Personería Distrital de Medellín

ESPECIFICACIONES TÉCNICAS
PROCESO DE SELECCIÓN SUBI_2025_03

ITEM	BIEN Y/O SERVICIO	CANTIDAD	ESPECIFICACIONES TÉCNICAS DETALLADAS DEL BIEN Y/O SERVICIO
1	**Renovación de EDR protección avanzada de endpoints**	**300**	**Protección de ENDPOINTS** - FC2-10-FEDR1-349-01-DD para administración de EDR completa. EDR identifica y detiene las brechas en tiempo real de forma automática y eficiente con un agente ligero. Como parte de la plataforma de operaciones de seguridad de Fortinet, reduce de manera proactiva la superficie de ataque, evita la infección de malware, detecta y desactiva amenazas potenciales de inmediato y automatiza los procedimientos de respuesta y corrección con libros de jugadas personalizables en sistemas operativos heredados y actuales Protección avanzada de endpoints de EDR. Reduzca la superficie de ataque y aproveche las políticas listas para usar que están estrechamente asignadas al marco MITRE ATT&CK para que los equipos de seguridad puedan responder a una multitud de tácticas, técnicas y procedimientos avanzados que se encuentran en ataques como el ransomware. **Protección contra brechas en tiempo real:** Durante un incidente de seguridad, EDR puede evitar la exfiltración de datos y protegerse contra el ransomware. También revertirá los cambios maliciosos. **Reducción de la superficie de ataque:** EDR puede descubrir y controlar dispositivos fraudulentos, dispositivos IoT y aplicaciones, además de sus respectivas vulnerabilidades en tiempo real. **Protección OT:** EDR garantiza una alta disponibilidad para los sistemas OT incluso durante un incidente o violación de seguridad. **Seguridad de Sistemas POS.** EDR evita la exfiltración de datos en caso de que el sistema se vea comprometido. Ofrece parches virtuales para proteger los sistemas POS de vulnerabilidades. **Conectividad de Estructura:** EDR se integra con Fortinet Security Fabric para compartir inteligencia y respuesta a incidentes de identidad, firewalls, correo electrónico y más. **Unidades:**

			Se requieren renovar 300 licencias que puedan ser utilizadas tanto en estaciones de trabajo: EDR es compatible con los sistemas operativos Windows, MacOS y Linux, y ofrece protección fuera de línea, Vigencia de la licencia: por el Fabricante 1 año. Servicios: El p **Documentación** El proponente deberá entregar ficha técnica de las licencias, certificado de distribuidor autorizado emitido por fabricante y deberá contar con al menos un ingeniero de sistemas y/o ingeniero en telecomunicaciones con mínimo 10 años de experiencia con la idoneidad adecuada para desarrollar el objeto contractual, con certificación vigente de **Fortigate Certified Profesional Network Security.**
2	**Renovación de, licenciamiento por 12 meses Forticare Premuin y Fortiguard Unified Protection (UTP) para equipo Fortigate 200F existente**	**1**	**FortiGate-200F** **Serial : FV400DTA18000173** **Funciones de Seguridad:** Firewall, IPS, antivirus, antispam, filtrado web, VPN El proponente debe incluir Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) por 12 meses, **SKU FG-200F-BDL-950-12** **Soporte.** Se deberá comunicar al personal de sistemas (Administrador del Sistema) de la Personería de Medellín con un(os) profesional(es) de soporte técnico con máximo dos (2) horas de respuesta después de reportado un incidente, en concordancia con el nivel de prioridad de la solicitud. El proponente deberá atender ilimitadamente las solicitudes de soporte de la entidad. En modalidad remota y con atención presencial 7x24. Para garantizar el optimó funcionamiento de las soluciones implementadas y/o soportadas, los profesionales de soporte deberán poseer un alto nivel de conocimiento y experiencia, certificada. **Alcance** El proponente deberá suministrar soporte técnico en modalidad hibrida 8 días x 5 horas, atendido por ingeniero especialista del producto con certificación mínimo **Fortigate Certified Profesional Network Security, FCP**, durante 1 año. Las actividades presenciales se brindarán en la ciudad de Medellín. Atención telefónica, correo electrónico. **Pruebas de Vulnerabilidades** Incluye la realización de pruebas controladas de seguridad sobre la infraestructura perimetral y aplicaciones web institucionales, **enfocadas en:** • Evaluación de configuración y políticas de seguridad en FortiGate y FortiWeb. • Análisis de vulnerabilidades en el portal web institucional y sistemas asociados (como SIP). • Identificación de brechas en OWASP Top 10 y servicios expuestos (SSL, DNS, HTTP, etc.). • Informe técnico con hallazgos, nivel de riesgo (CVSS) y recomendaciones de mitigación. **Entregables:** • Informe técnico de vulnerabilidades. • Informe ejecutivo para toma de decisiones.

