ANEXO 1

FICHA DE CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN (FCT)

1 DENOMINACIÓN DEL BIEN O SERVICIO

Realizar auditoria y análisis de vulnerabilidades a los sistemas de información de acuerdo con el modelo de seguridad y privacidad de información del Ministerio del Trabajo.

2 CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS (UNSPSC)

Grupo	Segmento	Familia	Clase	Producto	Código UNSPSC	Descripción
Servicios	80	10	15	00	80101500	Servicios de consultoría de negocios y administración corporativa
				07	80101507	Servicios de asesoramiento sobre tecnologías de la información
	81	10	27	02	81102702	Servicios de ingeniería y diseña para sistemas de control de procesos
		11	15	00	81111500	Ingeniería de software o hardware
			18	01	81111801	Seguridad de los computadores, rede o internet
	84	11	16	00	84111600	Servicios de auditoria

3 UNIDAD DE MEDIDA

Para este proceso no aplica unidad de medida, toda vez que el cumplimiento se dará una vez todas las obligaciones contractuales se hayan desarrollado satisfactoriamente.

4 NORMATIVIDAD APLICABLE ESPECÍFICA PARA EL SERVICIO Y/O BIEN

Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

Resolución 746 de 2022. "Por el cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021"

Manual de Gobierno Digital – MINTIC.
Modelo de Seguridad y Privacidad de la Información – MINTIC.
NTC-ISO-IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.
NTC-ISO-IEC 27002:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
ISO/IEC 27003:2017: Este documento proporciona orientación sobre los requisitos para un sistema de gestión de seguridad de la información (SGSI) según lo especificado en ISO/IEC 27001 y proporciona recomendaciones ("debería"), posibilidades ("puede") y permisos ("puede") en relación con ellos.
NTC-ISO-IEC 27005:2020: Tecnología de la información. Técnicas de seguridad. Gestión de riesgos para la seguridad de la información.
CONPES 3701: Este documento CONPES busca fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio.
CONPES 3854 de 2016: Este documento CONPES busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
CONPES 3995: Política nacional de confianza y seguridad digital, establece medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.
Demás normas relacionadas en el normograma del proceso de Gestión de Tecnologías de la Información y Comunicaciones del Ministerio del Trabajo. (Anexo 1)

5 ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR

La auditoría y análisis de vulnerabilidades a los sistemas de información de acuerdo con el modelo de seguridad y privacidad de información del Ministerio del Trabajo deberá realizar las siguientes actividades:

a) Auditoria al cumplimiento los controles, del estándar ISO/IEC 27001:2022 asociados al Grupo interno de trabajo de soporte informático. Está auditoría está enfocada en la revisar los controles de seguridad implementados en el SGSI, evaluando su eficacia para proteger la información y mitigar riesgos.

b) Análisis de vulnerabilidades a los sistemas de información. Esta actividad consiste en el análisis de vulnerabilidades a los sistemas de información que se indican en este documento y a la realización de pruebas de penetración a la plataforma tecnológica

5.1 Auditoria al cumplimiento del estándar ISO/IEC 27001:2022.

La auditoría deberá estar enfocada al cumplimiento de los requisitos habilitantes de la norma para la aplicación de los controles definidos en el estándar ISO//IEC 27001:2022, proyectando este análisis en el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información dando un indicador de cumplimiento de controles del anexo A, de la norma ISO 27001:2022. La dependencia en la cual se realizará el proceso de auditoría es la siguiente: Grupo interno de trabajo de soporte informático.

Esta actividad requiere la profundización en la verificación, análisis y evaluación de las amenazas y riesgos los activos del Grupo interno de trabajo de soporte informático y verificar la aplicación de los controles de seguridad.

Esta auditoría de gestión será externa, de segunda parte, enfocada en la revisión de los controles de seguridad implementados en el SGSI, evaluando su eficacia para proteger la información y mitigar riesgos.

Para el desarrollo de la presente auditoria, el contratista deberá desarrollar las directrices para la auditoría de los sistemas de gestión de la seguridad de la información definida en la ISO/IEC 27007:2020.

