ANEXO TÉCNICO No. 2 – SERVICIOS DE SEGURIDAD TECNOLÓGICA.

El presente anexo describe los procedimientos, características técnicas, exigencias y requisitos para la provisión de los servicios requeridos contemplando los siguientes aspectos:

- **Infraestructura de seguridad**
- **Servicios para Networking**
- **Servicios gestión de identidades**
- **Servicios SOC**
- **Servicios de certificados**
- **Servicios antimalware - antivirus**
- **Servicios prevención de pérdida de datos (DLP)**
- **Servicios NAC (Network Access control)**
- **Servicios seguridad web**
- **Acuerdos de nivel de servicio**
- **Transición de entrada en operación**.
- **Transición, cierre y entrega**.

1. INFRAESTRUCTURA DE SEGURIDAD

ENTerritorio cuenta con dos (2) centros de datos en Modalidad IaaS (Centro de Datos Principal en modalidad de IaaS CCP y Centro de Datos Alterno en modalidad de IaaS CCA), un (1) Centro de Datos Básico (CCB) y las sedes de Calle 26 y la sede del Archivo Central Histórico, para garantizar la operación integral de TIC, para cumplir con los compromisos establecidos en la normatividad que aplica a la Entidad y para culminar exitosamente los proyectos en ejecución:

No	Sede: Nombre, Propiedad y Ubicación	Abreviatura	Necesidad que soporta
1	Centro de Datos Básico Propiedad de Enterritorio Calle 26 No 13-19 Bogotá Edificio Enterritorio Piso 28	CCB	Soporta los siguientes servicios básicos: Directorio Activo Microsoft Secundario para estaciones de usuario final replicado desde el Directorio Activo principal en el CCP, Servidor DNS, Servidor DHCP, Servidor de Impresión, Controladora Antivirus a Endpoint, Consola Exchange con funcionalidad Relay de correo. Firewall en HA (Fortigate), Analizador de logs del FW (Fortianalizer), Nessus. Servidores de Cámaras de Seguridad. Servidores de Servicios Biométricos
2	Centro de Datos Principal en modalidad de IaaS	CCP	Centro de Datos principal en modalidad de IaaS de Enterritorio con el 100% de los servicios de TIC ambientes de pruebas, producción y proyectos en implementación, alojados en Tenant de uso exclusivo de Enterritorio.
3	Centro de Datos Alterno en modalidad de IaaS	CCA	Centro de Datos alterno en modalidad de IaaS de Enterritorio para los servicios de contingencia del ambiente de producción alojados en Tenant de uso exclusivo de Enterritorio.
4	Sede Archivo Central Histórico. Propiedad de Enterritorio	ACH	Sede de documentación, digitalización, indexado y custodia de la documentación física de ENTerritorio.

	Calle 12 No. 79a-25 Villa Alsacia de la ciudad de Bogotá		

Cuadro. Centros de datos Enterritorio

Se requiere implementar los sistemas de protección y gestión necesarios para garantizar la integridad, confidencialidad y disponibilidad de la información, así como la conexión y acceso seguro a los Centros de Datos descritos anteriormente.

Todas las características de seguridad solicitadas se deben ajustar a la familia de normas ISO27000[1]. El CONTRATISTA debe realizar los ajustes que fueran necesarios sobre los sistemas de seguridad de acuerdo con lo contemplado en estas normas, al igual que implementar controles orientados a la protección de la información para evitar, identificar y responder a intentos de intrusión o ataques informáticos. Los controles mínimos por contemplar son:

- Protección de intrusos en tiempo real:
  - Sistemas de detección de intrusos IDS
  - Sistemas de prevención de intrusos IPS
  - Firewall
- Control de acceso a red (Network Access Control-NAC).
- Gestión de identidades, autenticación y manejo de contraseñas.
- Protección de malware, antivirus y ataques de día cero para:
  - Terminales de usuario,
  - Servidores
  - Sistema de correo.
- Cifrado:
  - Implementación y administración de las VPN para los usuarios externos a las sedes.
  - Comunicaciones encriptados entre las sedes.
  - Respaldos de bases de datos, imágenes de Servidores y Sistemas Operativos, y copias de respaldo.
- Protección para Aplicaciones WEB con una solución independiente.
  - Sistema WAF.
  - Servicio, de prevención, detección y respuestas a ataques de negación de servicios DoS.
- Correlación de logs y eventos (SIEM) para:
  - Servidores en IaaS.
  - Servidores físicos de CCB.
  - Dispositivos de Red.
  - Office365.
- Gestión y aplicación de actualización y parches para:
  - Servidores.
  - Estaciones de usuario.
  - Dispositivos de Red
- Sistema de Prevención de Perdida de Datos (DLP).
  - Infraestructura en IaaS.
  - Infraestructura de Office365.

[1] ISO27000: estándares sobre Sistemas de Gestión de la Seguridad de la Información de ISO/IEC.

  - Estaciones de usuario.
- Hardening de SO, BD y sistemas de enrutamiento y conmutación.
- Desarrollo Seguro:
  - Enmascaramiento en las bases de datos de pruebas.

El CONTRATISTA debe proveer, configurar, administrar y mantener los dispositivos de seguridad de cada uno de los Centros de Datos, al igual que configurar, administrar, mantener y renovar el licenciamiento con fabricante de los dispositivos de propiedad de ENTerritorio ubicados en el Centro de Datos Básico de calle 26 descritos a continuación:

- Fortigate_500D en Alta Disponibilidad.
- FortiAnalyzer 400E.