			• Validación post-corrección (una ronda de verificación). Duración del análisis: Máximo 10 días calendario. **Documentación:** Certificación expedida directamente por el fabricante FORTINET en la cual se indique que el proponente es representante o distribuidor autorizado. Contar con al menos 2 personas certificadas en **Fortigate Certified Profesional Network Security vigente expedido por el fabricante al momento de presentar su oferta**
3	**Renovación de licenciamiento Fortiweb Maquina Virtual: Subscription license with Bundle for FortiWeb-VM (2 CPU) 1 Year Subscription license for FortiWeb-VM (2 CPU) with Standard bundle included**	**1licencia anual**	**Fortiweb Maquina Virtual: Subscription license with Bundle for FortiWeb-VM (2 CPU) 1 año SERIAL: FWBVMSTM24001077** FortiWeb adopta un enfoque integral de la seguridad de las aplicaciones web: La reputación IP, la protección DDoS, la validación de protocolos, las firmas de ataques a aplicaciones, la defensa contra bots y muchas más funciones protegen sus aplicaciones de una amplia gama de amenazas, incluidas las 10 principales de OWASP. **Caracteristicas principales:** Rendimiento HTTP: 100 Mbps Licencias de aplicación. Ilimitado Dominios administrativos: de 4 a 64 en función de cantidad de memoria Hipervisores compatibles: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) y Microsoft Azure. **Compatibilidad con la interfaz de red (mínimo / máximo):** 1 / 4 (10 VMware ESX) **Soporte de almacenamiento (mínimo / máximo):** 40 GB / 2 TB **Documentación** Certificación expedida directamente por el fabricante FORTINET en la cual se indique que el proponente es representante o distribuidor autorizado. Contar con al menos 2 personas certificada en **NSE4, Fortigate Certified Profesional Network Security vigente expedido por el fabricante**
4	**Renovar Licenciamiento de Veritas - 19788-M0016 BACKUP EXEC SILVER WIN 1 FRONT END TB ONPREMISE STANDARD SUBSCRIPTIO N + ESSENTIAL MAINTENANCE LICENSE INITIAL 12MO GOV**	1 licencia Anual	**Licencia VERITAS Backup Exec Silver 1 año** • Administración central del servidor de respaldo • Instalar y proteger servidores de archivos físicos, virtuales y en la nube. • Protección y recuperación de aplicaciones y bases de datos. • Protección de Windows y Linux • Protección de almacenamiento compartido NDMP y SAN • Des duplicación de datos en todos sus datos, incluso en la nube • Bibliotecas de cintas físicas y virtuales ilimitadas. • Agente para VMware & Hyper-V • Hasta 4 drives/librerías físicas o virtuales • Eliminación de duplicados e información redundante • Agente en Windows • Backup físico y virtual en servidores Windows y Linux • Copia de seguridad en cinta, disco o nube • Soporte técnico 24x7 • Capacitad de 3 Tb

5	**Adquirir Positive SSL Wildcard para asegurar el dominio personeriamedellin.gov.co**	**1 Dominio**	Adquirir, suministrar, Instalar y configurar el servicio de certificado SSL que permita validar 1 dominio (personeriamedellin.gov.co) y permita subdominios ilimitados; sin que la Entidad deba estipular en la operación secundaria el número exacto de subdominios para los que desea la licencia. El contratista debe garantizar que el servicio soporta: - Cifrado SHA2 y ECC de 128/256 bits. - Contar con sello de seguridad. - Que el servicio soporta compatibilidad con cualquier navegador y navegadores móviles. - Que el servicio soporte la instalación en ambientes Windows y Linux. - La licencia permite colocar el certificado en un solo dominio con número ilimitado de subdominios. La vigencia del certificado digital SSL es de 1 año, desde el momento de su instalación.
6	**Renovar licenciamiento de Adobe Illustrator CC para mac**	1 licencia Anual	Renovación Licencia de Adobe Illustrator CC por un año para Mac: VIP Gobierno Illustrator CC for teams ALL Licencia Nueva CCT Multiple Platforms Multi Latin American Languages 12 Meses 1 Usuario Nivel 1 1 – 9. **Documentación**: Teniendo en cuenta que adobe sólo distribuye su licenciamiento por partner y socios autorizados por ellos el oferente deberá acreditar ser partner autorizado de adobe.
7	**Renovar licenciamiento de Acrobat Pro DC**	1 licencia Anual	Acrobat Pro incluye todo lo de Acrobat Standard, además de funciones avanzadas de PDF y de firma electrónica, como: • Convertir documentos escaneados en archivos PDF editables en los que se pueden realizar búsquedas • Comparar archivos PDF para revisar fácilmente las diferencias • Censurar información confidencial de un PDF • Insertar un logotipo y dirección de URL personalizada de tu marca en los acuerdos • Crear formularios web y plantillas de firma electrónica reutilizables • Cobrar pagos con Braintree (cuando esté disponible) • Recibir y rastrear varias firmas electrónicas con el envío masivo. **Documentación**: Teniendo en cuenta que adobe sólo distribuye su licenciamiento por partner y socios autorizados por ellos el oferente deberá acreditar ser partner autorizado de adobe.
8	**Adquirir licenciamiento de Adobe Premiere Pro**	1 licencia anual	Para edición y corte de videos, añade efectos, mezcla audio, y anima títulos. Añade fotogramas. Potencia tu flujo de trabajo con IA. Se necesita licenciamiento por 12 meses del paquete Adobe Premiere Pro que incluye: • Premiere Pro para computadora. • Adobe Express y Adobe Firefly. • Tutoriales, fuentes, plantillas y más.

