

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

1. OBJETO

DTC85 Contratar la prestación de servicios de una empresa especializada, para la realización de un test de intrusión (Ethical Hacking). para TRANSMILENIO S.A. en los segmentos que el Ente Gestor determine.

1.1. Alcance del Objeto

Estructurar e implementar el esquema de actividades pertinentes para llevar a cabo un test de intrusión ética (Ethical Hacking) e Ingeniería Social, que permita evaluar el estado actual de seguridad perimetral de la red interna y el nivel de concientización de los funcionarios respecto al manejo de seguridad de la información, plasmando en un informe detallado, los posibles planes de acción y recomendaciones en materia de seguridad, que le posibiliten a TRANSMILENIO S.A., implementar los controles adecuados para eliminar las vulnerabilidades encontradas.

Realizar Ethical Hacking para 400 direcciones IP internas, 5 externas y 5 aplicaciones informáticas que la entidad indicará a través del supervisor.

Desarrollar pruebas de ingeniería social a mínimo 30 funcionarios de la entidad para determinar a través del supervisor en grado de apropiación y generación de la cultura en lo que a seguridad informática se refiere.

Realizar pruebas de ingeniería social de manera presenciales en las instalaciones de TRANSMILENIO S.A., en máximo dos (2) sesiones, en la fecha y hora que el ente gestor determine, garantizando cobertura a funcionarios de planta y contratistas, incluyendo directivos de todas las áreas de la Entidad.

Las pruebas a ejecutar deben validar: Seguridad física, seguridad de los equipos, y prácticas de los usuarios internos con respecto a la disposición y tratamiento de la información y en lineamiento de las políticas de seguridad de la información soportadas en el estándar ISO/IEC 27001: 2013 y/o ISO/IEC 27001: 2022.

1.2. Clasificación UNSPC

Segmento	Familia	Clase	PROD	Producto
81	11	20	00	Servicio de datos
80	10	15	00	Servicios de Consultoría de negocios y administración Corporativa.
81	11	18	00	Servicios de sistemas y administración de componentes de sistemas.
81	11	22	00	Mantenimiento y soporte de software

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

2. PLAZO DE EJECUCIÓN

Dos (2) meses, contados a partir de la suscripción del acta de inicio.

3. DEFINICIONES

Adware: Software que se apoya en anuncios como parte del propio programa. La publicidad generada es mostrada después de la instalación de dicho programa.

Amenaza: Circunstancia que tiene el potencial de causar daños o pérdidas puede ser en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DOS).

Antispam: Aplicación o herramienta informática que se encarga de detectar y eliminar correo no deseado.

Antivirus: Software utilizado para eliminar programas elaborados con intención destructiva.

Aplicación engañosa: Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.

Autenticación básica: Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

Ataque Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Ataque Dirigido: Son aquellos ataques realizados normalmente de manera silenciosa e imperceptible, cuyo objetivo es una persona, empresa o grupos de ambas.

Armouring: Es una técnica que utilizan los virus para esconderse e impedir ser detectados por los antivirus.

Blacklist (Lista negra): Es un proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Bots (Red): Son grupos de ordenadores infectados controlados de forma remota por un hacker.

Buffer Overflow: El desbordamiento de búfer es un error o vulnerabilidad de codificación de software que los piratas informáticos pueden aprovechar para obtener acceso no autorizado a los sistemas corporativos.

Bulo: Mensaje de correo electrónico con contenido falso o engañoso, pero con contenido de alto impacto.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Permiten hacerse con el control de los ordenadores ajenos sin permiso de los usuarios. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente.

Carga destructiva: Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Cracker: Personas que rompen algún sistema de seguridad, (Fines de lucro, protesta o desafío).

Crimeware: Software malicioso como los virus, troyanos, spyware y más.

Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

Cibercrimen: Actos delincuenciales en el ciberespacio donde el principal objetivo es cometer ilícitos contra individuos, organizaciones y empresas.

Ciberdelito: Operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Cifrado: Proceso de codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

Control de acceso a la red (Nac): Su principal objetivo es asegurar que todos los dispositivos que sean conectados a las redes corporativas cumplan con las políticas de seguridad establecidas para evitar amenazas.

Correo no deseado: Cualquier comunicación que nos llega por cualquier medio no habiendo sido solicitada y que no era esperada por el usuario que la recibe.

Cookie: Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

Cross Site Script (XSS): Los ataques de secuencias de comandos entre sitios (XSS) son un tipo de vulnerabilidad de seguridad que se puede encontrar en algunas aplicaciones web. Los ataques XSS permiten a los atacantes inyectar secuencias de comandos del lado del cliente en páginas web vistas por otros usuarios.