El contratista debe ofertar en un ítem independiente el costo de arrendamiento de los anteriores 2 dispositivos a partir de junio de 2023 cuando finalice la vida útil de los mismos.
Adicionalmente se deben proveer, configurar y administrar los equipos de seguridad perimetral en modalidad de Arrendamiento de la sede del Archivo Central Histórico. Actualmente se cuenta en modalidad arrendamiento con los siguientes equipos:

- FortiGate-80F
- FortiAP-221E

Los controles de seguridad de NGFW (IPS, IDS, Firewall), WAF y NAC deben estar en capacidad de integrarse con la plataforma FortiAnalyzer con la que cuenta la entidad, para tener funcionalidad de logging y reportes centralizados.

El CONTRATISTA debe mantener la operación de esos sistemas de seguridad mediante el arrendamiento de equipos de características iguales o superiores. FortiAP-221E.

Ítem	Descripción	Cantidad
1	• NGFW (Next Generation Firewall) como mínimo con las siguientes características técnicas: ○ Equipo para instalar en Rack de 1U. Debe incluir instalación y montaje. ○ Implementación en alta disponibilidad en Centro de Datos Principal y Centro de Datos Alterno ○ Puertos Ethernet WAN: 12 (GE) y 2 (10G SFP+) ○ Puertos LAN: 8 (GE) y 2 (10G SFP+) ○ Debe contar con interfaz de consola ○ Throughput de Firewall mínimo de 8Gbps ○ Administración: ▪ Debe tener soporte Multifactor MFA para los administradores ○ Soporte para VLAN 802.1q ○ Soporte par puertos troncales ○ Soporta balanceo de carga, failover, alta disponibilidad (HA) ○ Soporta balanceo de carga entrante ○ Soporte para VPN: ▪ Soporte para Server, IPsec, PPTP VPN Server, PPTP/L2TP ▪ Mínimo 500 usuarios ▪ SSL-VPN Throughput mínimo 6 Gbps ○ Debe tener gestión y monitoreo de ancho de banda en tiempo real ○ Integración de usuarios con Directorio Activo (LDAP)	1

	○ Incluir soporte de QoS para VoIP ○ Incluir filtrado y bloqueo de web por URL ○ 8 millones de sesiones concurrentes ○ Incluir IPS (mínimo 9Gbps) ○ Throughput de Prevencion de Amenazas 7 Gbps ○ Incluir protección contra malware, antivirus, Antibotnets, IDS ○ Inspección de tráfico SSL ○ Debe contar con logs locales y soporte para logs remotos	
2	• Acces Point Wifi para interiores: ○ Numero de radios: mínimo tres ○ Antenas internas mínimo 3 ○ Bandas de operación: 2.400–2.4835, 5.150–5.250, 5.250–5.350, 5.470–5.725, 5.725–5.850 ○ Estándares soportados: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3az ○ Velocidad de transferencia: ▪ En banda 2.4Ghz: mínimo 500 Mbps ▪ En banda 5Ghz: mínimo 1200 Mbps ○ 2 Puertos RJ45 ○ Debe incluir herrajes para Montaje en techo ○ Alimentación 802.3af PoE. Se debe incluir el inyector PoE ○ Soporte de WiFi 6	2
3	• Controladora WiFi: o Capacidades de Filtrado Web, WIDS y Control de Aplicaciones o Capacidad de Portal cautivo o Capacidad de band steering o Distribución de clientes en los AP. o Manejo de QoS o Soporte de IPv6 o Soporte de hasta 500 AP o Protección contra Asociación / Autenticación / Inundación EAPOL, Desautenticación broadcast, MAC spoofing, Detección y contención de red ad-hoc, Detección de puente inalámbrico (wireless bridge), Detección de AP mal configurados, Verificación de OUI MAC	2

2. SERVICIOS PARA NETWORKING

Dentro la gestión de Networking (entendida como servicios de enrutamiento y conmutación), Centros de Cómputo, seguridad, y administración de la nube pública el CONTRATISTA deberá proveer los siguientes servicios:

- Administración de Políticas de Seguridad: Este componente está conformado por administración, gestión, mantenimiento y actualización de los dispositivos y herramientas mediante las cuales se implementan las políticas y procedimientos de seguridad definidos en el Sistema de Gestión de Calidad de ENTerritorio.

- Administración de redes y subredes: Implementación y mantenimiento de las redes y subredes necesarias para una adecuada segmentación y enrutamiento entre los diferentes segmentos y ambientes de producción, pruebas y desarrollo; así como entre las diferentes infraestructuras IaaS y las sedes de ENTerritorio.

  Administración, habilitación y asignación de servicios de conectividad a la red para

usuarios.

Las configuraciones solicitadas de red y seguridad se deben realizar para direccionamiento y tráfico IPv4 e IPv6.

Coordinación y supervisión con los ISP de la instalación de enlaces y servicios de telecomunicaciones y ejecución de protocolos de pruebas de aceptación.

Contar con sistemas de IPS e IDS.

Administrar, aprovisionar, eliminar y depurar las redes VPN que requiera ENTerritorio.

- Administración de Riesgos e incidentes de Seguridad: provee las herramientas para la identificación, reporte, métrica, alerta y gestión de eventos e incidentes de seguridad.