			• 100GB de espacio en la nube. 500 créditos generativos al mes
9	**Renovar licenciamiento de Adobe Photoshop Oficial Software de fotografía y diseño**	1 licencia Anual	Renovación Licencia de Adobe Photoshop Oficial | Software de fotografía y diseño por un año para Mac Para la edición de imágenes y de diseño gráfico. Crea y mejora fotografías, ilustraciones e imágenes en 3D. Edita vídeos, simula cuadros reales.
10	**Renovar licenciamiento de TeamViewer Para equipos a la última versión que permita la realización de tres (3) sesiones simultaneas soporte remoto anual**	3 licencia Anual	**Características principales que debe cubrir:** • Debe permitir Asistir a los empleados que trabajan desde casa, al personal que se encuentra en corregimientos y casas de justicia. • Debe permitir reducir el riesgo de los daños que puedan sufrir las computadoras portátiles y de escritorio cuando se envían a reparación. • Mejorar las tasas de resolución en la primera llamada • Debe permitir Asistencia personalizada. • Debe permitir el desarrollo de marca personalizado para las aplicaciones de asistencia. • Gestión integrada de casos de servicio e integración en los principales sistemas de atención. • Posibilidad de dejar notas en el escritorio de computadoras remotas. • Integración en Mobile Device Management (gestión de dispositivos móviles) y otras aplicaciones
11	**Renovar servicios de servidores en nube Azure (Todo el Año) e integracion AD fisico y renovacion de licencias de server (Ver cuadro item 11)**	1	Se deberán renovar los siguientes servidores y servicios • Servidor de Personería en línea • Servidor de Pagina web • Servidor de SIP • Servidor de BD • Servidor de Centro pensamiento • Servidor de App de apoyo • Servidor de Intranet • Red Virtual • Direccionamiento IP Publico Estático Nota: ver cuadro servicios y servidores en la nube Azure

Personería
Distrital de Medellín

CLIENTE	DESCRIPCION	SERVICIO ANUAL	CANT.	OBSERVACION
personeriamedellin.gov.co	Backup - Azure VM - US East 2		7	
personeriamedellin.gov.co	Bandwidth Inter-Region - Inter Continent - Intercontinental		7	
personeriamedellin.gov.co	Bandwidth Inter-Region - Intra Continent - North America		7	
personeriamedellin.gov.co	IP Addresses - Standard IPv4		7	
personeriamedellin.gov.co	Rtn Preference: MGN		7	
personeriamedellin.gov.co	Standard HDD Managed Disks - S4 LRS		7	
personeriamedellin.gov.co	Standard HDD Managed Disks - Snapshots ZRS - US East 2		7	
personeriamedellin.gov.co	Standard SSD Managed Disks - E15 LRS - US East 2		7	
personeriamedellin.gov.co	Standard SSD Managed Disks - E30 LRS - US East 2		7	
personeriamedellin.gov.co	Standard SSD Managed Disks - E4 LRS		7	
personeriamedellin.gov.co	Standard SSD Managed Disks - E6 LRS - US East 2		7	
personeriamedellin.gov.co	Virtual Machines BS Series - B2ms - US East 2		5	
personeriamedellin.gov.co	Virtual Machines BS Series - B4ms - US East 2		2	

ITEM 11 – SERVIDORES Y SERVICIOS A RENOVAR				
REQUERIMIENTO	**DESCRIPCION**	**UNIDAD**	**CANT.**	**OBSERVACION**
Servidor de Personería en línea	Servidor en nube con mínimo 8 Gb de RAM, 2 procesador VCPU, y almacenamiento de 50GB, Sistema operativo Linux	Global	1	Componentes para uso de una página web
Servidor de Pagina web	Servidor en nube con mínimo 8 Gb de RAM, 2 procesador VCPU, y almacenamiento de 50GB, Sistema operativo Linux	Global	1	Componentes para uso de una página web
Servidor de SIP	Servidor en nube con mínimo 14 Gb de RAM, 4 procesador VCPU, y almacenamiento de 200GB, Sistema operativo Linux	Global	1	Componentes para uso de una página web
Servidor de BD	Servidor en nube con mínimo 14 Gb de RAM, 4 procesador VCPU, y almacenamiento de 4TB, Sistema operativo Linux	Global	1	Base de datos postgresSQL
Servidor de Centro pensamiento	Servidor en nube con mínimo 8 Gb de RAM, 2 procesador VCPU, y almacenamiento de 50GB, Sistema operativo Linux	Global	1	Herramienta Moodle
Servidor de App de apoyo	Servidor en nube con mínimo 8 Gb de RAM, 2 procesador VCPU, y almacenamiento de 50GB, Sistema operativo Linux	Global	1	Componentes para uso de una página web
Servidor de Intranet	Servidor en nube con mínimo 8 Gb de RAM, 2 procesador VCPU, y almacenamiento de 50GB, Sistema operativo Linux	Global	1	Componentes para uso de una página web de Intranet
Red Virtual	Interconectividad de los servidores y servicios	Global	1	
Direccionamiento IP Publico Estático	Interconectividad de los servidores y servicios publicados en Internet	Global	1	

ESPECIFICACIONES TECNICAS PARA LAS PRUEBAS DE PENTESTING, ANÁLISIS DE VULNERABILIDADES, PRUEBAS DE PENETRACIÓN EXPLOIT Y ETHICAL HACKING.

Se busca realizar mediante servicio técnico especializado y de Ingeniería pruebas de pentesting, análisis de vulnerabilidades, pruebas de penetración Exploit e Ingeniería social bajo el alcance de Ethical Hacking, para identificar y detectar vulnerabilidades existentes en la Infraestructura Tecnológica de los siguientes sistemas de hardware y Software de la Personería Distrital de Medellín:

- Software administrativo y operativo (SIP)

COMPONENTE 1: Objetivo: Realizar una auditoría técnica en modalidad pentesting caja negra, a la Infraestructura que cubra las pruebas durante un tiempo de 1 semana y permita la identificación de riesgos y vulnerabilidades a las que la organización se encuentra expuesta, de manera que sea posible planificar controles de seguridad para reducir los riesgos informáticos.

