Colombia Digital

Contenido

Identificación del Ítem

- **Nombre del ítem:** Herramienta de vulnerabilidades para activos
- **Clasificación técnica:** servicios de ciberseguridad.
- **Prioridad o criticidad:** Alta

Descripción de la necesidad

La entidad designada por la Corporación Colombia Digital, como entidad responsable de la política exterior del Estado colombiano y de la representación diplomática ante el mundo, administra una infraestructura tecnológica crítica que soporta múltiples servicios misionales, incluidos los canales de atención consular, plataformas de cooperación internacional, servicios a ciudadanos colombianos en el exterior y sistemas diplomáticos y administrativos de alto nivel de confidencialidad.

En este contexto, y ante el aumento sostenido de ciberamenazas globales, la tecnificación de los atacantes, la automatización de los vectores de ataque y la exposición de la entidad en múltiples superficies (locales, web, nube y dispositivos de identidad), se hace imprescindible contar con una solución tecnológica integral de ciberseguridad, orientada a la gestión unificada de vulnerabilidades, la detección temprana de amenazas, la respuesta coordinada a incidentes de seguridad informática y el análisis de huella digital en entornos públicos.

La necesidad parte de la obligación institucional de garantizar la seguridad, disponibilidad, integridad y confidencialidad de los sistemas que soportan la política exterior del país y la atención a millones de ciudadanos dentro y fuera del territorio nacional, conforme a lo dispuesto por el marco normativo nacional (Ley 1581 de 2012, Decreto 620 de 2020, CONPES 3995) y estándares internacionales como ISO 27001, NIST y Zero Trust.

El objetivo es adquirir una solución tecnológica unificada que permita descubrir, evaluar y priorizar de manera continua los riesgos y vulnerabilidades en toda la superficie de ataque de la entidad, incluyendo activos de TI, recursos en la nube, aplicaciones web e identidades en el Directorio Activo

La solución deberá proveer una visión completa y unificada de la exposición al riesgo cibernético a través de un único portal , permitiendo a la entidad anticipar amenazas, priorizar esfuerzos de mitigación y tomar mejores decisiones de seguridad; con una duración de 36 meses. Esta solución deberá contemplar los siguientes tipos de activos:

A continuación, envió información solicitada a la fecha

- Total, de servidores físicos: **4**
- Total, de servidores virtuales En Hiperconvergencia: **187**
- Total, de servidores en nube: **16**
- Total, de equipos de comunicaciones y seguridad en nube: **5**
- Total, de consolas de administración y seguridad: **25**
- Total, de equipos de comunicaciones:

  - Switches **114**
  - Firewalls **11**
  - WLC **3**
  - APS **138**
  - NAC **2**
- Total, de equipos de registraduría: **8.**
- Identidades en el Directorio Activo: **4.000**

La solución deberá permitir la detección temprana de vulnerabilidades, la priorización de riesgos según criticidad y la generación de reportes técnicos detallados que faciliten la gestión de remediación por parte del equipo interno. Asimismo, deberá incluir actualizaciones automáticas de firmas, integración con herramientas de seguridad existentes (SIEM, ticketing) y capacidad de escaneo continuo y programado de los activos mencionados.

Con esta contratación, la entidad busca garantizar un nivel de seguridad proactivo y sostenible, minimizando riesgos de incidentes cibernéticos y cumpliendo con los estándares de seguridad, normativos y de continuidad operativa requeridos para la operación de sus sistemas críticos.

Lugar de ejecución / instalación

SEDES DE LA ENTIDAD DESIGNADA POR LA CORPORACIÓNY DE SU FONDO ROTATORIO	
UBICACIÓN DE SEDES	
SEDE	**DIRECCIÓN**
Nivel Central (San Carlos)	Carrera 5 N° 9 - 03 de Bogotá D.C.
Calle 98	Av 19 N° 98-03 Edificio Torre 100 de Bogotá D.C.
Pasaportes	Calle 12 C N° 8-27 de Bogotá D.C.
Cartagena	Centro - Calle de la Factoría N° 36-57 de Cartagena de Indias – DTC y C.

*Las sedes relacionadas están sujetas a cambio o cierre de las sedes.