CVE/MITRE: Common Vulnerabilities and Exposures (CVE) es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente. CVE fue lanzada en 1999 por la corporación MITRE para identificar y categorizar vulnerabilidades en software y firmware.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Definición de virus: Procedimiento por medio del cual el antivirus actualiza su base de datos de definiciones de virus. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Desbordamiento de búfer: Se producen cuando un programa sobrescribe otras partes de la memoria del equipo para almacenar más datos de los permitidos, provocando errores o bloqueos.

Driver: Es un programa, conocido como controlador, que permite la gestión de los dispositivos conectados al ordenador (generalmente, periféricos como impresoras, unidades de CD-ROM, etc).

Dropper: Es un fichero ejecutable que contiene varios tipos de virus en su interior.

Economía Clandestina: La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Ethical hacking: También conocido como hacking ético es la práctica de realizar evaluaciones de seguridad utilizando las mismas técnicas que emplean los hackers, pero con la debida aprobación y autorización de la organización a la que se está hackeando.

Exploit: Un error en el software que representa una brecha de seguridad.

Extorsión: El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.

Extensión: Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: NOMBRE.EXTENSIÓN.

Filtración de datos: Divulgaciones que no están autorizadas que tratan de adquirir información confidencial y que pueden dar lugar a robos o fugas.

Firewall: Un componente de hardware o software diseñado para bloquear el acceso no autorizado.

Firma de Antivirus: Las bases de firmas de un antivirus son el conjunto de cadenas que posee para detectar distintos códigos maliciosos. Sus actualizaciones se producen cuando el producto descarga nuevas firmas, que son incorporadas a su base para así poder detectar más amenazas.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Reeware: Salida no controlada de información que hace que esta llegue a personas no autorizadas.

Freeware: Es todo aquel software, legalmente distribuido, de forma gratuita.

GAP: Un análisis de brechas GAP es un método para evaluar las diferencias de rendimiento entre los sistemas de información de una empresa o las aplicaciones de software para determinar si se cumplen los requisitos del negocio y, de no ser así, qué pasos se deben tomar para garantizar que se cumplan con éxito.

Gateway: Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

Greylisting o Lista Gris: Una lista gris o greylist es una técnica para el control de mensajes spam. Es un método de defensa que bloquea la mayoría del spam que se recibe en un servidor de correo.

Gusanos: Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

Hacker: Persona experta en tecnología dedicada a intervenir y /o realizar alteraciones técnicas con buenas o malas intenciones.

Hacking: Acceder de forma ilegal a datos almacenados en un ordenador o servidor.

Hacktivismo: Es la función del Hacking y el activismo, la política y la tecnología.

Hardware: Término que hace referencia a cada uno de los elementos físicos de un sistema informático (pantalla, teclado, ratón, memoria, disco duro, otros)

HTTP (HyperText Transfer Protocol): Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

Ingeniería Social: Término que hace referencia al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo.

Incidente Informático: Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

Inyección de código SQL: Técnica donde el atacante crea o altera comandos SQL, para exponer datos ocultos, sobrescribir los valiosos, o ejecutar comandos peligrosos en un equipo que hospeda bases de datos.

Índice de peligrosidad: Es un valor calculado que permite medir lo peligroso que puede llegar a ser un virus.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Infección: Es la acción que realizan los virus virus, consistente en introducirse en el ordenador o en áreas concretas de éste y en determinados ficheros.

IP (Internet Protocol) / TCP-IP: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes.

Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Lista Blanca: Método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad.

Malware: Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

Mecanismo de Propagación: Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema.

Mutex: Técnica utilizada por algunos virus para controlar el acceso a recursos (programas u otros virus) y evitar que más de un proceso utilice el mismo recurso al mismo tiempo.

Negación de servicio (DoS): Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Nivel de Propagación: Se trata de un valor que indica cómo de rápido se puede extender o se ha extendido el virus por todo el mundo. Es usado para mirar la peligrosidad del mismo.

Nuke (ataque): Caída o pérdida de la conexión de red, provocada de forma intencionada por alguna persona. El ordenador sobre el que se realiza un nuke, además puede quedar bloqueado.

Parches: Programa que se encarga de hacer cambios en busca de la corrección de vulnerabilidades de seguridad.

Pharming: Redirigir el tráfico a un sitio web falso para capturar información confidencial de los usuarios.