5.1.1 Plan de auditoria

El plan de auditoría lo deberá entregar el contratista dentro de los 3 días siguientes al inicio de ejecución (o reunión de apertura) ; debe incluir mínimo los siguientes elementos:

1. Objetivos de la auditoría
2. El alcance de la auditoría, la identificación del Ministerio, sus funciones, políticas y lineamientos aplicados a los aplicativos y sitios web.
3. Los criterios de auditoría y la información documentada del Ministerio.
4. Las ubicaciones (físicas y virtuales), las fechas, el horario y la duración de las actividades de auditoría, las reuniones con los auditados.
5. Un reporte de contexto alineados con el estándar ISO/CEI 27001:2022 Anexo A y el estándar ISO//IEC 27001:2022 a los aplicativos y sitios web establecidos.
6. Los métodos de auditoría que se van a usar, incluyendo el grado en que se necesita el muestreo de la auditoría para obtener las evidencias de auditoría suficientes.
7. Los roles y responsabilidades de los miembros del equipo auditor, así como los guías y los observadores o intérpretes.
8. La asignación de los recursos apropiados en consideración de los riesgos y oportunidades relacionados con las actividades que se van de auditar.
9. Estructura del informe de resultados de la auditoría que incluya las conformidades, oportunidades de mejora, no conformidades y conclusiones.
10. Plan de riesgos en función del logro de los objetivos de la auditoría y las oportunidades.
11. Los requerimientos de confidencialidad y la seguridad de la información.
12. Las actividades de seguimiento de la auditoría planificada.
13. Elaborar las actas de las sesiones de auditoria firmadas por los auditados.
14. Preparación de las conclusiones de la auditoría.
15. Realización de la sesión de cierre de la auditoría.

Nota: Algunas actividades de la auditoría se podrán realizarse de manera remota cuando no sea posible la evaluación en sitio, en este caso, se utilizarán medios electrónicos para obtener las pruebas garantizando juicios objetivos conforme a los criterios establecidos y se alternarán con la verificación de las condiciones físicas de la infraestructura tecnológica en las instalaciones del Ministerio de acuerdo con el cronograma o plan de trabajo.

5.1.2 Ejecución del plan de auditoría

Las actividades de auditoría deberán ser llevadas a cabo teniendo en cuenta la siguiente secuencia:

1. Realización de la reunión de apertura.
2. Revisión documental durante la realización de la auditoría.
3. Comunicación durante la auditoría.

4. Asignación de roles y responsabilidades de guías y observadores.
5. Recolección y verificación de información.
6. Generación de hallazgos de auditoría.
7. Preparación de conclusiones de auditoría.
8. Realización de reunión de cierre.

5.2 Análisis de vulnerabilidades

Para esta actividad se requiere la ejecución de prueba de penetración a los sistemas de información, sistemas operativos, base de datos, red de transporte de datos y equipos de seguridad perimetral, se aplicarán conforme los lineamientos definidos por el estándar Penetration Testing Execution Standard – PTES definido en la URL http://www.pentest-standard.org/index.php/Main_Page y subsecuentes elementos del sitio web.

Las características mínimas que debe planearse para esta fase serán las siguientes:

1. La prueba será una prueba de penetración interna.
2. El método de acceso será mediante White-Box Pentesting.
3. Análisis autenticado
4. Análisis intrusivo
5. Escaneo de vulnerabilidades avanzado y completo.
6. Obtención de datos activa (OSINT).

El Ministerio del Trabajo se compromete a brindar toda la información técnica necesaria para que de esta forma se pueda auditar la protección y los controles del objetivo, buscando ser minuciosa y a su vez el analista pueda construir una visión completa de las pruebas y sus respuestas, generando amplitud y profundidad en el análisis y resultados

El Ministerio del Trabajo requiere que en el proceso de pruebas de penetración sean desarrolladas las siguientes actividades:

- Interacciones previas al compromiso
- Recopilación de inteligencia
- Modelado de amenazas
- Análisis de vulnerabilidades
- Explotación
- Explotación posterior
- Informe final pruebas de penetración

Para el desarrollo del ítem 5.2 Análisis de vulnerabilidades, es necesario:

A. Entregar el artefacto plan del despliegue del estándar Penetration Testing Execution Standard – PTES, cronograma de ejecución, alcance, relación de las herramientas a ser utilizadas en cada etapa.
B. Informe técnico del desarrollo de las pruebas de penetración conforme PTES, que contenga como mínimo la siguiente información: Dirección IP, nombre del sistema de información/equipo/servicio evaluado, nivel de riesgo, numero de vulnerabilidades clasificadas en alto, medio, bajo, descripción de la vulnerabilidad, impacto según CVE, tratamiento de la vulnerabilidad, remediaciones y controles

compensatorios en cada vulnerabilidad, aspectos positivos encontrados durante las pruebas, resultado del proceso de explotación de vulnerabilidades y oportunidades de mejoramiento.