La definición y ubicación de los diferentes equipos será indicada por el supervisor del contrato al momento del inicio del proyecto, esto de acuerdo con un replanteo que deberá hacer el contratista del diseño de red, incluyendo el plan de migración, implementación, puesta en funcionamiento y soporte.

Generalidades
La solución tecnológica deberá traducir la información obtenida por medio de evaluación de vulnerabilidades, evaluación de líneas base de configuración y evaluación de cumplimiento regulatorio sobre todos los activos TI, recursos en la nube, contenedores, aplicaciones web y sistemas de identidad, con el fin de priorizar acciones y comunicar el riesgo cibernético.

La solución ofertada deberá estar licenciada por un periodo de 36 meses para un total de 3000 activos, distribuidos de la siguiente manera:
La solución ofertada deberá soportar un licenciamiento flexible, el cual permita asignar el licenciamiento de acuerdo con las necesidades de evaluación y modificar dicha asignación siempre que sea necesario.
La solución ofertada deberá ser de licencia exclusiva de la Entidad, no se aceptarán soluciones de uso compartido, licenciamiento open source y reúso de licenciamiento.
La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.
La solución ofertada permitirá anticipar las amenazas y priorizar los esfuerzos de mitigación con el fin de evitar ataques.
La solución ofertada permitirá comunicar el riesgo cibernético, con la finalidad de tomar mejores decisiones.
La solución ofertada deberá contar con una vista de exposición, la cual permita enfocar los esfuerzos de seguridad brindando información clara y concisa de la exposición con respecto a la seguridad de la Entidad. De la misma forma deberá proporcionar una puntuación global unificada de la exposición obtenida a partir de diferentes fuentes de datos.
La solución ofertada deberá tener capacidades que permitan análisis, visualización y priorización de rutas de ataques proporcionando una respuesta enfocada de forma preventiva con el fin de interrumpir las rutas que pueden ser utilizadas por un atacante. Dicho análisis deberá ser soportado bajo las criticidades expuestas en el marco MITRE ATT&CK.
La solución ofertada deberá contar con un Inventario de Activos centralizado, con el objetivo de proporcionar una visibilidad completa hacia todos los activos
independientemente de la fuente de datos (Activos TI, Activos Nube, Aplicaciones Web, Identidades del Directorio Activo), permitiendo la agrupación por medio de etiquetas.
La solución ofertada permitirá gestionar la superficie de ataque externa, con el fin de identificar y reducir riesgo, brindando a la entidad la visión de un atacante.
La solución ofertada deberá realizar una gestión de vulnerabilidades basadas en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas.
La solución ofertada deberá realizar una evaluación de vulnerabilidades en entornos web de manera automatizada de manera completa y precisa.

La solución ofertada permitirá la protección de la infraestructura en la nube, permitiendo una visibilidad completa y de manera continua de exposiciones, vulnerabilidades y permisos de acceso; priorizando tareas de remediación.
La solución ofertada permitirá la protección del Directorio Activo, permitiendo identificar brechas de seguridad, malas prácticas de configuración y ataques en tiempo real.
La solución ofertada permitirá proveer métricas de evaluación de los programas de evaluación y remediación de la Entidad.
La solución ofertada permitirá realizar una evaluación de la exposición de manera comparativa entre unidades de negocio o ubicaciones a nivel interno de la entidad; de la misma forma con competidores de la industria de manera externa. Con el fin de obtener información que permitan una toma de decisiones certeras.
La solución ofertada deberá soportar funcionalidades de seguridad de doble factor de autenticación.
La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).
La solución ofertada deberá ser provista por un partner perteneciente al programa de canales de la fábrica que provea la solución y pertenecer por lo menos a uno de los dos niveles más altos del mismo. Se deberá presentar certificación del fabricante.
Con fin de garantizar el cumplimiento de los requisitos plasmados en el presente documento, el oferente deberá entregar junto con la oferta, los datahseet u hojas de datos y/o manuales de usuario que avalen el cumplimiento técnico de la solución ofertada. Se deberá presentar certificación del fabricante indicando productos y cantidades ofertadas.
Gestión de Vulnerabilidades
La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de los activos TI de la Entidad y hacer parte de una plataforma de gestión de ciberexposición.
La solución ofertada deberá estar en la capacidad de cubrir más de 88.900 CVEs IDs y 30.500 Bugtraq IDs, con una baja tasa de falsos positivos.
La solución ofertada podrá gestionar vulnerabilidades de sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores Web e infraestructuras esenciales y las infracciones de cumplimiento.
La solución ofertada deberá proporcionar una consola de gestión en la nube para la gestión de la información de seguridad.