COMPONENTE 2: Objetivo: Evaluar el comportamiento, la estabilidad y la capacidad de respuesta del sistema cuando se enfrenta a distintos niveles de demanda, desde escenarios de uso normal hasta condiciones extremas. A través de la simulación de múltiples usuarios concurrentes accediendo a la URL, se busca identificar el rendimiento del sistema bajo carga progresiva, detectar cuellos de botella, establecer el punto de quiebre y verificar la capacidad de recuperación ante fallos.

COMPONENTE 3. Objetivo: Se requiere identificar las vulnerabilidades existentes en la infraestructura tecnológica que administra y soporta la Personería Distrital de Medellín, a los activos de redes de datos, procesamiento, almacenamiento, comunicaciones, equipos de seguridad electrónica, equipos de networking y redes inalámbricas que cubren y conforman la operación de tal forma de establecer la ruta a seguir con

las respectivas recomendaciones a las vulnerabilidades encontradas para su tratamiento o mitigación de acuerdo a su grado de criticidad.

CONTEXTO TECNICO

En el contexto de sus operaciones, la entidad ha venido implementando y evolucionando sus propias tecnologías de información a través de distintos tipos de aplicaciones, software y dispositivos de infraestructura tecnológica.

Esta descripción técnica pretende auditar potenciales vulnerabilidades de seguridad informática que pudieran poner en riesgo la continuidad de la operación de la organización, a través de un conjunto de pruebas de auditoría de seguridad informática, vulnerabilidades de la red de datos que puedan conducir a la implementación de controles para reducir los riesgos sobre la integridad, disponibilidad y confidencialidad de la información de la plataforma.

Adicionalmente, se pretende que las pruebas de carga y estrés permitan anticipar problemas de escalabilidad y asegurar que la infraestructura pueda sostener la operación sin degradar la experiencia del usuario, incluso en situaciones de alta exigencia.

METODOLOGIAS DE TRABAJO A IMPLEMENTAR

Para la ejecución de este alcance que se presenta a continuación, se deberá tener en cuenta las buenas prácticas establecidas en marcos de referencia internacionales como:

- ✓ CEH, ISO 27001, OSSTMM3 y OWASP
- ✓ GIAC Penetration Tester (GPEN)
- ✓ GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
- ✓ GIAC Web Application Penetration Tester (GWAPT)

- ✓ OSWP (Offensive Security wireless Professional)
- ✓ Certified Penetration Testing Engineer CPTE
- ✓ CompTIA Pentest+

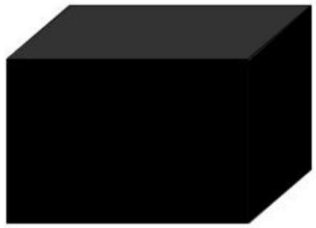
A continuación, presentamos un breve resumen de las normas, estándares y frameworks que se deberán tener en cuenta y de referencia para el logro del propósito.

C|EH™ Certified Ethical Hacker	CEH	CEH (Certified Ethical Hacker) del EC- Council relacionado con las pruebas de penetración, hacking ético y análisis de vulnerabilidades en sistemas y plataformas tecnológicas.
ISO 27001	Estándar ISO 27001	ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma 27002.
OSSTMM 3 The Open Source Security Testing Methodology Manual Contemporary Security Testing and Analysis	OSSTMM3	El Open Source Security Testing Methodology Manual, ofrece un marco para realizar pruebas de seguridad y obtener resultados verificables y evidencias sólidas que puedan ser utilizadas a la hora de tomar decisiones de seguridad

OWASP Open Web Application Security Project	OWASP	"OWASP Testing Guide" que establece un marco de referencia para la ejecución de pruebas de seguridad sobre aplicaciones web y así detectar posibles fallos.
GIAC PENETRATION GPEN TESTER	GIAC	GIAC Penetration Tester valida la capacidad de un profesional para realizar correctamente una prueba de penetración, utilizando las mejores técnicas y metodologías.
GIAC WEB APPLICATION GWAPT PENETRATION TESTER	GWAPT	GIAC Web Application Penetration Tester (GWAPT) valida la capacidad de un profesional para proteger mejor a las organizaciones a través de pruebas de penetración y un conocimiento profundo de la web Problemas de seguridad de las aplicaciones
C)PTE CERTIFIED PENETRATION TESTING ENGINEER	CPTE	El profesional certificado debe tener conocimiento en 5 elementos clave del Penetration testing (Pruebas de Penetración): recopilación de información, escaneo, enumeración, explotación y reporteo

AUDITORIA TECNICA

COMPONENTE 1: ESCENARIO PENTESTING CAJA NEGRA SIN AUTENTICACIÓN



El escenario de caja negra “Black Box” contempla la ejecución de una serie de pruebas de seguridad informática desde la posición de un atacante potencial con un bajo o nulo conocimiento de las características de los targets (aplicaciones y/o servidores) a analizar. Es lo más parecido a un ataque puro.

