ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON EL CONTRATO:

La ESAP ha desarrollado la implementación de un Sistema de Gestión de Seguridad de la Información SGSI basado en las mejores prácticas y estándares como ISO 27001:2013 y El componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea de Mintic. Dentro del proceso de mejora continua del SGSI la ESAP ha identificado la necesidad de contar con una herramienta de propósito específico que le permita realizar una gestión más eficiente de la seguridad de la información de la entidad y que este alineada con todos los aspectos de seguridad y privacidad de la información requeridos, y que incorpore todos los aspectos de la norma ISO 27001 de 2013. También se requiere un monitoreo y pruebas permanentes de seguridad de la infraestructura tecnológica que soporte los servicios más críticos de la entidad, para identificar vulnerabilidades, oportunidades de mejora y necesidad de actualizaciones de seguridad en sistemas operativos y aplicativos de negocio.

2. JUSTIFICACIÓN:

Dada la necesidad de llevar de forma organizada y mantener la trazabilidad de todo el proceso de SGSI en la entidad se requiere contar con una herramienta que permita manejar los componentes mas importantes de un Sistemas de Gestión de Seguridad en la Entidad. Con una plataforma que sea accesible desde cualquier regional de la ESAP y que cuente con las capacidades para que las directivas y el personal involucrado con la seguridad de la información pueda en todo momento poder validar e estado de la seguridad de la información en la entidad. Es por esto que se requiere una herramienta con presencia en el mercado nacional y deseablemente en entidades públicas realizando este tipo de gestión.

La ESAP también requiere los servicios especializados de pruebas de Vulnerabilidad y Ethical Hacking, dado que se requiere probar por personal externo a la entidad calificado el estado de seguridad en los sistemas y plataformas críticas de la entidad. Es por este que se requiere los servicios especializados de una empresa que suministre los PenTester necesarios para prestar este servicio. Personal especialista certificado en Certified Ethical Hacking y con conocimiento en los estándares y metodologías para este tipo de actividades como OWASSP.

3. DESCRIPCIÓN DEL OBJETO DEL CONTRATO O ESPECIFICACIONES:

3.1 OBJETO

Suministrar una herramienta de Software en Cloud u On Premise para el manejo del ciclo de vida del SGSI de la entidad. La herramienta debe ser WEB cono los niveles de seguridad, roles y módulos requeridos por las mejores prácticas de ISO 27001. También se requiere realizar dos (2) pruebas en

el año de Ethical Hacking a toda la infraestructura Crítica de la entidad, con personal certificado y amplia experiencia en este tipo de labores.

3.2 NIVEL DE CLASIFICADOR DE BIENES Y SERVICIOS

La codificación de bienes y servicios de acuerdo con el código estándar de productos y servicios de Naciones Unidas para la contratación que se pretende realizar es la siguiente:

Código UNSPSC 80101507 Producto: Servicios de asesoramiento sobre tecnologías de la información.

3.3 ESPECIFICACIONES TÉCNICAS

A. OBJETIVO GENERAL

Suministrar a la ESAP una herramienta para manejo del SGSI de la entidad y realizar las pruebas de vulnerabilidad y Ethical Hacking a la infraestructura critica de la entidad dos veces al año.

B. OBJETIVOS ESPECÍFICOS

1. Manejo integral, consistente y sólido bajo un esquema de mejoramiento continuo del SGSI.

2. Reducir el riesgo por vulnerabilidades en la infraestructura critica de la entidad.

3. Asegurar confianza del cliente.

C. REQUERIMIENTOS TÉCNICOS DEL PROYECTO

Conforme lo anterior, se deberán desarrollar de los siguientes aspectos:

1. El contratista debe suministrar una herramienta de Software, para la gestión del Sistema de Gestión de Seguridad de la Información (SGSI), debidamente licenciada como servicio u On premise (como mínimo por un año) y que cumpla y este alineada con la norma ISO/IEC 27001:2013. El software debe ser de uso específico para la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información con base en la norma ISO/IEC 27001:2013.

Características del software:

- Contar con un módulo específico para la gestión de los riesgos
- Permitir la gestión integral de la norma y cumplir con el ciclo completo de la misma, desde el inicio y planificación del SGSI hasta el mantenimiento y su mejora continua
- Gestionar los activos de información
- Determinar los controles a emplear para los riesgos de información
- Registrar e investigar los incidentes de seguridad de la información

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

- Determinar los procesos críticos
- Planear la recuperación y las pruebas
- Identificar los riesgos de los activos de información y hacer seguimiento a los planes de tratamiento.