La solución ofertada deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de:
· Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Dicha tecnología deberá estar patentada.
· Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes.
La solución ofertada deberá hacer uso de sensores los cuales podrán desplegarse en una variedad de plataformas, incluyendo: Windows Workstations y Servers, Linux, Mac OS ya sea en dispositivos virtuales o físicos.
La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad. Dicha calificación deberá ser obtenida a partir de los siguientes factores:
· La priorización deberá correlacionar información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación.
· El modelo de priorización deberá ser capaz de predecir si una vulnerabilidad tiene posibilidades de explotación en el futuro cercano.
· La priorización deberá considerar elementos de evaluación diversos, como: edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, número de días desde que se conoció una actividad de amenaza sobre la vulnerabilidad.
La solución ofertada deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo.
La solución ofertada deberá poder equilibrar cargas a través de múltiples escáneres de forma dinámica con base en la disponibilidad de cada escáner desplegado.
La solución ofertada deberá proveer una vista de soluciones que permitan enfocar en las secciones más importantes primero. Dicha vista deberá proveer los siguientes datos:
· Descripción de la solución.
· Número de dispositivos asociados a la solución.
· Número de instancias de vulnerabilidades asociadas a la solución.
· La calificación dinámica de probabilidad de explotación más alta para las vulnerabilidades asociadas a la solución.
La solución ofertada deberá incluir la posibilidad de programar ventanas de escaneo.

La solución ofertada deberá etiquetar los activos por grupos en función de las necesidades de la organización con la finalidad de categorizar los resultados y asignar las tareas correspondientes.
La solución ofertada deberá contar con un esquema de perfiles de usuarios basados en roles y garantizar los niveles adecuados de acceso a la plataforma.
La solución ofertada deberá permitir una evaluación de vulnerabilidades y/o postura de seguridad de manera autenticada, por de los siguientes sets de credenciales y sin limitarse a Windows, SSH y SNMPv3.
La solución ofertada deberá contar con un módulo que permita la creación de filtros para mejorar las búsquedas. Estos filtros deberán poder ser por lo menos: protocolo, IP, activo, identificador de la vulnerabilidad, identificador CVE, CVSS, vulnerabilidades por su puntaje dinámico, explotabilidad, severidad.
La solución ofertada deberá permitir la clasificación de activos identificados de manera manual o dinámica, con base en diferentes atributos encontrados en el análisis con base en etiquetas o en grupos de trabajo, para poder usarse en escaneos posteriores.
La solución ofertada deberá proporcionar información de capacidad de explotación contra las plataformas de validación como Metasploit, CoreImpact y Canvas.
La solución ofertada deberá ejecutar escaneos de auditoría de cumplimiento por medio de plantillas incluídas por defecto al menos para los siguientes tipos de sistemas: Adtran AOS, Alcatel TiMOS, Amazon AWS, Arista EOS, Blue Coat Proxy SG, Brocade Fabric OS, Check Point GAiA, Cisco ACI, Cisco Firepower, Cisco IOS, Citrix XenServer, Database, Dell Force10 FTOS, Extreme XOS, F5, FireEye, Fortigate Forti OS, HP Procurve, Huawei VRP, IBM iSeries, Juniper Junos, Microsoft Azure, Mobile Device Manager, Mongo DB, NetApp API, Office 365, OpenStack, NetApp Data ONTAP, PAN OS, Rackspace, RHEV, Salesforce.com, SonicWall SonicOS, Unix, VMWare vCenter/vSphere, Watchguard, Windows, ZTE Rosng
La solución ofertada deberá proporcionar por defecto plantillas de auditoria basadas en la política de cumplimiento de auditorías de CIS.
La solución ofertada deberá tener la capacidad de integrarse con sistemas tipo SIEM para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a vulnerabilidades. Por defecto debe tener la capacidad de integrarse al menos con las siguientes soluciones: Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic.