Phishing: Técnica utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

Piratería: Infringir los derechos de autor para obtener ganancias financieras o distribuir sin permiso un trabajo que se está preparado para su distribución comercial.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Programa malicioso: También conocidos como malware que contienen virus, spyware y otros programas indeseados que se instalan sin consentimiento.

Protección Heurística: En el contexto de la protección antivirus, la heurística se compone de un conjunto de reglas que se emplean para detectar el comportamiento de los programas maliciosos sin necesidad de identificar de forma exclusiva a la amenaza específica, como es requerida por la detección clásica basada en firmas.

Ransomware: Programa maligno que bloquea totalmente nuestro equipo y pide dinero a cambio de devolver el control.

Retest: El proceso de RETEST consiste en volver a verificar las vulnerabilidades o debilidades que fueron detectadas inicialmente, esto permite certificar la correcta mitigación y de esta forma disminuir el riesgo. El RETEST es una actividad independiente del tipo de análisis.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque.

Robo de datos: Los robos de datos pueden producirse tanto dentro de la empresa (por ejemplo, a manos de un trabajador descontento) como mediante ataques de delincuentes desde el exterior.

Rootkits: Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red.

Scareware: Hacer creer a los usuarios que el equipo está infectado, para hacer comprar una aplicación falsa.

Session hijacking: El ataque de secuestro de sesión consiste en la explotación del mecanismo de control de sesión web, que normalmente se gestiona mediante un token de sesión.

Sistema de detección de intrusos (IDS): Hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Sistema de prevención de intrusiones (IPS): Encargados de detectar y bloquear cualquier intento de intrusión, transmisión de código maliciosos, o amenazas a través de la red.

Sniffing: El sniffing es un tipo de ciberataque utilizado para poder escuchar todo lo que sucede dentro de una red, sobre todo en redes internas, las conocidas como intranet.

Software de seguridad fraudulento (rogue): Falsos programas de seguridad que no son realmente lo que dicen ser, sino que, todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios.

Spear phishing: Estafa por correo electrónico cuyo objetivo es acceso no autorizado a datos, se centra en organizaciones en busca de: robo de propiedad intelectual, datos financieros, secretos comerciales, otros.

Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas sin permiso de los usuarios.

SQL injection: Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos. Clasificación de los ataques Web por Inyección SQL.

Toolkit: Son programas de software que pueden usarse tanto por novatos como por expertos para facilitar el lanzamiento y distribución de ataques a computadoras en red.

Tracware: Es todo programa que realiza el seguimiento de las acciones que realiza el usuario mientras navega por Internet (páginas visitadas, banners que pulsa, etc.) y crea un perfil que utiliza con fines publicitarios.

UDP (User Datagram Protocol): es un protocolo de comunicación que se utiliza en Internet para transmisiones sujetas a limitaciones temporales, como la reproducción de vídeo o las búsquedas en DNS.

Variante: Es una versión modificada de un virus original, que puede infectar de forma similar o distinta y realizar las mismas acciones u otras.

Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

Virus: Programa de ordenador capaz de incrustarse en disco y replicarse repetidamente, sin el conocimiento o permiso del usuario.

Vulnerabilidad: Debilidad del sistema informática que puede ser utilizada para causar algún tipo de daño.

Zombie: Ordenadores infectados controlados de forma remota por los ciberdelincuentes.

4. CARACTERÍSTICAS Y CONDICIONES TÉCNICAS

El estudio requerido por la entidad, deben cumplir con las siguientes especificaciones:

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

4.1 Fases Actividades

4.1.1 Planeación

- Levantamiento de información preliminar:
- Entendimiento de los procesos y actividades de la entidad que soporte el proceso de TI, el GAP solo se hará sobre el proceso de TI.
- Conocimiento de la distribución de áreas y procesos de la entidad desde la perspectiva funcional y jerárquica.

4.2 Pruebas de vulnerabilidades

- ✓ Realización de pruebas de vulnerabilidad para un total de 400 direcciones IP privadas.
- ✓ Las pruebas deben ser realizadas con una herramienta en software y/o hardware licenciado por el proveedor y certificado CVE/MITRE.
- ✓ Se incluyen en las pruebas cinco (5) direcciones IP públicas y cinco (5) aplicaciones informáticas utilizadas por la entidad.
- ✓ Se debe llevar a cabo como mínimo un RETEST para hacer seguimiento de la disminución del riesgo.
- ✓ El RETEST se debe llevar a cabo máximo en 2 meses después de la entrega de los informes técnicos. Dicha prueba deberá ser soportada por carta de compromiso del contratista.
- ✓ Se deben incluir los informes técnicos de las herramientas, así como un informe ejecutivo.

