MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO	Coljuegos	FORMATO SOLICITUD DE ESTUDIO DE MERCADO	TRD: 100-500-10-4-485 Vigencia:19-08-2022 Versión: 12 Página: __ de __

I. DATOS GENERALES DE LA SOLICITUD:

Radicado No.	Al contestar por favor cite: Radicado No.: 20231300033843 Fecha: 2023-02-28 08:09		
Plazo Estimado del contrato/orden de compra:	5 meses	**Fecha Esperada de inicio (dd/mm/aaa):**	20/3/2023
Gerencia, Oficina o Vicepresidencia Responsable	Oficina de Tecnologia de la Información		
Lugar de Ejecución:	COLJUEGOS	**Supervisor Propuesto:**	Juan Sebastian Chaparro saenz

II. OBJETO DEL CONTRATO:

2.1 Descripción: (objeto en el PAA)
CONTRATAR UNA EMPRESA ESPECIALIZADA QUE BRINDE SERVICIOS INTEGRALES DE CIBERSEGURIDAD

III. FICHA TÉCNICA :

3.1 Información técnica :

Contratar los servicios especializados de consultoría para el fortalecimiento de la ciberseguridad de Coljuegos que permitirán desarrollar el diagnóstico, análisis vulnerabilidades y riesgos de seguridad mediante la ejecución de pruebas técnicas y de ingeniería social para la identificación de las debilidades y así mismo la entrega de un plan de recomendaciones para la subsanación de los hallazgos.
Para lo anterior, se requiere contratar una empresa consultora para cubrir la necesidad de mejora en el componente de Cyberseguridad del proceso TIC de la entidad.
Como primer aspecto en tener en cuenta es el volumen de dispositivos electrónicos distribuidos entre dos (2) centros de datos:
Centro de datos Externo: 22 servidores
Centro de datos Local: 40 Servidores, 22 dispositivos de red
Numero de sistemas de Informacion: 10
Alcance
1. Diagnosticar el estado actual del sistema de gestión de seguridad, para los activos de la organización que están relacionados con la ciberseguridad. Realizar levantamiento y valoración de activos de información, análisis de vulnerabilidades e identificación de recomendaciones de ajustes o complemento a los riesgos de seguridad de la información a nivel interno y externo de Coljuegos
2. En la identificación de las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad se deberán ejecutar pruebas de vulnerabilidad y de Pentesting en servidores, equipos de cómputo, elementos activos de red, sistemas de información. Las pruebas de vulnerabilidad deben ser planeadas y coordinadas con la entidad y autorizadas por éste para ser ejecutadas.
3. El proveedor deberá identificar y valorar la criticidad de los activos sugeridos y acordados con la Entidad.
4. Realizar una prueba de ingeniería social por lo menos para un mínimo de 3 integrantes de cada área basado en el organigrama de la Entidad (17 áreas).
5. Las pruebas de penetración avanzada deberán ejecutar análisis y explotación manual sin limitar los resultados en los hallazgos de herramientas de escaneo y sin afectar la operatividad de los sistemas de Coluegos.

3.2 funcional: Coljuegos como entidad responsable de manejo de información y datos sensibles, debe garantizar la seguridad e integridad de la información que se almacena y recibe por medio de la infraestructura tecnologica de la entidad, por tal motivo se hace necesario realizar un diagnostico del estado actual de la infraestructura (Dispositivos) que hacen parte del componente de Ciberseguridad de los procesos TIC de la entidad; debido a que hacen parte fundamental de la seguridad de la información. Para esto se hace necesario el desarrollo de una serie de actividades que permitan identificar las vulnerabilidades, riesgos de seguridad, ingeniería social para la identificación de debilidades, informe final de de recomendaciones con el cual se pueda establecer un plan de remediación que permita la implementación de los correctivos y mejoras para el componente de Ciberseguridad de la entidad. Acercandose asi a un modelo de seguridad que pueda contribuir a un nivel de madurez en la transparencia de la gestión pública y mejores practicas de seguridad, en busqueda de la futura implementación de la ISO 27001.

3.3 Compra presupuestada en PAA inicial:	Si: X	No	Valor:	$	300.000.000

Nota: Si es "SI" numero de linea en el Plan de Egresos. Si es NO numero de acta y fecha de comité de contratacin que autoriza esta contratación.	118

IV. DEFINICIÓN DE LA NECESIDAD:

4.1 Perfil del proveedor : Se solicita que el proveedor cuente con minimo 5 años de experiencia en el desarrollo de proyectos de seguridad de la información similares al objeto de este contrato, el equipo de consultor debe contar con minimo 3 profesionales en ingenieria con Maestria o Especialización en Seguridad de la Información, que en el equipo de consultores se cuente con personal certificado (Se exigira minimo 5 cerificaciones vigentes) en :
-ISO27001:2013
-CISM
-COBIT
-CISA
-CHFI
-CISSP