La solución ofertada deberá tener la capacidad de integrarse con soluciones tipo Privileged Access Management (PAM), pudiendo hacerlo de forma nativa al menos con los siguientes fabricantes: Arcon, Beyond Trust, Centrify, Cyber Ark, Hashi Corp, Thycotic.
La solución ofertada deberá proporcionar una integración con los sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Por lo menos se deben soportar: Microsoft WSUS/SCCM, Red Hat Satellite, HCL BigFix, Symantec Altiris, Dell KACE K1000.
Gestión de Vulnerabilidades en Aplicaciones Web
La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la Entidad; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
La solución ofertada deberá poder escanear aplicaciones modernas desarrolladas en frameworks JavaScript, AJAX, HTML5 and Single Page Applications.
La solución ofertada permitirá observar las vulnerabilidades a lo largo del tiempo, según su nivel de riesgo, clasificación en OWASP Top 10, de la misma forma que sus descripciones e instrucciones de remediación.
La solución ofertada deberá ser tipo SaaS, de la misma forma tendrá capacidad para ser desplegada como un contenedor de Docker, permitiendo el escaneo de sitios públicos y privados.
La solución ofertada permitirá realizar escaneos sin degradación de performance en el sitio, por medio de escaneos seguros, permitiendo definir sitios que no deben ser escaneados a partir de la URL, o extensiones de archivos
La solución ofertada deberá contar con dos escaneos predefinidos que permitan detectar rápidamente problemas de ciberhigiene:
- SSL/TLS Scan
- Config Audit Scan
La solución ofertada deberá permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.
La solución ofertada deberá soportar escaneos con autenticación avanzada como:
· HTTP Server Authentication
· Web Application Authentication (Login Form, Cookie Authentication, Selenium Authentication, API Key, Bearer Authentication)
· Client Certificate Authentication

La solución ofertada deberá contar con las siguientes plantillas de escaneo:
· API
· Config Audit
· log4Shell
· Overview
· PCI
· Quick Scan
· Scan
· SSL/TLS
La solución ofertada permitirá conocer el estado y progreso de una tarea de escaneo; de la misma forma generar tareas de escaneo programadas y envío de resultados por medio de correo electrónico.
La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura.
La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad.
Gestión de la Superficie de Ataque Externa
La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la Entidad; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
La solución ofertada deberá permitir una integración nativa con la solución de Gestión de Vulnerabilidades en Aplicaciones Web, que permita lanzar escaneos de vulnerabilidades y escaneos de sitios web de los activos descubiertos
La solución ofertada deberá identificar activos basado en:
· Registros DNS
· Direcciones IPs
· ASN
La solución ofertada deberá tener la capacidad de obtener información sobre la superficie de ataque externa en cuestión de minutos.
La solución ofertada deberá categorizar activos con base a más de 200 campos de metadata, permitiendo la utilización de filtros.

La solución ofertada deberá tener la capacidad de monitorear y notificar los cambios sobre los activos expuestos a internet de manera periódica: diaria o semanal.
La solución ofertada deberá estar en la capacidad de descubrir dominios relacionados a los activos identificados y clasificados en el inventario de la solución, suministrando razones del porque el dominio debería ser parte de la organización.
La solución ofertada deberá tener la capacidad de administrar los activos de la organización, permitiendo el uso de filtros, tags y tipo de datos.
La solución ofertada deberá estar en la capacidad de notificar los cambios que se presenten sobre los activos del inventario por medio de los siguientes medios:
· Correo Electrónico
· Slack
· ServiceNow
La solución ofertada permitirá incorporar un dominio sugerido al inventario
La solución ofertada permitirá el uso de subscripciones con el fin de notificar cambios sobre la superficie de ataque, incluyendo:
· Identificación de nuevos servidores
· Nuevos puertos abiertos o cerrados
· Nuevo Software
La solución ofertada contará con las siguientes subscripciones predefinidas:
· Compliance
· Expposición
· Geografía
· Higiene TI
· Marketing
· Tecnología
Gestión de Infraestructura Nube
La solución ofertada deberá Gestionar las Vulnerabilidades de todas las cargas de trabajo (CWPP), Gobierno y Cumplimiento de la infraestructura nube (CSPM), Gobierno de
Identidades (CIEM), Análisis e Identificación de Comportamiento Malicioso (CDR) y Gobierno de Infraestructura como Código (IaC / DevSecOps) de la entidad, bajo una arquitectura CNAPP; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.