  En caso de la materialización de un riesgo, el CONTRATISTA, en coordinación con el Supervisor del Contrato o quien este designe, debe actuar como primer respondiente acorde al procedimiento P-TI-10 GESTION DE INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN.

- Auditoria: Configurar los registros de auditoria de todos los dispositivos de hardware y software que hacen parte de la infraestructura tecnológica en todas las sedes y centros de datos.

- Actualizaciones: De versiones e instalación de parches de software, firmware y sistemas operativos, de acuerdo con las recomendaciones de los fabricantes.

  Contar con mecanismos para regresar (rollback) a la última versión estable en caso de que las actualizaciones fallen.

- Control de ingeniería de tráfico: tanto en la red LAN, WAN y WiFi, a fin de identificar potenciales congestiones, sobre utilización o subutilización de los anchos de banda disponibles.

  Estudiar y definir los parámetros de impacto en la red en materia de tráfico, al momento de liberar nuevos servicios, nuevas aplicaciones o actualizaciones, haciendo las reconfiguraciones para asegurar el adecuado desempeño de las aplicaciones en la red.

- Gestión de identidades: este componente permite la administración y autenticación de usuarios, incluye la creación, baja y auditoria de los usuarios en todos los sistemas.

- Gestión de la capacidad: Administración, coordinación y ejecución de ampliaciones a nivel de equipos de la red LAN, WAN, Wifi y seguridad.

- Implementación de portales cautivos: para el acceso a las redes WiFi en las sedes de ENTerritorio descritas en el cuadro No 1.

- Integración: proporcionar un punto central de monitoreo y gestión de todos los aspectos

de la seguridad de la Entidad que permita tomar acciones preventivas ante los incidentes detectados. Todos los sistemas de seguridad deben operar de manera integrada y deben reportar al SIEM.

El CONTRATISTA debe realizar el estudio y análisis de los logs y alarmas que arrojen los sistemas de administración y gestión de la seguridad.

- Monitoreo de la seguridad: El CONTRATISTA deberá monitorear los componentes de comunicaciones, enrutamiento, conmutación, almacenamiento, procesamiento y seguridad asociados a los centros de datos y las sedes.

  Asimismo, deberá notificar de forma inmediata a la supervisión del contrato o a quien este delegue toda novedad, alerta e incidencia presentada.

- Respaldos: cumplir con la política de respaldo y restauración de la información de la Entidad definida en el ANEXO TÉCNICO 1: SERVICIO ESPECIALIZADO DE CENTRO DE CÓMPUTO PARA AMBIENTES PRODUCTIVOS Y DE PRUEBAS, NUBE PUBLICA, Y SERVICIOS DE ADMINISTRACIÓN Y MANTENIMIENTO.

- Soporte técnico integral ilimitado: en horario 7x24x365 para la plataforma de red de la Entidad (LAN, WAN, WiFi) en las sedes y centros de datos.

  Los horarios de producción serán definidos por el Grupo de Tecnologías de la Información, para organizar y automatizar las tareas y trabajos específicos para la red, sistemas y aplicaciones.

3. GESTION DE IDENTIDADES

El contratista deberá proveer la gestión de inicio de sesión unificado, a través de un SSO integrado con el Directorio Activo de ENTerritorio.

En la actualidad se cuenta con el servicio de SSO de Oracle OID, el cual debe ser migrado durante la vigencia del contrato al SSO de Microsoft Azure.

Todas las aplicaciones que se implementen deben estar integradas con el SSO a implementarse. La Migración se debe realizar en coordinación con el Grupo de Tecnologías de la Información o los proveedores de las aplicaciones existentes. Se entregará el Mapa de Aplicaciones al Inicio del Contrato.

4. SERVICIOS SOC

El contratista deberá prestar los servicios de ciberseguridad, SOC (Centro de Operaciones de Seguridad), para ello deberá realizar seguimiento y análisis de la actividad de la red, servidores, puntos finales, bases de datos, aplicaciones y sitios web, en horario 7x24x365, buscando eventos anómalos que puedan ser indicio de un incidente o compromiso de seguridad. Mejorando la capacidad de vigilancia, detección y respuesta a amenazas en la operación diaria de la Entidad.
El contratista deberá validar que los posibles eventos e incidentes de seguridad se identifiquen, analicen, defiendan, investiguen e informen correctamente, cumpliendo con los parámetros, las

mejores prácticas[2] en seguridad, y normatividad establecida en la Entidad[3], para ello como minino debe cumplir:

- Monitoreo centralizado de logs y correlación de eventos: Contar con las herramientas para correlacionar eventos y logs en tiempo real. El sistema SIEM recopilará los eventos de todos los dispositivos de red, seguridad, autenticación (Directorio Activo), bases de datos, aplicaciones, sitios web, que el supervisor del contrato determine.
- El tiempo de almacenamiento de los logs se hará de acuerdo con la política de retención establecidos por el supervisor del contrato. Mínimo se debe contar con un tiempo de retención de 6 meses.
- Deberá tener la capacidad de realizar:
    - Detección en tiempo real de amenazas y actividades anómalas.
    - Correlación de eventos e incidentes de diferentes dispositivos, incluyendo plataformas de seguridad, servidores, switches, routers de diferentes fabricantes.
    - Posibilidad de generación de reglas de parsing para logs de eventos de plataformas que no estén soportadas.
    - Personalización y parametrización de reglas de correlación.
    - Descubrimiento de dispositivos automático y manual.
    - Capacidad de procesamiento hasta 1000 EPS o 100 dispositivos
    - Manejo de indicadores de compromiso licenciados.
    - Auditoría de políticas de red y de servidores.
    - Integración con fuentes de inteligencia de amenazas de terceros
    - Gestión de logs.
    - Análisis de seguridad orientado al riesgo.
    - Cumplimiento en el marco de la serie de normas ISO27000.
    - Alertas para prevención y detección de intrusiones y vulnerabilidades.
    - Alertas de robo de Información confidencial.
    - Detectar, analizar, contener y remediar eventos e incidentes de seguridad que se puedan presentar.
    - Detección de modificación de archivos o carpetas en servidores críticos.
    - Detección de cambios de registro en servidores Windows
- Guardar la confidencialidad de la información recopilada, asegurando que no será utilizada para fines diferentes a los indicados por ENTerritorio, y que no será expuesta o compartida con ninguna otra persona, Entidad u organización sin la autorización expresa del Supervisor del Contrato.
- Deberá crear las alarmas de acuerdo con los niveles de criticidad que sean acordados con el supervisor del contrato. Las notificaciones se harán vía correo electrónico.
- Informes y reportes:
    - El SoC debe estar en capacidad de generar reportes e informes cuando el supervisor del contrato lo requiera. Los formatos de reportes soportados como mínimo serán .DOC, PDF, CSV y Texto Plano.
- El servicio de SOC deberá contar con funcionalidades de análisis de comportamiento, detección avanzada de amenazas y respuesta a incidentes.
- La gestión de incidentes de seguridad se debe realizar mediante la herramienta de Gestión de incidentes de Enterritorio:
    - Se debe crear un ticket asignando: número de incidente, criticidad, riesgo evaluado, alertas generadas y respuesta ante el mismo.

[2] Las mejores prácticas contempladas en las normas ISO 27000
[3] Manuales, procedimientos, guías, instructivos y formatos del Sistema de Gestión de Calidad de ENTerritorio

- Se debe guardar registro de las acciones tomadas por el analista, los escalamientos y demás actividades realizadas, de forma que se pueda establecer una línea de tiempo del incidente.

- Proveer un servicio de análisis forense para los casos en que sea necesario investigar incidentes informáticos. Los procedimientos de investigación deberán estar en concordancia con la norma ISO/IEC 27037[4] y la legislación vigente en Colombia.

5. SERVICIOS DE CERTIFICADOS

El contratista debe proveer los certificados de seguridad de la entidad que cumplan con:

- Técnicas y configuraciones que mantengan la integridad y confidencialidad de los datos en tránsito.
- El manejo de las llaves privadas de cifrado será acordado con el supervisor del contrato, en concordancia con la política de Controles Criptográficos de la Entidad.
- Proveer y configurar los certificados y esquemas de encripción para las VPN y para los canales de datos privados. Las características de estas serán acordadas con el supervisor del contrato.
- Proveer a ENTerritorio los certificados digitales necesarios para la correcta y segura operación de las diferentes soluciones:
  - Certificado Digital en modalidad wildcard para los dominios www.enterritorio.gov.co y sus subdominios.
  - Certificado Digital para el dominio sso.enterritorio.gov.co.
  - Certificados para el dominio y la aplicación www.tecuidamos.com.co.
  - Certificados de telefonía y comunicaciones. El sistema actual utiliza 2 certificados, siendo inherentes al servicio de telefonía. En caso de que la implementación de la solución de telefonía descrita en el Anexo 6 requiera de certificados digitales, el contratista deberá garantizar dichos certificados con el fin que funcione sin inconvenientes durante el plazo de ejecución del contrato.
- Proveer los certificados con el protocolo TLS 1.2. (o superior). Si por razones de compatibilidad se requiere instalar una versión anterior de TLS, esta debe ser aprobada por el supervisor del contrato.
- Los certificados digitales usarán como mínimo ECC (256 bits) o RSA (2048 bits). Para las funciones de HASH se debe usar mínimo SHA-256.
- Todos los algoritmos de cifrado de los certificados, encripcion y hash deben ser aprobados previamente con el supervisor del contrato.

6. ANTIMALWARE - ANTIVIRUS

El CONTRATISTA debe proveer y administrar un servicio de software de antivirus debidamente licenciado. Debe contar como mínimo con las siguientes características:

- Proveer clientes y cobertura para todos los equipos relacionados en el ANEXO 3. ARRENDAMIENTO.
- Contar con consola de administración centralizada.

[4] ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

- Contar con clientes para para toda la infraestructura de servidores en las sedes, centros de datos, IAAS y nube pública.
- Contar con cliente para correo electrónico en la nube y Outlook de acuerdo con el ANEXO 7. MOVILIDAD INTEGRAL.
- La solución implementada debe proteger de: virus, troyanos, gusanos, spyware, ransomware, ataques de día cero, protección de las transacciones financieras, detección, bloqueo inteligente de anuncios, antispam y bloqueo de phishing y amenazas que pueda poner en riesgo la operación de la infraestructura aprovisionada.
- Análisis en tiempo real:
  - Escáner en tiempo real no debe sobrecargar los equipos o servidores, y debe mantener porcentajes de uso inferiores a un 50% de ocupación de procesamiento, memoria RAM y disco duro. Se debe limitar el uso de recursos usados por el antivirus.
- Actualizaciones automáticas que puedan gestionarse bajo ventanas de mantenimiento y horas específicas programadas.
- El CONTRATISTA debe proveer cualquier infraestructura que requiera para el monitoreo, operación o administración de la solución de antivirus.
- La plataforma de monitoreo deberá ser capaz de gestionar equipos y usuarios remotos que se encuentren fuera de la infraestructura física de la Entidad.
- Realizar la parametrización de políticas de antivirus y antimalware, programación de análisis en busca de virus y actualización del producto instalado en usuarios finales e infraestructura.
- La solución de antivirus debe integrar los logs con el SIEM que se implemente.

7. PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)

- El CONTRATISTA debe proveer y administrar un servicio de software de prevención de pérdida de datos (DLP) debidamente licenciada. Debe contar como mínimo con las siguientes características:

  - Proveer clientes y cobertura para todos los equipos relacionados en el ANEXO 3. ARRENDAMIENTO.
  - Contar con consola de administración centralizada.
  - Contar con clientes para toda la infraestructura de servidores en las sedes, centros de datos, IAAS y nube pública.
  - Configuración e implementación de reglas para:
    - Control de copiado de textos y documentos.
    - Detección y bloqueo de memorias USB y dispositivos plug and play.
    - Control de impresión.
    - Control de capturas de pantalla.
    - Control de correo electrónico (cliente y nube).
  - Apoyo en la creación de diccionarios personalizados de términos para bloqueo.
  - Implementación de políticas de clasificación de la información.
  - Realizar la integración de los logs del DLP con el SIEM.

8. NAC (NETWORK ACCESS CONTROL)

El Contratista debe proveer el servicio de NAC para el acceso a las redes de ENTerritorio. La solución podrá ser un appliance físico instalado en sitio o un appliance virtual integrado con las redes en la nube de ENTerritorio.
Debe contemplar, como mínimo, las siguientes características:

- Gestión del ciclo de vida de las políticas: permite gestionar y monitorear el cumplimiento de políticas de seguridad.
- Creación de perfiles: permite asignar roles y perfiles a los usuarios y sus dispositivos; el sistema debe permitir el aprovisionamiento y gestión de usuarios para esquemas Trae Tu Propio Dispositivo- TTPD (Bring Your Own Device-BYOD). El CONTRATISTA debe implementar lo contemplado en la guía del Sistema de Gestión de Calidad G-TI-01 GUIA TRAE TU PROPIO DISPOSITIVO (TTPD).
- Acceso a redes de invitados: administra el acceso de usuarios invitados a través de un portal cautivo de autoservicio personalizable que incluya registro y autenticación.
- Verificación de la política de seguridad: evalúa el cumplimiento de la política de seguridad por tipo de usuario, tipo de dispositivo y sistema operativo.
- Respuesta a incidentes: permite la aplicación automática de políticas de seguridad que bloqueen y aíslen dispositivos.
- Soporte de 802.1X, autenticación basada en MAC y MAB (MAC Authentication Bypass)
- Capacidad de integración con soluciones MDM (al menos AirWatch y Microsoft InTune)
- Cantidad de usuarios soportada:
    - La solución debe contar con un esquema dinámico de licenciamiento que permita incrementar o disminuir la cantidad de usuarios de acuerdo con la necesidad de la entidad.
    - Se estima que la cantidad de usuarios promedio mensual estará entre 750 y 1.000 usuarios. Con una posibilidad de crecimiento de 10%.
- Integración: se debe integrar con las soluciones de enrutamiento, conmutación y seguridad solicitadas en el presente Anexo.
- El contratista deberá realizar la configuración y puesta en funcionamiento de la solución de NAC de acuerdo con las políticas que el Supervisor del Contrato le indique.

9. SEGURIDAD WEB

El CONTRATISTA debe proveer soluciones de seguridad web para todas las páginas públicas de la Entidad. Debe contemplar, como mínimo con las siguientes características:

- Servicio para la protección de aplicaciones WEB (sistema WAF):
    - Se requiere protección a todos los dominios de la Entidad.
    - La disponibilidad del servicio debe cumplir el acuerdo de nivel de servicio descrito en el presente documento.
    - Protección contra las amenazas del OWASP Top 10
    - Protección para APIs
    - Mitigación contra bots
    - Políticas de geolocalización
    - Protección contra defacement
- Servicio de prevención, detección y respuestas a ataques de negación de servicios DoS:

- Se requiere protección a todos los dominios y servicios Web de la Entidad.
- Troughtput estimado 1Gbps

10. ACTUALIZACIÓN, HARDENING Y GESTIÓN DE VULNERABILIDADES

10.1. ACTUALIZACION:

- Se requiere que el CONTRATISTA actualice los sistemas operativos de los servidores, estaciones de trabajo y equipos que lo requieran. Este procedimiento se debe ejecutar 3 veces al año o cuando los fabricantes publiquen actualizaciones críticas.
- El plan de actualización debe ser presentado al supervisor del contrato y aprobado por este al inicio de cada vigencia durante el plazo de ejecución del contrato.
- Deberá ejecutarse gradualmente de forma que se mantenga la compatibilidad y funcionalidad de los sistemas existentes.
- Deberá contemplarse mecanismos para regresar (rollback) a la versión anterior de forma que si las actualizaciones fallan se pueda reversar el procedimiento realizado y continuar con la operación normal de los equipos.
- En caso de que por razones de compatibilidad no se pueda realizar la migración o actualización de versiones de un sistema operativo, software, firmware o equipo, se deben implementar mecanismos de mitigación y salvaguardas para mantener la operación segura los sistemas de la Entidad.
- Para los equipos que no estén en red o que no se encuentren en el Directorio Activo por estar fuera de la red LAN, se deberá realizar actualizaciones mediante CD, DVD, Memorias USB o los medios que estime idóneos el Contratista.