A través de esta técnica se realizan pruebas de penetración sin tomar en cuenta la estructura interna de código, detalles de implementación de las plataformas ni escenarios de ejecución internos con usuarios autenticados en el software; ya que el atacante solo contará con información pública propia de las plataformas y con la visibilidad de lo que hay explícitamente expuesto hacia Internet sin autenticación.

RECONOCIMIENTO PASIVO - FOOTPRINTING

A través de técnicas de recopilación de información y footprinting, se buscará identificar los datos sensibles pueda estar expuestos en Internet cubriendo el siguiente:

- Identificación de fugas de información originadas en el dominio o direcciones IP de la compañía.
- Análisis de metadatos de archivos presentes en la plataforma web principal de la compañía.
- Cosecha de correos electrónicos: Identificar los correos electrónicos expuestos en Internet y que pudieran ser susceptibles a Ingeniería social o Phishing
- Análisis de configuración de seguridad del dominio que permite identificar el estado de seguridad de los registros DNS recomendados para mitigar riesgos informáticos.

RECONOCIMIENTO ACTIVO – FINGERPRINTING

Con el propósito de cubrir integralmente la verificación de la seguridad a nivel de la capa de transporte, se auditarán los 65.536 puertos tanto TCP como UDP por cada servidor del alcance.

Escaneo de puertos TCP y UDP

- Identificación de estado de puertos TCP y UDP con los siguientes tipos de escaneo
  - TCP Connect, TCP SYN, TCP ACK
  - UDP
  - TCP FIN, TCP XMAS, TCP NULL
- Identificación de nombres y versiones de servicios, sistemas operativos y otros datos potencialmente relevantes sobre los servidores.
- Enumeración de servicios ANÁLISIS DE VULNERABILIDADES

ANÁLISIS DE VULNERABILIDADES

En esta fase de la auditoría se realiza un escaneo de vulnerabilidades a través de herramientas que identifican CVEs conocidas de acuerdo con MITRE y también vulnerabilidades de OWASP sobre los servidores contemplados en el alcance y en búsqueda de los siguientes tipos de vulnerabilidades:

- Vulnerabilidades de software CVE en servicios
- Vulnerabilidades de configuración
- Vulnerabilidades inducidas (Posibles backdoors/rootkits)
- Contraseñas débiles
- Errores en manejo de certificados
- Configuraciones por defecto

Las vulnerabilidades serán reportadas por CVE y clasificadas según el estándar CVSS para identificar el impacto sobre la confidencialidad, la integridad y la disponibilidad en las categorías Críticas, Altas, Medias y Bajas.

Además, se identificarán las recomendaciones para tratar cada una de las vulnerabilidades en función de las prioridades por tipo de activo.

EXPLOTACIÓN DE VULNERABILIDADES

Durante esta fase y bajo el consentimiento del cliente se utilizarán herramientas de explotación (Metasploit o scripts en ruby o en python) que permitan tomar provecho de las vulnerabilidades identificadas y donde corresponda durante el desarrollo del componente 3 de esta propuesta.

Considerando que el alcance de la fase explotación representa incertidumbre ya que su dimensión dependerá de la cantidad de vulnerabilidades a cubrir; se propone la explotación de las vulnerabilidades

altas y medias que surjan durante el proceso de análisis de vulnerabilidades en cualquiera de los activos cubiertos en el alcance. Para este alcance se plantea realizar las pruebas necesarias que permitan explotar hasta un total de 8 vulnerabilidades altas y medias seleccionadas por target o en su defecto invertir hasta 2 jornadas completas (días hábiles) por target en el ejercicio de explotación.

PRUEBAS DE FUERZA BRUTA

Se identificarán interfaces de login en los target contempladas en el alcance y sobre ellas se realizarán pruebas de fuerza bruta en búsqueda de identificar lo siguiente:

- Credenciales de usuarios críticos
- Nombres de usuario
- Contraseñas
- Sistemas de Login Vulnerables

PRUEBAS DE FUZZING

A través de técnicas de fuzzing web se buscará identificar variables vulnerables a inyecciones en las aplicaciones web contempladas en el alcance, esto contempla lo siguiente

- Identificación de bugs de implementación
- Inyección de datos malformados/semi-malformados de manera automatizada.
- Uso de vectores peligrosos de fuzzing conocidos (cadenas maliciosas)

PRUEBAS DE VULNERABILIDADES WEB

Por medio de herramientas y comandos disponibles en la herramientas de auditoría, se realizará la identificación de los siguientes tipos de vulnerabilidades:

- SQL Injection
- XSS Reflected, XSS Stored
- CSRF
- File Inclusion (LFI, RFI)
- Command Injection
- Fuerza bruta

Nota: En las API que lleguen a identificarse, se buscará aplicar estas técnicas para identificar la superficie de ataque

PRUEBAS DE VULNERABILIDADES CMS/LMS

En el caso de que se identifiquen CMS/LMS populares en el mercado, se realizarán pruebas específicas sobre potenciales vulnerabilidades para las aplicaciones que están basadas en esta tecnología buscando identificar:

- Fuerza bruta sobre CMS/LMS
- Validación de potenciales plugins o temas vulnerables
- Reconocimiento de usuarios
- Identificación de vulnerabilidades en directorios

Personería
Distrital de Medellín

AUDITORÍA A POSTERIORI

El alcance incluye la ejecución de una auditoría a posteriori (Re-test) luego de que la organización haya aplicado los controles según los hallazgos identificados y reportados por la auditoría.

