Profesional especializado / Profesional universitario / Contratista /Responsable de Seguridad de la Información Oficina TIC	Informe de análisis de vulnerabilidades – pentest vigente actualizado
6	**Realizar la explotación** Obtiene acceso al sistema, de acuerdo con las vulnerabilidades identificadas en la fase anterior o sobrepasando los controles de seguridad existentes.		Profesional especializado / Profesional universitario / Contratista /Responsable de Seguridad de la Información Oficina TIC	Informe de análisis de vulnerabilidades – pentest vigente actualizado

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
7	**Realizar la Post – explotación** Identifica qué información se puede obtener y a que otros sistemas de información se puede acceder, identifica configuraciones, escalamiento de privilegios y demás actividades relacionadas con la fase.		Profesional especializado / Profesional universitario / Contratista /Responsable de Seguridad de la Información Oficina TIC	Informe de análisis de vulnerabilidades – pentest Final
8	**Realizar los reportes** Documenta todos los resultados obtenidos en cada una de las fases, teniendo en cuenta el tipo de audiencia se elabora un reporte gerencial y uno técnico. En estos reportes lista las recomendaciones de remediación por cada amenaza o vulnerabilidad evidenciada.		Profesional especializado / Profesional universitario / Contratista /Responsable de Seguridad de la Información Oficina TIC	Reporte gerencial y técnico
9	**Aprobar los reportes** Revisa y aprueba los reportes, informes y recomendaciones.	Visto bueno de los reportes, informe y recomendaciones	Jefe Oficina TIC	Correo de aprobación o corrección.
	¿Aprueba los reportes, informe y recomendaciones? **Si:** Operativiza el procedimiento DES-PC-07 Administración del riesgo y continúa con la actividad No 10. **No:** Solicita las correcciones y Continúa con la actividad No 8.			
10	**Comunicar las amenazas, vulnerabilidades y planes de manejo** Presenta al jefe de la oficina TIC y dueños de los controles, las amenazas y vulnerabilidades evidenciadas y los planes de	Política Institucional de la Administración del riesgo DES-PC-07 Administración	Profesional universitario / Contratista / Responsable de Seguridad de la Información Oficina TIC	Correo electrónico

No	ACTIVIDADES	PUNTO DE CONTROL	RESPONSABLE	REGISTRO
	manejo de riesgos para su ejecución y reporte.	del riesgo.		

7. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
01	20/09/2021	Se crea el procedimiento Análisis de Vulnerabilidades – pentest, basado en la Guía No. 1 del MinTic
02	18/11/2021	Se contempla, dentro de los lineamientos de operación y la actividad No. 3, la contratación de empresas externas para la realización de las pruebas de penetración.

8. AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Osbaldo Cortes Lozano	Profesional Universitario Oficina TIC	
	Rubén Buitrago Daza	Contratista – Oficina TIC	
	Juan Sebastián Perdomo	Profesional Universitario Oficina TIC	
	Gisela Arias Salazar	Contratista – Oficina TIC	
	Oscar Ricardo Rodríguez	Contratista – Oficina TIC	
	Fabian Andrés Lozano	Contratista – Oficina TIC	
	Sayra Paola Nova	Profesional Universitario Oficina TIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina de Tecnologías de Información y las Comunicaciones	César Mauricio Beltrán López Firmado digitalmente por César Mauricio Beltrán López Fecha: 2021.11.10 22:58:15 -05'00'
	Luz Mary Palacios Castillo	Profesional Universitario – Oficina Asesora de Planeación	
	German Guillermo Sandoval Pinzón	Contratista Oficina Asesora de Planeación	
Aprobó	Francisco José Ayala Sanmiguel	Jefe Oficina Asesora de Planeación	