La solución ofertada deberá soportar como mínimo con las nubes de Microsoft, Azure y Google.
La solución ofertada deberá poseer capacidades de autoremediación.
La solución ofertada deberá estar en la capacidad de evaluar y priorizar el riesgo de la infraestructura evaluada.
Gestión del Directorio Activo
La solución ofertada deberá auditar y monitorear de manera permanente la configuración del directorio activo con el fin de garantizar autonomía e imparcialidad en la detección de fallas; deberá ser provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
La solución ofertada deberá ser de un fabricante tercero al fabricante del Directorio activo a monitorear con el fin de garantizar una auditoria de un tercero con miras al aseguramiento del mismo.
La solución ofertada deberá proporcionar un análisis basado en grafos sobre las relaciones que se establecen entre los diferentes objetos que componen el directorio activo (usuarios, recursos, privilegios...).
La solución ofertada no debe requerir instalación de software o activaciones de funcionalidades sobre el directorio activo a monitorear.
La solución ofertada deberá estar en capacidad de inspeccionar y monitorear la configuración del directorio activo a partir de una cuenta de usuario con privilegios de lectura y con visibilidad de los contenedores de objetos borrados y atributos de credenciales.
La solución ofertada deberá mostrar gráficamente las relaciones del directorio activo para evaluar movimientos laterales desde activos potencialmente comprometidos.
La solución ofertada deberá poder visibilizar, monitorear y analizar eventos del directorio activo en tiempo real que potencialmente afecten el directorio activo.
La solución ofertada deberá ser compatible con Azure Entra ID para expandir el alcance de las identidades en una organización, sin incurrir en costos adicionales.
La solución ofertada deberá estar en capacidad de hacer una auditoría en tiempo real sobre el directorio activo, para alertar sobre posibles rutas de ataque y malas prácticas de configuración. Dentro de los hallazgos que ofrezca la solución se deben tener como mínimo:
· Configuración débil del protocolo Netlogon
· Certificados digitales asociados a cuentas privilegiadas
· Controladores de dominio gestionados por usuarios ilegítimos

· Uso de "primary group"
· Configuración riesgosa de ADCS
· Débiles políticas de credenciales
· Delegación de Kerberos riesgosa
· Falla de consistencia para "SDProp"
· Cuentas privilegiadas ejecutando servicios de kerberos
· Uso de algoritmos de cifrado débil en el servicio de PKI de directorio activo
· Controladores de dominio falsos
La solución ofertada deberá proporcionar información detallada sobre cada hallazgo, así como el detalle sobre cómo corregir cada configuración no recomendada.
La solución ofertada deberá soporta una cuenta señuelo cuyo único propósito es detectar a un atacante que intenta comprometer la red a través de Active Directory.
La solución ofertada deberá estar en capacidad de alertar de forma automática cuando se estén desarrollando ataques dirigidos al directorio activo, tales como:
· Ataques de enumeración
· Golden ticket - Yara Detection (debe permitir personalizar reglas Yara para identificar objetivos de ataque)
· Password spraying
· Dcsync
· Dcshadow
· OS Credential Dumping
· PetitPotam
· Explotación de DnsAdmins
· Password guessing
· Kerberoasting
· Extracción de NTDS, entre otros.
La solución ofertada deberá registrar en un repositorio independiente al directorio activo, los cambios que se realizan a nivel de configuración sobre el mismo.
La solución ofertada deberá permitir la generación de alertas sobre comportamientos específicos en el Directorio Activo, definidos por el administrador de la plataforma.