La auditoría a posteriori consiste en realizar (segundo ciclo) a la verificación posterior al proceso de tratamiento de los riesgos realizado por la organización, que permita validar del cierre eficaz de las brechas, vulnerabilidades y riesgos de seguridad identificados durante todo el proceso de auditoría.

En esta auditoría se cubre la verificación de los siguientes temas:

- Footprinting & Fingerprinting
- Escaneo de puertos
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades
- Superficie de ataque sobre APIs identificadas durante el ejercicio caja negra
- Retest de las vulnerabilidades reportadas

Nota: Las pruebas de API no corresponden a una prueba profunda específica de cada API, ya que cada una podría corresponder a un nuevo target en sí mismo y en la etapa del primer ejercicio caja negra no es posible determinar el esfuerzo requerido para cubrir todos los endpoints.

Adicionalmente a lo anterior, se cubrirán las siguientes pruebas de auditoría de seguridad informática:

- Verificar que el sitio utiliza métodos válidos para realizar la autenticación de los usuarios.
- Verificar el correcto cierre de sesión de los usuarios que utilizan el sitio.
- Análisis de los campos en busca de posibles puntos de inyección.
- Pruebas de fuzzing sobre los campos de autenticación.
- Verificar la aplicación de políticas de bloqueo de acceso por superar un tope máximo de intentos fallidos de login.
- Identificar la existencia de métodos de autenticación de doble factor.
- Verificar controles del lado del cliente y del lado del servidor.
- Verificación de controles contra enumeración de usuarios
- Analizar la presentación de la información correcta para cada uno de los usuarios de la aplicación.
- Comprobar el uso de mecanismos de cifrados seguros para el transporte de información sensible.
- Verificar el uso de llaves para el cifrado en tránsito
- Analizar la presentación de la información correcta para cada uno de los usuarios de la aplicación.
- Comprobar el uso de mecanismos de cifrados seguros para el transporte de información sensible
- Verificar el uso de llaves para el cifrado en tránsito

Adicionalmente y como un valor agregado, se realizarán las siguientes actividades de auditoría incluidas en el alcance:

Pruebas sin autenticación

- Pruebas de fuerza bruta
- Pruebas de inyección de cadenas malformadas XSS y SQL
- Pruebas de command injection

- Escaneo de vulnerabilidades

Nota: En este alcance se contempla el análisis de hasta 100 campos por cada target

COMPONENTE 2: PRUEBAS DE CARGA Y ESTRÉS

El alcance de las pruebas de estrés abarca la evaluación integral del comportamiento del sistema que responde ante solicitudes dirigidas a una URL específica, bajo diferentes niveles de carga, hasta alcanzar condiciones límite.

Las actividades que se llevarán a cabo incluyen:

1.Pruebas de carga progresiva

Se simulará un aumento gradual en la cantidad de usuarios concurrentes accediendo a la URL, con el objetivo de medir cómo se comporta el sistema a medida que la demanda crece. Se monitorearán métricas clave como el tiempo de respuesta, el uso de CPU y memoria, y la tasa de errores.

2.Pruebas de estrés extremo

Se someterá al sistema a una carga significativamente superior a la esperada en condiciones normales de operación, con el fin de identificar el punto de quiebre o saturación. Estas pruebas permitirán observar cómo responde la infraestructura ante escenarios de sobrecarga: si se degrada gradualmente, se detiene abruptamente o logra recuperarse

3.Pruebas de resistencia prolongada

Se mantendrá una carga moderada/alta sobre la URL durante un periodo extendido (por ejemplo, varias horas continuas), para observar el impacto sostenido en los recursos del sistema y detectar posibles fugas de memoria, degradación del rendimiento o pérdida de disponibilidad.

4.Simulación de picos repentinos

Se generarán ráfagas de tráfico que simulan eventos como promociones, campañas publicitarias o picos de uso inesperados. Esto ayudará a evaluar si el sistema puede absorber variaciones abruptas en la demanda sin comprometer su funcionalidad.

5.Validación de funcionalidades críticas

Las pruebas también verificarán que funciones clave asociadas a la URL (como autenticación, navegación, envío de formularios o procesamiento de pagos) sigan operando correctamente bajo carga.

6.Monitoreo de recursos e infraestructura

Durante todas las pruebas, se llevará a cabo una supervisión detallada del rendimiento del servidor, uso de la red, utilización de bases de datos, y respuestas.

Tipos de pruebas de estrés Las pruebas de estrés se enfocarán en evaluar el comportamiento y la estabilidad del sistema al exponer la URL objetivo a condiciones de carga extrema.

- Pruebas de carga: Simulación progresiva de usuarios concurrentes accediendo a la URL para medir el rendimiento general.
- Pruebas de estrés: Evaluación del punto de quiebre al forzar el sistema con volúmenes de tráfico superiores a lo esperado.
- Pruebas de resistencia: Análisis del comportamiento bajo una carga sostenida durante un periodo prolongado.
- Pruebas de picos: Simulación de incrementos abruptos de tráfico para medir la capacidad de respuesta ante escenarios inesperados.

Estas pruebas permitirán detectar cuellos de botella, evaluar la recuperación ante fallos y establecer umbrales seguros de operación bajo diferentes condiciones de uso.