Se deberán llevar a cabo como MÍNIMO las siguientes pruebas de vulnerabilidad:

- Debilidades de Autenticación.
- Cross site script.
- Ataques a las aplicaciones.
- Ataques al browser.
- Identificación del sistema Operativo.
- Identificación de instalaciones por defecto de servicios y aplicativos
- Identificación de puertos abiertos TCP y UDP.
- Identificación de los servicios en ejecución.
- Rompimiento de claves.
- Identificación de vulnerabilidades del SO.
- Negación de servicios.
- Búsqueda de información sensible accesible por la red.
- Sniffing.
- Buffer overflow.
- Directory Traversal.
- Session hijacking

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

- Mensajes y códigos de error incontrolados.
- SQL injection.
- Claves por defecto y claves fáciles.
- Intentos de autenticación a la base de datos.
- Extracción de información confidencial.

4.3 Soporte:

El contratista deberá prestar los servicios de Ethical Hacking en complemento con las pruebas de Ingeniería Social en las condiciones estipuladas en el presente estudio técnico y económico, sin que TRANSMILENIO S.A. incurra en costos adicionales diferentes a los incluidos en la propuesta económica. Se deben contemplar los siguientes puntos:

- ✓ El contratista deberá garantizar la integridad de la infraestructura computacional que ha de ser intervenida durante la ejecución del objeto contractual, así como la integridad, confidencialidad y disponibilidad de la información almacenada y circulante por dicha infraestructura.
- ✓ El contratista deberá hacer entrega semanalmente de los reportes estadísticos de incidentes de seguridad ocurridos y detectados durante el periodo de ejecución del objeto contractual al interventor del contrato.
- ✓ El contratista deberá disponer de los mecanismos de soporte que permitan registrar las solicitudes de los mismos, y hacerles seguimiento a los tickets generados durante la vigencia del contrato (help desk).
- ✓ Para dar inicio al contrato, se deberán acordar en conjunto con TRANSMILENIO S.A., los tiempos de atención y solución de las fallas o solicitudes de soporte que se puedan presentar, y los procedimientos para la mesa de ayuda, y entregarlos documentados al supervisor del contrato.

4.4 Entregables del Servicio:

La empresa que brindará el servicio deberá entregar el respectivo Plan de Proyecto (Marco PMI) donde se explicará detalladamente la metodología que se utilizará para el desarrollo del servicio debiendo contar el mismo con los siguientes requisitos mínimos:

- ✓ Fase de Planeamiento (Objetivos, áreas de trabajo involucradas, fechas tentativas de realización de pruebas y/o testeos, servicios a ser incluidos, técnicas y software a utilizarse, etc.)
- ✓ Fase de Levantamiento de información.
- ✓ Fase de Preparación de pruebas.
- ✓ Fase de Ejecución de pruebas.
- ✓ Fase de Documentación de resultados obtenidos.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

- ✓ El oferente que resulte favorecido con la adjudicación del contrato deberá presentar el respectivo Plan del proyecto, como requisito para suscribir el acta de inicio.

La empresa que brindará el servicio, al término del ejercicio deberá presentar un informe que deberá incluir:

- ✓ Informe ejecutivo que muestre las vulnerabilidades y amenazas y las recomendaciones de mejora, desde un enfoque general. El informe no deberá estar basado únicamente en lo reportado por las herramientas utilizadas, sino que deberá ser el resultado de un análisis detallado y personalizado de la plataforma informática con que cuenta TRANSMILENIO S.A.
- ✓ Matriz de riesgo basado en el informe de situación actual.
- ✓ Plan de acción preventiva y correctiva.
- ✓ Plan de aplicación inmediata de prevención y corrección.
- ✓ Información y material obtenido durante el servicio.
- ✓ Propuesta de políticas, normas, estándares, procesos y acuerdos organizacionales.
- ✓ Informe técnico que detalle todas las pruebas realizadas especificando su objetivo, las prevenciones, los resultados obtenidos, correcciones efectuadas.
- ✓ Resultado pruebas de ingeniería social.
- ✓ Charla de sensibilización.
- ✓ Recomendaciones de Mejores Prácticas.

Número de dispositivos que componen la infraestructura de Networking de TRANSMILENIO S.A.

DISPOSITIVO	CANTIDAD
Switches de core en HA	3
Switches de distribución (48 puertos)	32
Firewalls en HA	2
Endpoints	600
Access Point	28
Balanceadores	2

5. LUGAR DE EJECUCIÓN

La ejecución del contrato será en la Sede administrativa de TRANSMILENIO S.A., Avenida El Dorado 69-76 Torre 1 piso 6 Dirección de TIC.