10.2. HARDENING:

El CONTRATISTA debe realizar el hardening previo a la entrada en producción de los siguientes componentes:

- Sistemas operativos, tanto en los servidores como en las estaciones de los usuarios.
- Virtualizadores.
- Bases de datos.
- Software y servidores de aplicaciones.
- Sistemas en nube pública.
- Sistemas de enrutamiento y conmutación.
- Circuito Cerrado de Seguridad.

- El CONTRATISTA debe presentar las plantillas de hardening para cada sistema. Estas deben ser aprobadas por el supervisor del contrato.
- El CONTRATISTA debe realizar una revisión anual en todos los sistemas de las políticas de hardening implementadas y presentar un informe con las recomendaciones de mejora.

10.3. GESTION DE VULNERABILIDADES:

- El CONTRATISTA debe realizar la detección, gestión y solución de vulnerabilidades en los siguientes componentes:

- Sistemas operativos, tanto en los servidores como en las estaciones de los usuarios.
- Virtualizadores.
- Bases de datos.
- Software y servidores de aplicaciones.
- Sistemas en nube pública.
- Sistemas de enrutamiento y conmutación.
- Circuito Cerrado de Seguridad.

- El CONTRATISTA debe mitigar y solucionar las vulnerabilidades encontradas en la plataforma tecnológica.
- El CONTRATISTA deberá suministrar, a través de un tercero, el servicio de pentesting mínimo una (1) vez por año, durante el plazo de ejecución del contrato.
- El CONTRATISTA deberá presentar un informe con los resultados de las pruebas de pentesting, así como un Plan de Mejoramiento que contemple la solución o mitigación de las vulnerabilidades encontradas.

11. ACUERDOS DE NIVEL DE SERVICIO

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE INFRAESTRUCTURA DE SEGURIDAD**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.
MEDICIÓN:	Número de minutos en el que el servicio no está disponible
PENALIDAD	$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$ DISPONIBILIDAD EXIGIDA $\geq 99.98\ \%$
APLICA A:	Facturación de la línea de Seguridad en el componente INFRAESTRUCTURA DE SEGURIDAD

PENALIDAD POR NO CONFORMIDAD	DESCUENTO
$99.90\% \leq Disponibilidad < 99.98\%$	10%
$99.80\% \leq Disponibilidad < 99.90\%$	20%
$99.70\% \leq Disponibilidad < 99.80\%$	50%
$Disponibilidad < 99.70\%$	100%

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS PARA NETWORKING**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes.

<table>
<tr><td></td><td>Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</td></tr>
<tr><td>MEDICIÓN:</td><td>Número de minutos en el que el servicio no está disponible</td></tr>
<tr><td>PENALIDAD</td><td>$$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$$
DISPONIBILIDAD EXIGIDA $\geq$ 99.98 %
<table><tr><th>PENALIDAD POR NO CONFORMIDAD</th><th>DESCUENTO</th></tr><tr><td>$99.90\% \leq Disponibilidad < 99.98\%$</td><td>10%</td></tr><tr><td>$99.80\% \leq Disponibilidad < 99.90\%$</td><td>20%</td></tr><tr><td>$99.70\% \leq Disponibilidad < 99.80\%$</td><td>50%</td></tr><tr><td>$Disponibilidad < 99.70\%$</td><td>100%</td></tr></table></td></tr>
<tr><td>APLICA A:</td><td>Facturación de la línea de Seguridad en componente SERVICIOS PARA NETWORKING</td></tr>
</table>

<table>
<tr><td>NOMBRE ANS</td><td>DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS SOC</td></tr>
<tr><td>DEFINICIÓN:</td><td>La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes.
Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</td></tr>
<tr><td>MEDICIÓN:</td><td>Número de minutos en el que el servicio no está disponible</td></tr>
<tr><td>PENALIDAD</td><td>$$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$$
DISPONIBILIDAD EXIGIDA $\geq$ 99.98 %
<table><tr><th>PENALIDAD POR NO CONFORMIDAD</th><th>DESCUENTO</th></tr><tr><td>$99.90\% \leq Disponibilidad < 99.98\%$</td><td>10%</td></tr><tr><td>$99.80\% \leq Disponibilidad < 99.90\%$</td><td>20%</td></tr><tr><td>$99.70\% \leq Disponibilidad < 99.80\%$</td><td>50%</td></tr><tr><td>$Disponibilidad < 99.70\%$</td><td>100%</td></tr></table></td></tr>
<tr><td>APLICA A:</td><td>Facturación de la línea de Seguridad en componente SERVICIOS SOC</td></tr>
</table>

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS DE CERTIFICADOS**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del

	contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.
MEDICIÓN:	Número de minutos en el que el servicio no está disponible
PENALIDAD	$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$ DISPONIBILIDAD EXIGIDA $\geq 99.98\ \%$