COMPONENTE 3: ANALISIS DE VULNERABILIDADES A LA INFRAESTRUCTURA DE RED

Los análisis de vulnerabilidades de red se centran en identificar vulnerabilidades en la infraestructura de red de una organización. Comprueban si hay puertos abiertos, configuraciones incorrectas y posibles puntos de entrada a los que los atacantes podrían dirigirse. El análisis de red diagnostica esencialmente la postura de seguridad de los dispositivos de red, como enrutadores, conmutadores y firewalls

Una vulnerabilidad de seguridad es cualquier debilidad en la estructura, función o implementación de un activo o red de TI. Los hackers u otros actores de amenazas pueden explotar esta debilidad para obtener acceso no autorizado y causar daño a la red, a los usuarios o al negocio. Las vulnerabilidades comunes incluyen:

- Errores de codificación, como aplicaciones web que son susceptibles al scripting entre sitios, inyección SQL y otros ataques de inyección debido a la forma en que manejan las entradas de los usuarios.
- Puertos abiertos no protegidos en servidores, computadoras portátiles y otros endpoints, que los piratas informáticos podrían utilizar para difundir malware.
- Configuraciones incorrectas, como un depósito de almacenamiento en la nube que expone datos confidenciales a la red pública de Internet porque tiene permisos de acceso inadecuados.
- Faltan parches, contraseñas débiles u otras deficiencias en la higiene de la seguridad cibernética**.**

1. Las Etapas de evaluación de las vulnerabilidades.

Los diferentes tipos de evaluaciones de vulnerabilidad utilizan herramientas individuales para identificar los puntos débiles del sistema y de la red. Los sistemas independientes pueden necesitar varios tipos de evaluaciones para identificar todas sus posibles vulnerabilidades.

Existen 4 etapas principales para la evaliuacion de las vulnarabilidades estan son:

1.1 Identificación de activos y vulnerabilidades

La identificación es la primera etapa cuando se realiza una evaluación de la vulnerabilidad: antes de comenzar un escáner, se identifican los activos escaneables, incluyendo herramientas populares, como dispositivos móviles, dispositivos del Internet de las Cosas y programas basados en la nube. A continuación, la infraestructura es escaneada por herramientas automatizadas o manualmente por analistas de seguridad. Se elabora un informe de evaluación de vulnerabilidad que describe los puntos débiles identificados.

1.2 Análisis

En la etapa de análisis de una evaluación de vulnerabilidad, el objetivo es encontrar el origen y la causa de cada debilidad. Para identificar la causa raíz, los componentes de la infraestructura que son responsables de cada vulnerabilidad deben ser verificados y analizados más a fondo. En la etapa de análisis también se comprueba si hay sistemas mal instalados o actualizados.

1.3 Evaluación de riesgo y priorización

Después de haber identificado y analizado las vulnerabilidades, es el momento de llevar a cabo una evaluación de riesgos y determinar la priorización. La primera etapa debería haber proporcionado informes de evaluación, que pueden utilizarse para determinar qué vulnerabilidades son más peligrosas para una organización.

Durante una evaluación de riesgos, los analistas de seguridad asignan a cada vulnerabilidad una puntuación de gravedad; los números más altos indican puntos débiles que deben abordarse lo antes posible. Las vulnerabilidades se clasifican en función de una serie de factores, entre ellos:

- Los sistemas afectados
- La información puesta en riesgo
- Facilidad de ataque o compromiso
- Daño potencial a la infraestructura y a la organización

1.4 Reparación y mitigación

La etapa final al realizar una evaluación de vulnerabilidad es la de remediación y mitigación. Esta etapa es realizada por nuestros profesionales de ciberseguridad, y se centra en encontrar formas de aliviar las debilidades mientras se desarrollan planes para disminuir la posibilidad de que vuelvan a aparecer las vulnerabilidades. Al crear planes de remediación y mitigación, los profesionales deben centrarse en dos factores:

- Gravedad: tras la priorización, los equipos deben abordar primero las vulnerabilidades más graves. Con el tiempo, deberían ser capaces de crear y publicar correcciones para cada vulnerabilidad detectada pero la corrección temprana se centra en las más peligrosas.

- Exposición a la vulnerabilidad: determinar si una vulnerabilidad está orientada al público o a la Red también debería ser una de las principales preocupaciones de los profesionales de la reparación. Las vulnerabilidades orientadas a Internet son más fáciles de explotar por los ciberdelincuentes, por lo que estas debilidades deben mitigarse en primer lugar, seguidas de los dispositivos propiedad de los empleados y los que almacenan información sensible.

ENTREGABLES

INFORME DE PENTESTING CAJA NEGRA:

En este informe se deben describir los hallazgos y resultados obtenidos sobre los targets del alcance para cada uno de los siguientes procesos:

- Escaneo de vulnerabilidades
- Reporte de identificación de vulnerabilidades
- Análisis de vulnerabilidades críticas y altas
- Recomendaciones de control
- Evidencias de las acciones ejecutadas en cada uno de los componentes de la auditoría sobre el target
- Resultado de las actividades cumplidas durante las fases descritas en el alcance de la auditoría sobre el target
- Resultado de las actividades cumplidas durante las fases descritas en el alcance de esta propuesta
- Reporte de Análisis vulnerabilidades web
- Auditoría a posteriori
- Recomendaciones a partir de los hallazgos identificados durante las fases del alcance.