C. Informe conforme el estándar de ejecución de pruebas de penetración (PTES).
D. Artefactos y/o documentos productos de las siguientes etapas del estándar PTES:
    - Interacciones previas al compromiso
    - Recopilación de inteligencia
    - Modelado de amenazas
    - Análisis de vulnerabilidades
    - Explotación
    - Explotación posterior

Estas pruebas estarán enfocadas a la explotación de vulnerabilidades en:

A. Sistemas operativos con servicios expuestos conforme el modelo OSI.
B. Sistemas de información críticos para la operación de las actividades misionales y de apoyo de la entidad, listados en el título: Elementos de software y hardware objeto de pruebas
C. Motores de base de datos.
D. Redes y seguridad perimetral

5.2.1 Herramientas para el escaneo de vulnerabilidades.

El paquete de aplicaciones de software a ser usados como herramientas de escaneo de vulnerabilidades, deben ser herramientas propietarias bajo licencia de uso. No se admitirán herramientas open source, GNU, GPL, gratuitas, propietaria, de uso libre. Las herramientas deben ser de uso comercial y se debe acreditar el licenciamiento a nombre del contratista o del Ministerio del Trabajo.

Alguna de las características mínimas que debe poseer las herramientas de escaneo son las siguientes:

A. Escaneo eficiente de aplicaciones web
B. Escaneo eficiente de software administrador de base de datos.
C. Las herramientas deben contar con la identificación de más de 50.000 CVE (Common Vulnerabilities and Exposures).
D. Escaneo de vulnerabilidades avanzado y completo.
E. Utilizar para el desarrollo del análisis de vulnerabilidades herramientas homologadas por el CVE (Common Vulnerabilities and Exposures), y www.mitre.org, y estar actualizadas a la fecha de su utilización, para lo cual deberá adjuntar en los informes presentados certificado de homologación de CVE, o ruta de la página de CVE donde se pueda evidenciar que la herramienta ofrecida está homologada por dicha entidad.
F. Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).
G. Los hallazgos de las vulnerabilidades críticas deben ser informados inmediatamente al supervisor del contrato y al jefe de la Oficina de tecnologías de la Información y las Comunicaciones TICS.

5.2.2 Elementos de software y hardware objeto de pruebas

5.2.2.1 Sistemas de información que serán objeto de la prueba.

A. Sistema de procedimiento sancionatorio IVC: Sistema para registro y gestión del procedimiento administrativo sancionatorio.

B. Sistema de información de archivo sindical: Gestionar todos los trámites y procesos del archivo sindical.
C. Tramites y Servicios.: Ventanilla de radicación WEB de trámites y servicios, para realizar alguno de los 20 tramites ofertados por el ministerio del trabajo, acorde a lo definido por IVC
D. Gestión documental: Sistema de Información que utiliza el Ministerio a nivel nacional para su Gestión Documental.
E. PQRSD y preguntas frecuentes: Sistema de información web para atención al ciudadano
F. Cobro Coactivo: Sistema para el cobro coactivo del Ministerio del Trabajo-
G. Portal WEB www.mintrabajo.gov.co
H. RUTEC Registro Único de Trabajadores Extranjeros en Colombia
I. Sistema de información para el sistema general de riesgos laborales: Capturar el nivel de implementación de los estándares mínimos de RL en las empresas.
J. SIRITI: Sistema de Información Integrado para la Identificación, Registro y Caracterización del Trabajo Infantil y sus Peores Formas de trabajo.

El proveedor deberá realizar al menos un (01) ejercicio de pruebas de penetración conforme el estándar PTES a cada uno de los sistemas de información relacionados en el presente ítem. Efectuará las respectivas recomendaciones sobre los sistemas de información y pagina web objeto de las pruebas. Se deberá contar con el recurso humano y logístico especializado para esta actividad. Las pruebas deben ser planeadas en coordinación con el supervisor del contrato y autorizadas por éste.