4.2 Cantidad solicitada: El contratista debera abordar el objeto del contrato teniendo en cuenta lo siguiente:
Centro de datos Externo: 22 servidores
Centro de datos Local: 40 Servidores, 22 dispositivos de red
Numero de sistemas de informacion: 10
Alcance
1. Diagnosticar el estado actual del sistema de gestión de seguridad, para los activos de la organización que están relacionados con la ciberseguridad. Realizar levantamiento y valoración de activos de información, análisis de vulnerabilidades e identificación de recomendaciones de ajustes o complemento a los riesgos de seguridad de la información a nivel interno y externo de Coljuegos
2. En la identificación de las amenazas y vulnerabilidades a las que se encuentra expuesta la Entidad se deberán ejecutar pruebas de vulnerabilidad y de Pentesting en servidores, equipos de cómputo, elementos activos de red, sistemas de información. Las pruebas de vulnerabilidad deben ser planeadas y coordinadas con la entidad y autorizadas por éste para ser ejecutadas.
3. El proveedor deberá identificar y valorar la criticidad de los activos sugeridos y acordados con la Entidad.
4. Realizar una prueba de ingeniería social por lo menos para un mínimo de 3 integrantes de cada área basado en el organigrama de la Entidad (17 áreas).
5. Las pruebas de penetración avanzada deberán ejecutar análisis y explotación manual sin limitar los resultados en los hallazgos de herramientas de escaneo y sin afectar la operatividad de los sistemas de Coluegos.

V. RESULTADOS ESPERADOS:

5.1 Resultados

Como resultado de la consultoría realizada se deben entregar los siguientes productos:
1. Entrega del plan de gestión del proyecto, metodología de Ethical Hacking y cronograma de ejecución.
2. Informe de resultados del análisis, evaluación y diagnóstico de la situación actual e Identificación de brechas para cada dominio de ISO/IEC 27001.
3. Informe Ejecutivo y técnico de Resultados de vulnerabilidades y de todas aquellas acciones y resultados del Ethical Hacking, el cual debe contener:
• Nombre del servidor
• Dirección IP
• Nombre del sistema de información.
• Información básica del sistema
• Definición de la línea base de seguridad del sistema de información que incluya: fecha, servidor, sistema operativo, base de datos (donde aplique), servicios web (donde aplique), aplicación, versiones de los componentes, Nivel de exposición del servidor, vulnerabilidades altas, medias, bajas.
• Grado de vulnerabilidad del sistema de información
• Vulnerabilidades criticas
• Vulnerabilidades altas
• Vulnerabilidades medias
• Recomendaciones del experto de seguridad de la información.
4. Instructivo de clasificación y etiquetado de activos de información.
5. Documento que contenga la metodología utilizada, resumen de actividades, principales hallazgos, conclusiones y recomendaciones.
6. Informe de los resultados de pruebas presenciales y no presenciales que contengan como mínimo:
• Explicación de la metodología empleada por las diferentes técnicas
• Resultado de ejecución de las pruebas
• Evidencias fotográficas en caso que aplique
• Vulnerabilidades encontradas y riesgos encontrados a partir de las mismas
• Documento plan de acción para la mitigación de los riesgos encontrados
7. Informe de los resultados de las pruebas de Fake Mailing
8. Gestión de riesgos de seguridad de la información:
• Documento con la metodología de la gestión de riesgos.
• Matriz de valoración riesgos de seguridad de la información
• Documento con el plan de tratamiento de riesgos
9. Elaborar un plan de remediación conforme a los resultados de las actividades
Documento de recomendaciones basado en los resultados.
10. Procedimiento para la gestión de vulnerabilidades técnicas donde se indique la metodología, tipos de pruebas, frecuencia de los escaneos a la infraestructura tecnológica de la entidad para mantener esta ejecución en el tiempo.