La solución ofertada deberá tener la capacidad de integrarse con sistemas tipo SIEM o SOAR para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a incidentes.
La solución ofertada deberá generar alertas en formato syslog o por correo electrónico.
Soporte
La solución deberá contar con soporte del fabricante en un esquema 24 x 7 x 365.
El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
El fabricante deberá contar con un equipo de Customer Success Management (CSM) en español.
Implementación
La solución ofertada deberá proveerse como servicio en la nube o en formato de despliegue en premisa. (Máquinas virtuales o bare metal)
La solución ofertada no deberá requerir la instalación de agentes o software en los controladores de dominio ni la creación de cuentas con privilegios administrativos.
La solución ofertada deberá ser totalmente implementada y configurada por el proponente, de acuerdo a las mejores prácticas del fabricante. Y complementada con los servicios de profesionales del fabricante para garantizar un adecuado despliegue.
Los servicios de implementación del fabricante deberán soportar hasta cinco de las tecnologías propuestas
Entrenamiento
Se deberá considerar capacitación directa de fabricante a nivel de la solución ofertada como mínimo para 2 integrantes del equipo de seguridad de la entidad, en al menos dos

Solución de administración, gestión y respuesta a eventos de ciberseguridad.

La entidad requiere una solución para la administración de la detección de ciber amenazas y la coordinación de respuesta de defensa, con el objetivo de fortalecer la estrategia de ciberseguridad de la entidad.

La solución debe incluir las siguientes funcionalidades:

Detección de Amenazas:

- Monitoreo continuo de eventos de seguridad: Recopilación y análisis de logs de seguridad de diversas fuentes (endpoints, servidores, red, aplicaciones, nube).
- Detección de anomalías y comportamientos sospechosos: Utilización de técnicas de aprendizaje automático (machine learning) e inteligencia artificial (IA) para identificar actividades anómalas.
- Integración con plataformas EDR existentes: Integración nativa con Forti EDR, Sophos, Crowdstrike, Carbon Black u otras plataformas EDR que la ENTIDAD pueda implementar en el futuro.
- Análisis de vulnerabilidades: Escaneo continuo de vulnerabilidades en la infraestructura de la ENTIDAD e identificación de activos expuestos.
- Identificación de indicadores de compromiso (IoC): Correlatar eventos de seguridad con bases de datos de IoCs para identificar amenazas conocidas.

Gestión de Incidentes:

- Clasificación y priorización de alertas: Asignación de severidad a las alertas en función del riesgo potencial.
- Investigación y análisis de incidentes: Herramientas para la investigación y análisis de incidentes, incluyendo la capacidad de realizar búsquedas, correlaciones y análisis forense.
- Automatización de flujos de trabajo de respuesta: Orquestación y automatización de acciones de respuesta a incidentes, como el bloqueo de IPs, aislamiento de equipos o la desactivación de cuentas de usuario.
- Generación de informes y dashboards: Generación de informes personalizables y dashboards con métricas e indicadores clave de rendimiento (KPIs) de seguridad.

Respuesta a Incidentes:

- Contención y erradicación de amenazas: Herramientas y procedimientos para contener y erradicar amenazas, incluyendo la eliminación de malware, el parcheo de vulnerabilidades y la restauración de sistemas.
- Recuperación de sistemas afectados: Capacidad para restaurar sistemas a un estado seguro después de un incidente.
- Coordinación de la respuesta a incidentes: Facilitar la comunicación y la colaboración entre los equipos de seguridad durante la respuesta a incidentes.

Inteligencia de Amenazas:

- Acceso a información actualizada sobre amenazas: Acceso a fuentes de inteligencia de amenazas, como feeds de amenazas, bases de datos de vulnerabilidades e informes de investigación.
- Análisis de la huella digital de la ENTIDAD en la web superficial y oscura: Monitoreo de la presencia de la ENTIDAD en internet, incluyendo la detección de sitios web falsos, filtraciones de datos y menciones en foros de hackers.

- Monitoreo de la reputación de la marca ENTIDAD: Detección de campañas de phishing, suplantación de identidad y otras amenazas que puedan afectar la reputación de la ENTIDAD.

Arquitectura: Solución SaaS (Software as a Service) alojada en la nube, con alta disponibilidad y redundancia.

Escalabilidad: Capacidad para procesar grandes volúmenes de datos (mínimo 25 GB por día) y adaptarse al crecimiento de la ENTIDAD.