Las acciones que se realicen para el análisis de vulnerabilidades no deberán causar ningún tipo de afectación e indisponibilidad de servicios de la Entidad.

5.2.3 Sistemas operativos objeto de pruebas.

Se desarrollará el proceso de pruebas de penetración a 30 máquinas con sistemas operativos virtualizados, dentro de los cuales habrá Windows server y Linux.

5.2.4 Motores de base de datos objeto de pruebas

Para el desarrollo de este proceso, se enfocarán en la totalidad de los despliegues de motores de base de datos que se encuentren instalados.

Los motores de base de datos a los cuales se les desarrollara las pruebas son las siguientes distribuciones:

A. Microsoft SQL Server
B. Oracle Database

5.2.5 Redes y seguridad perimetral objeto de pruebas

Es requerido evaluar los elementos de hardware o software definidos de la infraestructura del Ministerio del Trabajo, tanto en los segmentos de red expuestos en la DMZ como en los segmentos de red internos. Los elementos para probar son:

A. Verificar e identificar vulnerabilidades en las configuraciones de los router de borde que le prestan el servicio de transmisión de datos e internet al Ministerio del Trabajo.
B. Verificar el versionamiento y necesidades de actualización al Firmware de los router de borde que le prestan el servicio de transmisión de datos e internet al Ministerio del Trabajo.
C. Verificar e identificar vulnerabilidades en las configuraciones de los Firewall implementados.

5.3 Productos

Todos los necesarios, definidos y requeridos dentro del presente documento dentro de los que se destacan los siguientes:

A. **Plan de Auditoría**: En donde se establezca la planificación, ejecución y la comunicación de los resultados de la Auditoria.

B. **Informe Final del resultado de la auditoria** debe ser claro y estructurado para proporcionar una visión completa y comprensible de los hallazgos, recomendaciones y conclusiones, el Informe deberá contar como mínimo con los siguientes elementos: Reporte del cumplimiento de implementación de los controles del anexo A de la norma ISO 27001:2022 y norma ISO/IEC 27002:2022. resumen Ejecutivo, descripción del Entorno, Metodología de Auditoría, Hallazgos, Conclusiones, Recomendaciones, Plan de Acción, Anexos, Firma y Aprobación

C. **Plan Análisis de Vulnerabilidades**: Entregar el documento del plan de ejecucion del estándar Penetration Testing Execution Standard – PTES, en donde se establezca la planificación, ejecución y la comunicación de los resultados Debe contar como mínimo con los siguientes componentes: Metodología, cronograma, Herramientas y Técnicas, Criterios de Evaluación, Roles y Responsabilidades, Priorización y Clasificación, Reporte de Resultados, Plan de Acción y remediación, Revisión y Seguimiento, Documentación y Archivo,

D. **Informe final del análisis de vulnerabilidades**, el cual contendrá al menos los siguientes elementos según los establecido en el estandar Penetration Testing Execution Standard – PTES:

- ✓ Interacciones previas al compromiso
- ✓ Recopilación de inteligencia
- ✓ Modelado de amenazas
- ✓ Análisis de vulnerabilidades
- ✓ Explotación
- ✓ Explotación posterior

a. El informe técnico del desarrollo de las pruebas de penetración conforme PTES, deberá contener, además de los definido por el estándar, la siguiente información: Dirección IP, nombre del sistema de información/equipo/servicio evaluado, nivel de riesgo, numero de vulnerabilidades clasificadas en alto, medio, bajo, descripción de la vulnerabilidad, impacto según CVE, tratamiento de la vulnerabilidad, remediaciones y controles compensatorios en cada vulnerabilidad, aspectos positivos encontrados durante las pruebas, resultado del proceso de explotación de vulnerabilidades y oportunidades de mejoramiento.

b. Informes de pruebas de penetración conforme el estándar The penetration testing execution standard, cuyos elementos del informe se evidencian en la URL http://www.pentest-standard.org/index.php/Reporting .

c. Entregar el artefacto plan del despliegue del estándar Penetration Testing Execution Standard – PTES, cronograma de ejecución, alcance, relación de las herramientas a ser utilizadas en cada etapa.