PENALIDAD POR NO CONFORMIDAD	DESCUENTO
$99.90\% \leq Disponibilidad < 99.98\%$	10%
$99.80\% \leq Disponibilidad < 99.90\%$	20%
$99.70\% \leq Disponibilidad < 99.80\%$	50%
$Disponibilidad < 99.70\%$	100%

APLICA A:	Facturación de la línea de Seguridad en componente SERVICIOS DE CERTIFICADOS

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS ANTIMALWARE - ANTIVIRUS**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.
MEDICIÓN:	Número de minutos en el que el servicio no está disponible
PENALIDAD	$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$ DISPONIBILIDAD EXIGIDA $\geq 99.98\ \%$

PENALIDAD POR NO CONFORMIDAD	DESCUENTO
$99.90\% \leq Disponibilidad < 99.98\%$	10%
$99.80\% \leq Disponibilidad < 99.90\%$	20%
$99.70\% \leq Disponibilidad < 99.80\%$	50%
$Disponibilidad < 99.70\%$	100%

APLICA A:	Facturación de la línea de Seguridad en componente SERVICIOS ANTIMALWARE - ANTIVIRUS

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes. Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del

<table>
<tr><td></td><td>contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</td></tr>
<tr><td>MEDICIÓN:</td><td>Número de minutos en el que el servicio no está disponible</td></tr>
<tr><td>PENALIDAD</td><td>$$\left(1-\frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$$
DISPONIBILIDAD EXIGIDA $\geq$ 99.98 %
<table><tr><th>PENALIDAD POR NO CONFORMIDAD</th><th>DESCUENTO</th></tr><tr><td>$99.90\% \leq Disponibilidad < 99.98\%$</td><td>10%</td></tr><tr><td>$99.80\% \leq Disponibilidad < 99.90\%$</td><td>20%</td></tr><tr><td>$99.70\% \leq Disponibilidad < 99.80\%$</td><td>50%</td></tr><tr><td>$Disponibilidad < 99.70\%$</td><td>100%</td></tr></table></td></tr>
<tr><td>APLICA A:</td><td>Facturación de la línea de Seguridad en componente SERVICIOS PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)</td></tr>
</table>

<table>
<tr><td>NOMBRE ANS</td><td>DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS NAC (NETWORK ACCESS CONTROL)</td></tr>
<tr><td>DEFINICIÓN:</td><td>La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes.
Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</td></tr>
<tr><td>MEDICIÓN:</td><td>Número de minutos en el que el servicio no está disponible</td></tr>
<tr><td>PENALIDAD</td><td>$$\left(1-\frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$$
DISPONIBILIDAD EXIGIDA $\geq$ 99.98 %
<table><tr><th>PENALIDAD POR NO CONFORMIDAD</th><th>DESCUENTO</th></tr><tr><td>$99.90\% \leq Disponibilidad < 99.98\%$</td><td>10%</td></tr><tr><td>$99.80\% \leq Disponibilidad < 99.90\%$</td><td>20%</td></tr><tr><td>$99.70\% \leq Disponibilidad < 99.80\%$</td><td>50%</td></tr><tr><td>$Disponibilidad < 99.70\%$</td><td>100%</td></tr></table></td></tr>
<tr><td>APLICA A:</td><td>Facturación de la línea de Seguridad en componente SERVICIOS NAC (NETWORK ACCESS CONTROL)</td></tr>
</table>

NOMBRE ANS	**DISPONIBILIDAD SERVICIO DE SEGURIDAD EN COMPONENTE SERVICIOS SEGURIDAD WEB**
DEFINICIÓN:	La indisponibilidad es el número total de minutos, durante el mes contratado, en los que el servicio no está disponible o funcional en su totalidad, dividido en el número total de minutos en el mes contratado. La medición la hace el contratista monitoreando permanentemente el servicio durante el mes.

<table>
<tr><td></td><td>Los resultados del monitoreo son mantenidos por el contratista para que puedan ser consultados por ENTerritorio en cualquier momento durante el plazo de ejecución del contrato. La información mantenida por el contratista le debe permitir a ENTerritorio verificar la disponibilidad histórica del servicio en los meses anteriores y durante el mes en curso.</td></tr>
<tr><td>MEDICIÓN:</td><td>Número de minutos en el que el servicio no está disponible</td></tr>
<tr><td>PENALIDAD</td><td>$$\left(1 - \frac{\text{Número total de minutos en que el servicio no está disponible}}{\text{Número de días en el mes contratados x 24 horas x 60 minutos}}\right) \text{X } 100$$
DISPONIBILIDAD EXIGIDA $\geq$ 99.98 %
<table><tr><th>PENALIDAD POR NO CONFORMIDAD</th><th>DESCUENTO</th></tr><tr><td>$99.90\% \leq Disponibilidad < 99.98\%$</td><td>10%</td></tr><tr><td>$99.80\% \leq Disponibilidad < 99.90\%$</td><td>20%</td></tr><tr><td>$99.70\% \leq Disponibilidad < 99.80\%$</td><td>50%</td></tr><tr><td>$Disponibilidad < 99.70\%$</td><td>100%</td></tr></table></td></tr>
<tr><td>APLICA A:</td><td>Facturación de la línea de Seguridad en componente SERVICIOS SEGURIDAD WEB</td></tr>
</table>