El contratista debe capacitar en el manejo de la herramienta a mínimo cinco (5) funcionarios que la ESAP defina.

2. Análisis de vulnerabilidades – Pruebas de intrusión.

a) A través de un test de seguridad, realizar una evaluación y un diagnóstico tecnológico mediante el análisis de vulnerabilidades de los elementos que hagan parte de la plataforma tecnológica y de la explotación de estas vulnerabilidades con el fin de atacar la red, de manera controlada y sin causar daños a la misma (hacking ético), dentro del alcance definido en la presente ficha técnica.

b) Realizar estas pruebas tanto a nivel interno como externo, deben desarrollarse desde Internet y en la red interna, de tal manera que permita conocer hasta donde un ataque a los activos de la ESAP, puede ser efectivo y encontrar así los elementos a mejorar.

c) Efectuar de manera práctica e idónea la verificación y la efectividad de los controles establecidos y aplicados tanto a nivel interno como externo, sometiéndolos a pruebas con técnicas diseñadas para vulnerar su seguridad, y con el manejo de sofisticadas herramientas manejadas por un grupo de profesionales con amplia experiencia en su utilización y un alto sentido de la ética.

d) Realizar el análisis de vulnerabilidades y pruebas de intrusión desde una perspectiva interna y externa a los siguientes dispositivos relacionados con la operación:

i. Servidores

ii. Bases de Datos

iii. Servidores Web

iv. Aplicaciones

v. Firewalls

vi. vlans

e) Dentro de la metodología propuesta de test de intrusión incluir para el análisis de vulnerabilidades la utilización de las siguientes guías metodológicas:

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

- OWASP – OPEN WEB APPLICATION SECURITY PROJECT, Se seguirá la guía de OWASP top 10 para el test sobre las aplicaciones a evaluar que sugiere:

  A1. Inyección de Código

  A2. Cross Site Scripting

  A3. Autenticación y gestión Sesión

  A4. Ref. directa a objetos

  A5. Cross Site Request Forgery

  A6. Configuración insegura

  A7. Almac. Criptográfico inseguro

  A8. Fallos de restricción a URLs

  A9. Protección insuficiente de la capa de transporte

  A10. Redirecciones y reenvíos no validados.

- ITSAM–INFORMATION TECHNOLOGY SECURITY ASSESSMENT METHODOLOGY, Se seguirá la metodología de ISAM para el test interno que sugiere:

  I. Estudio de requerimientos y evaluación de la situación.

  II. Revisión de la documentación.

  III. Identificación de riesgos.

  IV. Análisis de Vulnerabilidades

  V. Análisis de Datos

  VI. Reportes.

- OSSTMM – OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL, Se seguirá la metodología de OSSTMM en las secciones que aplique a las presentes pruebas de intrusión tanto internas como externas que sugiere:

  Sección A -Seguridad de la Información

  A. Revisión de la Inteligencia Competitiva

  B. Revisión de Privacidad

  C. Recolección de Documentos

ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

Sección B – Seguridad de los Procesos

A. Testeo de Solicitud

B. Testeo de Sugerencia Dirigida

C. Testeo de las Personas Confiables

Sección C – Seguridad en las tecnologías de Internet

A. Logística y Controles

B. Exploración de Red

C. Identificación de los Servicios del Sistema

D. Búsqueda de Información Competitiva

E. Revisión de Privacidad

F. Obtención de Documentos

G. Búsqueda y Verificación de Vulnerabilidades

H. Testeo de Aplicaciones de Internet

I. Enrutamiento

J. Testeo de Sistemas Confiados

K. Testeo de Control de Acceso

L. Testeo de Sistema de Detección de Intrusos

M. Testeo de Medidas de Contingencia

N. Descifrado de Contraseñas

O. Testeo de Denegación de Servicios

P. Evaluación de Políticas de Seguridad

Sección D – Seguridad en las Comunicaciones

A. Testeo de PBX

B. Testeo del Correo de Voz

C. Revisión del FAX

D. Testeo del Modem

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

Sección E – Seguridad Inalámbrica

A. Verificación de Radiación Electromagnética (EMR)

B. Verificación de Redes Inalámbricas [802.11]

C. Verificación de Redes Bluetooth

D. Verificación de Dispositivos de Entrada Inalámbricos

E. Verificación de Dispositivos de Mano Inalámbricos

F. Verificación de Comunicaciones sin Cable

G. Verificación de Dispositivos de Vigilancia Inalámbricos

H. Verificación de Dispositivos de Transacción Inalámbricos

I. Verificación de RFID

J. Verificación de Sistemas Infrarrojos

K. Revisión de Privacidad

Sección F – Seguridad Física

A. Revisión de Perímetro

B. Revisión de monitoreo

C. Evaluación de Controles de Acceso

D. Revisión de Respuesta de Alarmas

E. Revisión de Ubicación

f) En el proceso de análisis de vulnerabilidades y pruebas de intrusión, realizar el levantamiento de información necesaria para la generación del test de intrusión tanto externo como interno. El nivel de información solicitado y el entregado por la ESAP relacionadas con la operación, será para realizar las pruebas en modo graybox (Caja Gris), se especificarían como mínimo las direcciones IP de los sistemas a los cuales se les quiere realizar el test.

g) Realizar la detección de vulnerabilidades (ver tabla 1) para identificar problemas con potenciales ataques entre otros. (Usando las metodologías OWASP, OSSTMM, ITSAM).

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

h) Determinar y documentar los objetivos específicos con mayor probabilidad de éxito durante el ataque o aumento en el grado de penetración para alcanzar cualquiera de las metas definidas.

i) Con los objetivos seleccionados y utilizando las vulnerabilidades descubiertas en la etapa del ataque, probar la existencia real de las vulnerabilidades y determinar el impacto de las mismas, además de determinar el surgimiento de nuevas vulnerabilidades no detectadas en las fases anteriores, las cuales serán incluidas en el análisis para su tratamiento.

j) Realizar un análisis, evaluación y documentación de resultados, con base en la información recolectada antes, durante y después de las pruebas.

k) Generar un informe detallado con los resultados obtenidos durante todo el proceso de ejecución de las pruebas, con el correspondiente análisis de dicha información para poder ser interpretada de manera correcta y entender las implicaciones a nivel de seguridad de la información sobre la infraestructura informática analizada, con las recomendaciones necesarias para solucionar dichos problemas.

l) Realizar un proceso de hardening a la plataforma de servidores (físicos y virtuales) y a los equipos activos (dispositivos de red), sede nivel central.

Cliente	• Debilidades de Autenticación • Cross Site script • Ataques Java	• Ataques al Browser • Keylogger • Usuarios y Grupos de usuarios
Red	• Comprobación de password y protocolos de ciframiento débiles. • Enumeración de la red, descubrir los todos los elementos posibles • Enumeración y Explotación de Wi-Fi • Enumeración y Explotación de BlueTooth	• Reconocimiento de la red • Sniffing • Ataques man-in-the- middle • Spoof de DNS • Reenrutamiento
Gateway	• IP-email-Spoof • Explotación de vulnerabilidades	• Filtering bypass • Sniffing
Sistemas operativos	• Identificación del sistema operativo del objetivo. Instalaciones por defecto de servicios y aplicativos. • Identificación de los puertos abiertos en los objetivos (TCP, UDP). • Negación de Servicios • Búsqueda de información sensible accesible por la red, como la existente en las carpetas compartidas.	• Identificación de los servicios que se están ejecutando en los objetivos. • Rompimiento de claves • Identificación de vulnerabilidades del SO.
Servidores Web	• Identificación del sistema operativo del objetivo Vulnerabilidades asociadas a malas prácticas de programación, puertas traseras instaladas. • Negación de Servicios	• Identificación de los servicios que se están ejecutando en los objetivos. • Explotación de vulnerabilidades • Búfer Overflow • Configuración por defecto
Aplicaciones	• Formas y manejo de sesiones • Directory Traversal - Inyección de código • Meta-caracteres • Session Hijacking	• Códigos de error y Manipulación de parámetros. • Búfer Overflow • Rompimiento de claves y autenticación.
Base de datos	• SQL Injection • Queries estructurados • Claves por defecto	• Claves fáciles • Autenticación de base de datos • Extracción de información confidencial

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

ANEXO TÉCNICO 5

FORTALECIMIENTO SGSI-ESAP

A. ENTREGABLES

Los documentos que el contratista deberá entregar a la ESAP, como resultado del desarrollo el proyecto son los siguientes:

1. Herramienta de gestión (software), instalada y en producción.
2. Documentación con informes detallados con el análisis evaluación de resultados, con base en la información recolectada antes, durante y después de las pruebas, con las recomendaciones necesarias para la solución de Dichos problemas.
3. Documento Word y PDF