Integración: Compatibilidad e integración con las plataformas y sistemas existentes en la entidad, incluyendo:

- Sistemas operativos Windows y Linux
- Firewalls (Palo Alto, Fortinet, Checkpoint)
- Plataformas de correo electrónico (Office 365)
- Directorio Activo
- Interfaz de Usuario: Interfaz intuitiva y fácil de usar, con capacidades de personalización y visualización de datos.
- Informes: Generación de informes personalizables y dashboards con métricas e indicadores clave de rendimiento (KPIs) de seguridad, con opciones de exportación en diferentes formatos.

API: Disponibilidad de una API documentada y segura para la integración con otras herramientas de seguridad de la ENTIDAD.

Cumplimiento: La solución debe cumplir con las regulaciones y estándares de seguridad aplicables, incluyendo la Ley 1581 de 2012 (protección de datos personales) y el Estándar ISO 27001.

La solución debe cubrir la totalidad de la infraestructura tecnológica de la ENTIDAD, incluyendo:

- Equipos de usuario final: Monitoreo de endpoints (portátiles, equipos de escritorio) para detectar malware, actividad sospechosa y vulnerabilidades.
- Servidores: Monitoreo de servidores físicos y virtuales, incluyendo servidores web, de correo electrónico, de bases de datos y de aplicaciones.
- Redes: Monitoreo del tráfico de red para detectar intrusiones, ataques de denegación de servicio (DoS) y otras amenazas.
- Aplicaciones: Monitoreo de aplicaciones web y de escritorio para detectar vulnerabilidades y ataques.
- Nube (Office 365): Monitoreo de la actividad en la nube de la ENTIDAD, incluyendo el acceso a correo electrónico, archivos y aplicaciones.
- Dominio web (https://www.Entidad.gov.co/): Monitoreo del dominio web de la ENTIDAD para detectar ataques, vulnerabilidades y cambios no autorizados, y todos los subdominios de la entidad.

Además de la solución tecnológica, se requieren los siguientes servicios:

- Instalación, Configuración y Puesta en Funcionamiento: El proveedor debe encargarse de la instalación, configuración y puesta en funcionamiento de la solución, incluyendo la integración con los sistemas existentes de la ENTIDAD.

- Soporte de Fábrica: Se requiere un servicio de soporte técnico de fábrica con un tiempo de respuesta garantizado de [Insertar tiempo de respuesta] para incidencias críticas.

- Capacitación y Transferencia de Conocimiento: El proveedor debe proporcionar capacitación al personal de la ENTIDAD sobre el uso y la administración de la solución. La capacitación debe incluir materiales de formación (manuales, tutoriales) y sesiones prácticas.

- Mantenimiento: El proveedor debe proporcionar actualizaciones y parches de seguridad para la solución de forma regular.

- La solución debe ser compatible con el idioma español.
- El proveedor debe contar con un equipo de soporte técnico con experiencia y certificaciones en ciberseguridad.

Alcance de suministro

El alcance del servicio contempla dos componentes principales: pruebas de penetración y análisis de vulnerabilidades, enfocados en garantizar la seguridad integral de los activos tecnológicos de la entidad durante el período contractual.

Servicio de Ethical Hacking

- Ejecución de dos (2) pruebas de Ethical Hacking sobre 250 dispositivos de la infraestructura tecnológica, incluyendo servidores, dispositivos de red y sistemas críticos.
- Identificación de vulnerabilidades, debilidades de configuración, errores de diseño y posibles vectores de ataque que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.
- Aplicación de metodologías reconocidas internacionalmente (OWASP, NIST, PTES, OSSTMM) para garantizar un análisis sistemático y confiable.
- Elaboración de reportes técnicos detallados, incluyendo hallazgos, evidencia, nivel de criticidad y recomendaciones de mitigación priorizadas.
- Seguimiento, acompañamiento y verificación de la remediación de las vulnerabilidades identificadas.
- El CONTRATISTA deberá contemplar el suministro de servicios profesionales adicionales para la remediación de las vulnerabilidades encontradas, garantizando que las recomendaciones generadas por el Ethical Hacking puedan ser implementadas de manera efectiva en los sistemas, aplicaciones y activos de la entidad.