6. FORMA DE PAGO

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

El valor del contrato será pagado de conformidad con lo siguiente:

1. Primer pago correspondiente al 50% del valor total del contrato, una vez se hayan realizado las pruebas de Ethical hacking de acuerdo con lo descrito en el anexo técnico, previa validación del informe de actividades y resultados por parte del supervisor del contrato.
2. Segundo pago correspondiente al 50% restante, una vez se haya entregado por parte del contratista el informe consolidado de análisis de vulnerabilidades, generación de los planes de acción correspondientes a las vulnerabilidades identificadas, así como la realización de las sesiones de sensibilización y la ejecución de la totalidad de las actividades contractuales establecidas, previa validación del informe de actividades y resultados por parte del supervisor del contrato.

La factura deberá estar soportada por certificación del cumplimiento del (los) pago(s) de las obligaciones al sistema de seguridad social integral y parafiscales respecto de sus empleados en el periodo facturado.

Los pagos se realizarán de acuerdo con lo siguiente:

- El pago se realizará dentro de los treinta (30) días hábiles siguientes a la presentación de la factura mensual y demás documentos antes descritos.
- El valor por pagar comprende todos los costos directos e indirectos y demás gastos e impuestos causables a cargo del CONTRATISTA.
- Para la realización del pago o abono en cuenta se deberá contar con el recibo a satisfacción del objeto y cumplimiento de las obligaciones contractuales mediante el informe de actividades por parte del CONTRATISTA debidamente cargado y aprobado en SECOP II por el Supervisor, con su respectivo informe de supervisión.
- El valor de la presente contratación será cancelado por TRANSMILENIO S.A., mediante transferencia electrónica en la CUENTA BANCARIA de la Red ACH designada por el CONTRATISTA. La modificación a la cuenta bancaria referenciada en el presente parágrafo no requerirá la expedición de contrato adicional, modificatorio u otro sí, sino la simple manifestación de ello por parte del contratista al supervisor y la Dirección Corporativa.

7. SUPERVISIÓN

La supervisión y control de la debida ejecución del objeto contractual será ejercida por el Profesional Especializado 06 - Seguridad de la Información de la Dirección de TIC usuario o a quien designe el ordenador del gasto.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

8. OBLIGACIONES DE LAS PARTES

8.1. OBLIGACIONES GENERALES DEL CONTRATISTA

Para prestar el servicio requerido por TRANSMILENIO S.A., el CONTRATISTA deberá cumplir con las siguientes obligaciones generales:

1. Cumplir cabalmente con el objeto contractual, las obligaciones contractuales, el alcance del objeto y con cada uno de los servicios descritos en este documento.
2. Permitir la práctica de auditorías por parte de TRANSMILENIO S.A., o a quien el ente Gestor designe y de los diferentes órganos de control, de acuerdo con la Ley.
3. Garantizar el cubrimiento del 100% de los gastos que ocasione la ejecución del contrato.
4. Responder a las solicitudes de documentación e información que le solicite TRANSMILENIO S.A.
5. Responder sin perjuicio de la respectiva garantía por la calidad de los servicios contratados.
6. Cumplir con los compromisos asumidos en la oferta. Una vez surtido el tercer requerimiento de cumplimiento hecho por TRANSMILENIO S.A., por medio escrito o electrónico y de no recibir respuesta oportuna por parte del contratista, se iniciará el proceso administrativo a que haya lugar.
7. Abstenerse de dar declaraciones o entregar información en redes sociales, medios de comunicación y/o a cualquier agente externo a TRANSMILENIO S.A; sin previa consulta y autorización de la Subgerencia de Comunicaciones y Atención al Usuario de TRANSMILENIO S.A.
8. Firmar el correspondiente acuerdo de confidencialidad
9. Asistir a las reuniones de avance del proyecto citadas por TRANSMILENIO S.A. y al Comité de Comunicaciones que con motivo de la ejecución del contrato solicite la Dirección de Tecnologías de la Información y las Comunicaciones de TRANSMILENIO S.A.
10. Acatar las instrucciones que durante el desarrollo del contrato se le impartan por parte de TRANSMILENIO S.A a través del supervisor del contrato.
11. Asegurar que desde el día de la suscripción del Acta de inicio del Contrato y hasta la terminación del mismo, su personal y equipos disponibles cumplan los requerimientos mínimos exigidos contractualmente.
12. Proceder a efectuar el cambio, sin condicionamiento alguno, sobre su equipo de trabajo o personal cuando se genere situaciones que amerite su retiro por cuanto se está afectando la ejecución normal de contrato y así lo solicite TRANSMILENIO

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

S.A.; el contratante estará indemne por cualquier reclamación que eventualmente llegare a efectuar el trabajador, por lo cual el contratista hará personal y directamente las gestiones necesarias para este efecto.