<table>
<tr><td>NOMBRE ANS</td><td>IMPACTO OPERATIVO</td></tr>
<tr><td>DEFINICIÓN:</td><td>El contratista deberá prestar los servicios de ciberseguridad, SOC (Centro de Operaciones de Seguridad), realizando un seguimiento y análisis de la actividad de la red, servidores, nube publica, puntos finales, bases de datos, aplicaciones, sitios web y todos los componentes de la plataforma tecnológica, en horario 7x24, para evitar ataques que causen indisponibilidad en el servicio.
Al presentarse incidentes o eventos de seguridad que causen indisponibilidad o afectación en la operación de ENTerritorio, se realizará la penalización de la línea.</td></tr>
<tr><td>MEDICIÓN:</td><td>Impacto de los eventos o incidentes de seguridad que causan indisponibilidad, perdidas de información o afectación a la información de ENTerritorio:
<table><tr><th></th><th>Descripción</th></tr><tr><td>Insignificante</td><td>1) No genera reprocesos.
2) Impacto operacional no visible para la organización y sus involucrados.
3) Procesos críticos: hay interrupción de las operaciones menor o igual a 0,5 días hábiles (4 horas laborales).
Procesos no críticos: hay interrupción de las operaciones menor o igual a 2 días hábiles (16 horas laborables).</td></tr><tr><td>Menor</td><td>1) Genera reprocesos mínimos.
2) No se requiere de una intervención de otras áreas ni de la alta gerencia.
3) Procesos críticos: hay interrupción de las operaciones entre 0.5 y 1.5 días hábiles (>4 y <=12 horas laborables).
Procesos no críticos: hay interrupción de las operaciones entre 2 y 5 días hábiles (>16 y <= 40 horas laborables).</td></tr><tr><td>Moderado</td><td>1) Genera reprocesos que afectan una o varias actividades dentro de un mismo proceso.
2) Se requiere de la intervención de diferentes responsables de proceso o área de la posible utilización de recursos y asistencia externa.
3) Pérdida de información (propia o de clientes) que se puede recuperar fácilmente.
4) Procesos críticos: hay interrupción de las operaciones entre 1.5 y 4.5 días hábiles (>12 y <=36 horas laborables).
Procesos no críticos: hay interrupción de las operaciones entre 5 y 7.5 días hábiles (>40 y <= 60 horas laborables).</td></tr><tr><td>Mayor</td><td>1) Los reprocesos generados afectan a varios procesos.</td></tr></table></td></tr>
</table>

	Catastrófico	2) Intervención de las directivas de la compañía y movilización de recursos incluyendo asistencia externa. 3) Pérdida gran cantidad de información (propia o de clientes) que difícilmente se puede recuperar. 4) Procesos críticos: hay interrupción de las operaciones entre 4.5 y 7.5 días hábiles (>36 y <=60 horas laborables). Procesos no críticos: hay interrupción de las operaciones entre 7.5 y 20 días hábiles (>40 y <= 160 horas laborables).
		1) Los reprocesos afectan significativamente el desarrollo normal de la entidad 2) Intervención inmediata requerida por parte de la alta gerencia y Junta Directiva. 3) Pérdida gran cantidad de información (propia o de clientes) que no se puede recuperar 4) Procesos críticos: hay interrupción de las operaciones mayor a 7.5 días hábiles (>60 horas laborables). Procesos no críticos: hay interrupción de las operaciones mayor a 20 días hábiles (>160 horas laborables).
PENALIDAD	El incumplimiento de los Acuerdos de Niveles de Servicio (ANS), genera las siguientes penalidades para el contratista de acuerdo con su impacto:	
APLICA A:	Facturación de la línea de Seguridad	

PENALIDAD POR IMPACTO	DESCUENTO [% del valor mensual a facturar antes de IVA]
1 o más eventos o incidentes de seguridad insignificante	10%
1 o más eventos o incidentes de seguridad menor	20%
1 o más eventos o incidentes de seguridad moderado	50%
1 o más eventos o incidentes de seguridad mayor	70%
1 o más eventos o incidentes de seguridad catastrófico	100%

NOTA: La definición de eventos e incidentes de seguridad se toma en concordancia con los manuales y políticas de ENTerritorio y la norma ISO27035.

12. TRANSICION DE ENTRADA EN OPERACIÓN

El contratista deberá generar y presentar un plan de transición de entrada en operación para la implementación de los servicios y requerimientos de cada uno de los anexos y líneas de servicio; y deberá ejecutarlo en los tres (3) primeros meses del contrato, paralelo a la operación del operador actual.

13. TRANSICION, CIERRE Y ENTREGA

Cuatro (4) meses antes de la finalización del contrato el CONTRATISTA debe entregar al Supervisor del Contrato el plan de Transición. Este plan se debe ejecutar durante los tres (3) últimos meses de contrato.

Esta etapa se desarrolla en paralelo con la etapa de operación y no exime al Contratista de los descuentos por incumplimiento de ANS y del desarrollo normal de la operación.

Las actividades y entregables asociados a la transición del servicio son:

- Generar informes y BackUp de la configuración de las diferentes soluciones de seguridad.
- Desmontar agentes de monitoreo y seguridad.
- Entrega de la totalidad de credenciales de administración existentes y creadas al nuevo operador de los dispositivos de seguridad.
- Entrega de políticas, configuraciones y reglas de los dispositivos de seguridad.