Especificaciones técnicas mínimas requeridas

Las especificaciones técnicas de la solución se establecen son las siguientes:

Tipos de pruebas a realizar:

Gestión de vulnerabilidades: Gestión de vulnerabilidades consiste en una evaluación exhaustiva y sistemática de los sistemas de la organización, empleando tanto herramientas automatizadas como revisiones manuales. A diferencia del Pentesting, este enfoque se centra en identificar y clasificar las vulnerabilidades sin intentar explotarlas activamente. El objetivo es permitir la corrección oportuna de dichas fallas, garantizando una mayor seguridad del entorno tecnológico. Al utilizar un enfoque de Caja Gris, se combina información interna proporcionada por la organización con simulaciones externas, permitiendo identificar fallos que podrían pasar desapercibidos en evaluaciones tradicionales. Este método resulta ideal para detectar vulnerabilidades internas y priorizarlas según su impacto potencial sobre los activos críticos, proporcionando una visión más integral de los riesgos.

Enfoque de Caja Gris:

- Acceso a configuraciones de red e información interna limitada, lo que permite una evaluación más precisa de las debilidades estructurales.
- Credenciales de acceso con privilegios restringidos, simulando un ataque desde el interior de la red con acceso autorizado.
- Conocimiento parcial de la arquitectura y sistemas, lo que ofrece una visión más cercana a la de un atacante con acceso interno limitado.

Estándares y Normativas Aplicables:

Es necesario seguir las mejores prácticas definidas por reconocidos estándares internacionales, garantizando un enfoque metodológico y alineado con la industria:

- ISO/IEC 27001: Este estándar internacional para la gestión de la seguridad de la información establece las directrices para identificar, gestionar y reducir las vulnerabilidades dentro de un sistema de gestión de seguridad.
- NIST SP 800-53: Publicado por el Instituto Nacional de Estándares y Tecnología de EE.UU., este estándar proporciona un marco para la gestión de riesgos, que incluye el Gestión de vulnerabilidades y las estrategias de mitigación.
- OWASP Top 10: Aunque más enfocado en aplicaciones web, las prácticas recomendadas por OWASP son clave para identificar vulnerabilidades comunes que pueden afectar tanto a sistemas como a aplicaciones.
- CVE (Common Vulnerabilities and Exposures): Para la identificación precisa de vulnerabilidades, se hace uso del sistema CVE, que proporciona un lenguaje común y estandarizado para nombrar y describir vulnerabilidades.

Análisis de Metodología Aplicada:

- Identificación de Vulnerabilidades
- Clasificación y Priorización
- Recomendaciones de Mitigación

NOTA:

Los elementos deben ser compatibles 100% con los equipos de la entidad, y el fabricante deberá aportar certificación que lo acredite.

Debe Garantizarse la instalación en cada nodo de acuerdo con las especificaciones del fabricante.

El análisis se debe hacer para mínimo 250 equipos o dispositivos.

En ejecución:

De emitirse certificación de fabrica donde indique que los equipos intervenidos no perderán la garantía.

Debe generarse aprobación por parte del fabricante de la instalación de los elementos, con el fin de no afectar el contrato de soporte.

PARA ESTE ANEXO TECNICO SE BUSCA CONTRATAR "CONTRATAR LA IMPLEMENTACIÓN, SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN, PUESTA EN FUNCIONAMIENTO, SOPORTE TÉCNICO, MANTENIMIENTO Y CAPACITACIÓN DE UNA SOLUCIÓN INTEGRAL PARA LA ADMINISTRACIÓN, GESTIÓN Y RESPUESTA A EVENTOS DE CIBERSEGURIDAD, BAJO MODALIDAD SAAS (SOFTWARE AS A SERVICE), CON EL FIN DE FORTALECER LA ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN DE LA ENTIDAD DESIGNADA POR LA CORPORACIÓN, CONFORME A LAS ESPECIFICACIONES, FUNCIONALIDADES, ALCANCES Y CONDICIONES TÉCNICAS ESTABLECIDAS EN EL ANEXO TÉCNICO QUE FORMA PARTE INTEGRAL DEL CONTRATO." LOS SIGUIENTES SERVICIOS ENCONTRADOS EN LA OFERTA ECONOMICA ANEXADA:

3	Solución de administración, gestión y respuesta a eventos de ciberseguridad	Unidad	1