13. Velar por el cuidado de la marca y de TRANSMILENIO S.A, del Sistema TransMilenio y del SITP; en cada una de las acciones y sugerencias que imparta con motivo de la ejecución del contrato.
14. Gestionar y/o tramitar los permisos y demás acciones necesarias para el cumplimiento del contrato, así como, garantizar el cumplimiento de todos los requisitos legales para el desarrollo de cada una de las actividades. En cada caso el costo de los trámites y permisos que se requieran serán de exclusiva responsabilidad del contratista.
15. Garantizar el adecuado uso de los archivos generados y usados por el contratista, reconocimiento que son de propiedad exclusiva de TRANSMILENIO S.A. y no podrán ser usados para distribución propia y/o comercial del contratista.
16. Realizar junto con TRANSMILENIO S.A. la liquidación del contrato una vez terminada su ejecución.
17. Las demás derivadas de la naturaleza del contrato a adjudicar.

8.2. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

Para prestar el servicio requerido por TRANSMILENIO S.A., el CONTRATISTA deberá cumplir con las siguientes obligaciones específicas:

1. Entregar al supervisor a la firma del acta de inicio un documento detallando la ejecución del proyecto (Project Charter), enmarcado en el contexto de las mejores prácticas del PMI.
2. Realizar Ethical Hacking para 400 direcciones IP internas, 5 externas y 5 aplicaciones informáticas que la entidad indicará a través del supervisor.
3. Desarrollar pruebas de ingeniería social a mínimo 30 funcionarios de la entidad para determinar a través de dichas pruebas, el grado de apropiación y generación de la cultura en lo que a seguridad informática se refiere.
4. Realizar pruebas de ingeniería social de manera presenciales en las instalaciones de TRANSMILENIO S.A., en máximo dos (2) sesiones, en la fecha y hora que el ente gestor determine.
5. Realizar las pruebas de ingeniería social garantizando cobertura a funcionarios de planta y contratistas, incluyendo directivos de todas las áreas de la Entidad.
6. Garantizar que las pruebas a ejecutar permitan validar: Seguridad física, seguridad de los equipos, y prácticas de los usuarios internos con respecto a la disposición y tratamiento de la información.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

7. Realizar pruebas de vulnerabilidad utilizando herramientas especializadas de escaneo.
8. Realizar el proceso de análisis de las vulnerabilidades detectadas, clasificándolas de acuerdo con su grado de criticidad.
9. Llevar a cabo la explotación de vulnerabilidades, previas indicaciones impartidas por el supervisor del contrato, en lo referente a fecha, hora y funcionarios acompañantes, presentando informe detallado posterior a su realización.
10. Evaluar la seguridad informática de los dispositivos activos de comunicaciones señalados por TRANSMILENIO S.A., para los escenarios LAN y WAN, mediante la ejecución de pruebas de vulnerabilidad.
11. Emitir las recomendaciones de carácter preventivo y/o correctivos tendientes a dar el adecuado tratamiento a las vulnerabilidades identificadas.
12. Generar los planes de acción correspondientes a las vulnerabilidades identificadas, alineados con estándares internacionales de gestión de riesgos, seguridad informática y mejores prácticas en tecnología.
13. Presentar previo a la firma del acta de inicio la certificación vigente en ISO/IEC 27001:2013 y/o ISO/IEC 27001:2022 , con servicios de consultoría en seguridad de la información, gestión y mantenimiento para soluciones de conectividad y/o diseño, suministro, implementación, soporte, y mantenimiento de soluciones y servicios de seguridad de la información, conectividad y optimización para redes de nueva generación y/o servicios y soluciones de ciberseguridad, gobierno y outsourcing de tecnologías de información y/o monitoreo de eventos e incidentes de seguridad SOC y/o servicios de consultoría en seguridad de la información y ciberseguridad, cubiertos por el alcance de la certificación.

Nota: En caso de presentarse una unión temporal la certificación de ISO/IEC 27001:2013 y/o ISO/IEC 27001:2022 podrá ser acreditada por una de las empresas que conforman la unión temporal.