VI. OBLIGACIONES DEL CONTRATISTA:

6.1 Responsabilidades (Obligaciones Especificas):

Acciones para el Ethical Hacking

1. Realizar el análisis de vulnerabilidades para determinar los los riesgos existentes de los servicios a nivel interno y externo sin privilegios o con privilegios mínimos, aplicando como metodología base el marco de referencia OSSTMM (Open Source Security Testing Methodology Manual) y la OSCP (Offensive Security Certified Professional).
2. Testear los sistemas operativos, su configuración, puertos activos y servicios propios del sistema.
3. Evaluar la configuración de los equipos de seguridad tales como Firewall y WAF de los dos centros de datos, entre otros: lista de acceso, análisis de los puertos y los servicios abiertos. Para ello y como parte del proceso para la identificación de riesgos, se deberá analizar el tráfico y eventos del firewall y WAF dispuesto para la operación de los sistemas de información de Coljuegos. El contratista deberá determinar la existencia de comportamientos anómalos y tráfico hacia la red interna mediante la lectura, interpretación, correlación, análisis de los eventos registrados en los equipos de seguridad.
4. Realizar prueba de intrusión en la red de área local (LAN) tanto alámbrica como inalámbrica y con base en esta determinar el estado actual de la infraestructura tecnológica.
5. Realizar pruebas de Hacking Ético: Buffer-Overflows, descubrimiento de contraseñas a la fuerza, cracking de contraseñas sobre cuentas privilegiadas de Base de Datos, secuestro de sesiones, errores en aplicaciones o configuraciones débiles.
6. Realizar prueba de penetración en la IPs públicas, definidos en el alcance con el fin de determinar el estado actual de la infraestructura tecnológica y la seguridad de su interconexión.
7. Realizar análisis de vulnerabilidades en los hosts de la entidad y así mismo realizar re-test de las pruebas de vulnerabilidad.
8. Garantizar la integridad de los resultados generados durante la ejecución de las pruebas de vulnerabilidad.
9. Realizar un escaneo para las direcciones IPs y aplicaciones que hacen parte de la infraestructura externa e interna, e identificar las vulnerabilidades que afecten la información.
10. Ejecutar un análisis de vulnerabilidades hasta un máximo de 10 direcciones IPS externas de Coljuegos.
11. Ejecutar un análisis dinámico de aplicación sobre al menos 5 sitios públicos de la Entidad.
12. Elaborar y sustentar un informe de resultado que contenga los hallazgos tras el análisis de vulnerabilidad en la cual se puedan identificar los puntos críticos que deberán ser priorizados.
13. Elaborar plan de recomendaciones, que apoyará la priorización de los hallazgos.

Pruebas a desarrollar para el Ethical Hacking

1. Pruebas no presenciales

Las pruebas no presenciales estarán orientadas a ejecutar mecanismos que permitan explorar en internet, redes sociales, correo electrónico o página web cualquier información que vincule a la Entidad con el propósito de establecer si es posible encontrar datos confidenciales como lo son claves, nombres de servidores, direcciones ips, dominios, software, datos personales, entre otros, que puedan ser aprovechadas por terceros generando exposición a riesgos de seguridad de la información. El contratista deberá ejecutar técnicas como googlehacking, búsqueda de metadatos, búsqueda publicaciones en los portales de la Entidad o las que el contratista proponga.

2. Fake Mailing - phising

El contratista debe realizar el envío de correos electrónicos haciendo uso de la técnica mail relay, a través de un servidor de correo que lo permita a cuentas de correo de la entidad, previamente definidos por la entidad, para lograr los siguientes objetivos:

- Intentar obtener información privilegiada
- Intentar obtener nombres de usuarios y/o contraseñas
- Intentar que el usuario responda y/o reenvíe el correo

El contratista deberá realizar el intento o materialización de un ataque de phishing por medio del correo electrónico con el cual se intente que los receptores del mensaje ingresen a un link y accedan a una página web con las mismas características de algún servicio web provisto por la entidad.

3. Sesión o estrategia de concientización a usuarios

El contratista deberá realizar un máximo de 3 sesiones de concientización por concepto de seguridad de la información a los usuarios.

4. Remediación y Aseguramiento

Ejecutar la remediación de vulnerabilidades y aseguramiento sobre los servidores que soportan los 10 sistemas de información críticos para la Entidad, para la mitigación de los riesgos de seguridad resultantes del análisis de vulnerabilidades.

VII. COTIZACIONES RECIBIDAS:

7.1 Anexe Cotizaciones (Aréa usuaria):

A continuacion se anexa cotizacion de proveedor "Password Consulting" y se relacionan contactos de proveedores adicionales para su respectivo estudio; sin embargo el area de contratacion esta en libertad de extender la invitacion a otros proveedores o posibles candidatos interesados en el proceso.

MSL	cbejarano@msl-latam.com cbejarano@msl.com.co jpatino@msl-latam.com
ECOMIL	jrodriguez@ecomil.co jhincapie@ecomil.co
SOSNET	comercial@sos.net.co
Passwrod Consulting	comercial@sos.net.co

VIII. SOLICITUD Y RECEPCIÓN

SOLICITÒ

Firma:

Nombre: EDGAR EDUARDO ROMERO BOHORQUEZ

Jefe Oficina de Tecnologia de la Información

Correo Electronico:	eromero@coljuegos.gov.co	Extensión	201
Fecha:	2802/2023		
Elaboró: (Nombre y Cargo)	Stephany Grey Suarez Galván - Profesional 1 / Juan Sebastian Chaparro - Profesional especializado 1		
Revisó: (Nombre y Cargo)	Stephany Grey Suarez Galván - Profesional 1 / Juan Sebastian Chaparro - Profesional especializado 1 / Edgar Eduardo Romero Bohorquez - Jefe Oficina		
Folios:			2
Anexo:			Cotizacion de password, ecomil y sosnet, formato cotizacion en orfeo
Número de expediente:			Contrato nuevo