INFORME DE PRUEBAS DE CARGA Y ESTRÉS

Este informe deberá incluir de manera detallada toda la documentación, resultados y análisis derivados del proceso de evaluación del rendimiento del sistema. Este informe contendrá:

- Alcance de las pruebas: descripción de los componentes evaluados, tipo de pruebas realizadas (carga, estrés, resistencia, picos y entorno técnico utilizado.
- Escenarios de prueba: detalle de los casos simulados, incluyendo el número de usuarios concurrentes, patrones de tráfico y acciones ejecutadas sobre la URL.
- Metodología y herramientas utilizadas: explicación de cómo se llevaron a cabo las pruebas y qué herramientas se emplearon (por ejemplo, JMeter, Gatling, LoadView).
- Resultados y métricas clave
  - Tiempos de respuesta (promedio, mínimo, máximo).
  - Tasa de errores, Transacciones por segundo.
  - Utilización de CPU, memoria y red.
  - Latencia y comportamiento ante picos.
- Análisis e interpretación: identificación de cuellos de botella, puntos de quiebre, fallos de estabilidad o degradación del rendimiento.
- Evidencias: capturas de pantalla, gráficos de desempeño, logs y reportes técnicos
- Recomendaciones técnicas: propuestas de mejora para optimizar el rendimiento, la escalabilidad y la robustez del sistema.
- Conclusiones generales: valoración final sobre la capacidad del sistema para operar bajo distintas cargas y sugerencias para futuros ciclos de prueba.

INFORME DE VULNERABILIDADES DE RED Y DE HARDWARE:

En este informe deberá describir los hallazgos y resultados obtenidos sobre los componentes de la plataforma de Infraestructura de red existente como:

- Numero de IP Publicas e internas, Servidores de Windows y Linux si aplica Virtuales y Fisicos, Bases de datos, dispositivos y host, dispositivos de red, Segmentación de red VPN, seguridad electrónica CCTV.
- Metodología de ejecución del análisis de vulnerabilidades.
- Plan de Pruebas de análisis de vulnerabilidades en ambiente controlado con al menos dos (2) herramientas de software
- Lista de equipos activos analizados durante el escaneo.
- Tipos de pruebas realizadas por activo o grupo de activos.
- Consolidado de las vulnerabilidades encontradas relacionando los datos del activo relacionado (nombre, IP, URL, tipo de activo).
- Listado del total de vulnerabilidades.
- Recomendaciones a corto y largo plazo a cada una de las vulnerabilidades encontradas para su tratamiento o mitigación.

Acreditación Experiencia Especifica equipo de trabajo

Los proponentes deben acreditar que cuenta con el equipo mínimo de trabajo de acuerdo a lo establecido a continuación. Adicionalmente deberá allegar dentro de su propuesta los documentos que acrediten el los requisitos establecidos por perfil de los siguientes profesionales:

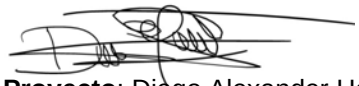
PERFIL	CANTIDAD	REQUISITOS
Líder de proyecto	1	Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniero de sistemas, Informática y/o electrónica. Título de posgrado en un programa de los mismos núcleos básicos del conocimiento enunciados, gestión o gerencia de proyectos o administración o afines. • Certificación en SOA.

PERFIL	CANTIDAD	REQUISITOS
		• Certificación en Azure. • Certificación en TOGAF 9. • Certificación Líder digital Management 4.0. • Certificación en Big Data. • Certificación metodologías agiles. Experiencia Profesional mínima de CINCO (05) AÑOS verificable con la tarjeta profesional.
Ingeniero de Implementación:	1	Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniero de sistemas, Informática y/o electrónica. Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniero de sistemas, Informática y/o electrónica. Título de posgrado en la modalidad de especialización en un programa de los mismos núcleos básicos del conocimiento enunciados. • Certificación en Profesional Network Security FPC o superior, o su equivalente en la marca oferente. • Certificación en CCNA. • Certificación en sistemas de Seguridad Electrónica. Experiencia Profesional mínima de CINCO (05) AÑOS verificable con la tarjeta profesional.

PERFIL	CANTIDAD	REQUISITOS
		Experiencia especifica mínima de un (1) contrato, en la dirección y/o gerencia y/o coordinador y/o profesional de proyectos ejecutados en entidades públicas o privadas que hayan tenido por objeto contractual o tengan incluido dentro de su alcance algunas de las actividades del presente objeto contractual (actualización, modernización, renovación de licenciamiento, migración, backup para los sistemas de información misionales, ciberseguridad y seguridad digital).
Profesional de despliegue	1	Titulo de pregrado en un programa según clasificación SNIES del núcleo básico de conocimiento en: sistemas, informática, electrónica, telecomunicaciones y/o afines. Profesional en un programa según clasificación SNIES del núcleo básico de conocimiento de: Ingeniero de sistemas, Informática y/o electrónica. Experiencia Profesional mínima de CUATRO (04) AÑOS verificable con la tarjeta profesional. • Certificación en Specialist Network Security o superior, o su equivalente en la marca oferente. • Certificación en CCNA. • Certificación en hacking ético.

_____
Nombre y firma Representante Legal

Personería
Distrital de Medellín



Proyecto: Diego Alexander Hoyos Arroyave **Reviso**: Olga Lucia Roldan Ruiz

PROYECTÓ:		REVISO:	
CODIGO	FGCT024	VERSION	10
RESOLUCION	804	VIGENCIA	10/11/2022

icontec ISO 9001 N° SC735-1

IQNET CERTIFIED MANAGEMENT SYSTEM