14. Estructurar y ejecutar un plan de sensibilización con base en los resultados obtenidos en la etapa de ingeniería social, con las siguientes características:
 - Charla de sensibilización en seguridad de la información, con una duración mínima de 45 minutos, dirigida a funcionarios de planta incluidos los directivos y contratistas, de la Entidad.
 - Se deben programar como mínimo dos fechas para la ejecución de la charla, a fin de asegurar la participación del mayor número de funcionarios de TRANSMILENIO S.A.
15. Presentar las hojas de vida del personal especializado a cargo del contrato como anexo a la propuesta económica, a fin de que éstas sean aprobadas por TRANSMILENIO S.A.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

16. Elaborar informes técnicos y gerenciales, con los resultados de las pruebas realizadas, la metodología, las brechas encontradas y recomendaciones puntuales sobre los puntos analizados.

17. Liderar, programar, ejecutar y documentar los aspectos definidos en las reuniones de seguimiento de contrato que permitan controlar el avance del mismo. La elaboración de las actas de reunión estará a cargo del Gerente del proyecto por parte del contratista y estarán suscritas por éste y el supervisor designado por TRANSMILENIO S.A.

18. Realizar un (1) retest para hacer seguimiento de la disminución del riesgo. Que se llevará a cabo máximo en dos (2) meses después de la entrega de los informes técnicos. Dicha prueba deberá ser soportada por carta de compromiso del contratista.

19. Recibir como mínimo una visita de auditoría y seguimiento por parte de TRANSMILENIO S.A., a las instalaciones de la empresa del contratista, para validar aspectos generales de seguridad de la información en lineamiento con las políticas vigentes en la materia al interior de TRANSMILENIO S.A.

20. Dar estricto cumplimiento de la Circular TMSA 009 de 2021, frente a la aplicación del Decreto Distrital 332 del 29 de diciembre del 2020 mediante el cual se incorpora medidas afirmativas que promuevan la participación de las mujeres en la ejecución de los negocios celebrado por el Distrito Capital. Para lo cual deberá incluir la respectiva certificación mensual por parte del revisor fiscal, indicando de forma detallada y expresa su cumplimiento porcentual. Sin perjuicio de lo anterior, la Entidad podrá requerir los soportes o información adicional que estime convenientes para verificar el cumplimiento de esta obligación contractual.

21. Las demás que se incluyan en los anexos de servicios de la prestación de servicios de Ethical Hacking.

8.3. OBLIGACIONES AMBIENTALES A CARGO DEL CONTRATISTA

De acuerdo con la Resolución 3179 de 2023 de la Secretaría Distrital de Ambiente " Por la cual se adopta la guía técnica para la formulación del Plan Institucional de Gestión Ambiental (PIGA), y se dictan lineamientos para su concertación, implementación, evaluación, control y seguimiento, y otras disposiciones", el Programa de Consumo sostenible debe evidenciar acciones que propendan por la implementación de lineamientos ambientales que promuevan el uso y consumo responsable de materiales, elementos, maquinaria, equipos o cualquier tipo de contratación que realice la entidad, mediante la asignación de obligaciones de orden ambiental y así hacer extensiva la cultura de gestión ambiental y responsabilidad social para lo cual deberá:

- Presentar un informe a la firma del Acta de Inicio, con la identificación de los residuos sólidos y residuos peligrosos que se pueden generar en el desarrollo del contrato y las correspondientes actividades generadoras, en caso de que aplique.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

- Realizar el manejo, recolección, transporte, tratamiento y disposición final de los residuos peligrosos generados en la ejecución del contrato conforme a lo establecido en la normatividad ambiental vigente, en caso de que aplique.
- Realizar la gestión de los escombros generados en la ejecución del contrato, de acuerdo con lo contenido en el Decreto 2981 de 2013, Decreto 357 de 1997, Resolución 507 de 2023 y las normas que les modifiquen, adicionen y a aquella que surja en relación con el tema y sea aplicable durante la ejecución del contrato. Adjuntar copia de los correspondientes certificados de recolección y disposición.
- Presentar un informe mensual en el que incluya las cantidades y actividades generadoras de residuos sólidos y residuos peligrosos y escombros durante la ejecución del contrato y describa las actividades desarrolladas para la gestión de esos residuos de conformidad con la normatividad vigente aplicable y adjuntar copia de los correspondientes certificados que soporten la gestión dada, en caso de que aplique.
- Capacitar periódicamente al personal, como mínimo una (1) vez cada trimestre del año, en gestión ambiental, gestión (manejo, disposición, recuperación y almacenamiento) de residuos sólidos y residuos peligrosos, así como en el manejo seguro de sustancias químicas. Adjuntar copia de los soportes de capacitación, en caso de que aplique.
- Verificar periódicamente el estado de licencias y permisos de orden ambiental de las empresas gestoras de residuos peligrosos con las cuales se dispondrán los residuos generados por ejecución contractual, en caso de que aplique.
- Dar cumplimiento a la normatividad ambiental vigente que por el objeto del contrato le sea aplicable y a aquella que surja en relación con el tema durante la ejecución del contrato, principalmente lo concerniente a la gestión de residuos sólidos y residuos peligrosos, en caso de que aplique.
- Cumplir con los requisitos de seguridad y salud ocupacional exigidos por las normas vigentes, en caso de que aplique.

8.4. SEGURIDAD INDUSTRIAL

Será responsabilidad del contratista salvaguardar la seguridad de todas las personas vinculadas en la prestación del servicio contratado.

9. TRANSPORTE Y COMUNICACIONES

El transporte de los equipos objeto de la presente contratación estará a cargo del oferente y se entregarán en la sede administrativa de TRANSMILENIO S.A., Avenida El Dorado 69-76 Torre 1 piso 6 Dirección de TIC.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

10. EQUIPO MÍNIMO REQUERIDO

EQUIPO DE TRABAJO:

El personal técnico ofrecido por el CONTRATISTA deberá contar al menos con dos ingenieros del siguiente perfilamiento:

10.1 LÍDER DEL PROYECTO:

Persona de contacto con quien TRANSMILENIO S.A., podrá efectuar el seguimiento a todas las obligaciones y responsabilidades del contrato.

ITEM	PERFIL	EXPERIENCIA CERTIFICABLE	TÍTULO DE POSGRADO	CERTIFICACIONES
LÍDER DE PROYECTO	INGENIERO DE SISTEMAS Y/O INGENIERO DE TELECOMUNICACIONES Y/O INGENIERO ELECTRONICO Y/O INGENIERO TELEMÁTICO	MÍNIMO (5) CINCO AÑOS DE EXPERIENCIA PROFESIONAL.	GESTIÓN Y/O GERENCIA DE PROYECTOS Y/O ADMINISTRACIÓN DE PROYECTOS	CERTIFICADO IPV6 SILVER Y/O GOLD IPV6 FORUM.
CANTIDAD	1			

10.2 ESPECIALISTA EN ANÁLISIS DE VULNERABILIDADES:

ITEM	PERFIL	EXPERIENCIA CERTIFICABLE	TÍTULO DE POSGRADO	CERTIFICACIONES
ESPECIALISTA EN ANÁLISIS DE VULNERABILIDADES	INGENIERO DE SISTEMAS Y/O INGENIERO DE TELECOMUNICACIONES Y/O INGENIERO ELECTRONICO Y/O INGENIERO TELEMÁTICO	MÍNIMO (3) TRES AÑOS DE EXPERIENCIA PROFESIONAL.	GESTIÓN Y/O GERENCIA DE PROYECTOS Y/O ADMINISTRACIÓN DE PROYECTOS Y/O GERENCIA DE SISTEMAS	Ingeniero certificado CEH versión 8 o superior.
CANTIDAD	1			

NOTA: Las hojas de vidas del recurso humano deberán presentarse por el proponente adjudicatario previo a la firma del acta de inicio, para la presentación en el proceso de selección cada proponente deberá acreditar compromiso de presentación del personal bajo las condiciones establecidas en los documentos del proceso.

Deberá prestar sus servicios como mínimo durante periodo de ejecución del contrato resultante del presente proceso y el tiempo de garantía ofrecido por el proponente. Los demás requisitos de este personal están establecidos en el estudio previo.

	PROCESO DE ADQUISICIÓN DE BIENES Y SERVICIOS ANEXO TÉCNICO	
	CÓDIGO: R-DA-103	FECHA: Diciembre 2018

11. Área responsable de la adquisición
<p>Aprobó: Director Nombre: Rafael Felipe Valdez Laguado Dependencia: Dirección de Tecnologías de la Información y las Telecomunicaciones</p> <p>Elaboró: Profesional Grado 06 Nombre: Javier Alfonso Castañeda Parra Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.</p> <p>Revisó: Contratista Apoyo Técnico Nombre: Germán Guerrero Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.</p> <p>Revisó: Contratista Apoyo Financiero Nombre: Gloria Alexandra Granados Novoa Dependencia: Dirección de Tecnologías de la Información y de la Comunicación.</p> <p>Revisó: Abogada Contratista Apoyo Jurídico Nombre: Isabel Cristina Cruz Moya Dependencia: Dirección de Tecnologías de la Información y de la Comunicación</p> <p>Fecha de elaboración del estudio (21/10/2024):</p>