5.4 Equipo de trabajo

De acuerdo con la naturaleza del contrato y las actividades a realizar, el contratista deberá garantizar el siguiente personal mínimo, para lo cual el oferente deberá incluir en su propuesta las hojas de vida de los miembros del equipo de trabajo.

i. Un (1) Auditor Líder: Ingeniero de sistemas, o Ingeniero de telecomunicaciones, o ingeniero de software, o Ingeniero electrónico, debe contar con posgrado (especialización o maestría) en gerencia de proyectos o en seguridad de la información o en seguridad informática o en gerencia de ingeniería, o en gerencia y tecnologías de la información, con experiencia relacionada en auditorias SGSI de mínimo tres (3) años y debe contar con certificación: Auditor líder ISO 27001:2022

ii. Un (1) Auditor Interno: Ingeniero de sistemas, o Ingeniero de telecomunicaciones, o ingeniero de software, o Ingeniero electrónico, debe contar con posgrado (especialización o maestría) en seguridad de la información o en seguridad informática, con experiencia relacionada en auditorias SGSI de mínimo dos (2) años, y debe contar con certificación: Auditor líder ISO 27001:2012 o auditor interno ISO 27001:2012.

iii. Un (1) Especialista pruebas de penetración: Ingeniero de sistemas, Ingeniero de telecomunicaciones, ingeniero de software, Ingeniero electrónico o ingenierías afines, debe contar con posgrado (especialización o maestría) en seguridad de la información, en seguridad informática, en seguridad física y de la Informática, en Seguridad de las Tecnologías de la información y de las Comunicaciones, en seguridad de redes telemáticas, en gestión de seguridad y riesgo informático o en ciberseguridad y ciberdefensa. Con experiencia relacionada específica ejecutado pruebas de análisis de vulnerabilidades y pruebas de penetración, de mínimo 3 años y debe contar con alguna de las siguientes certificaciones: CEH – Certified Ethical Hacker, CPTE Certified Penetration Testing Engineer, ECSA – Ec Council Certified Security Analist, LPT -EC-Council Licensed Pen Testing Tester, CompTIA Security + Certified, Mile2, CPEH – Certified Professional Ethical Hacker, OSCP - Offensive Security Certified Professional.

El personal profesional descrito anteriormente, estará sujeto a la verificación como requisito habilitante.

Nota:

- Los profesionales en Ingeniería antes descritos, deben contar con matrícula profesional.
- El contratista deberá garantizar que los profesionales evaluados como requisito habilitante, se mantengan durante la ejecución del contrato. Si por fuerza mayor es indispensable su cambio, se requiere solicitar por escrito el contratista dirigido al supervisor del contrato, anexando la hoja de vida del personal postulado con sus soportes. Esta solicitud será considerada por el supervisor del contrato para su respectiva aprobación.
- La experiencia de los profesionales en ingeniería para efectos de la verificación se contará a partir de la expedición de la tarjeta profesional.

El proponente adjudicatario deberá adjuntar con la propuesta las hoja de vida del personal propuesto como equipo técnico con todos los soportes de educación y/o acreditación, así como las certificaciones de experiencia, las cuales deberán acreditarse en idioma español o en su defecto acompañadas con traducción simple al español.

Las certificaciones aportadas de experiencia deberán contener como mínimo:

i. Nombre de la empresa.
ii. Fecha de vinculación (día, mes y año) y de retiro (día, mes y año).
iii. objeto del contrato o cargo, descripción de las funciones y/o actividades desempeñadas para el caso de certificación de experiencia
iv. Fecha de expedición de la certificación.

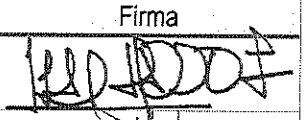
En todos los casos las certificaciones podrán ser verificadas por el Ministerio del Trabajo.

- Las certificaciones de los cursos deben ser emitidos por entidades autorizadas.
- Las certificaciones de los cursos deben tener los respectivos códigos para verificación en los sitios web oficiales.
- Las certificaciones de los cursos deben estar vigentes en el momento de la firma del contrato y podrán venir en idioma español o inglés.

En el evento en que algún miembro del equipo de trabajo presente título obtenido en el exterior, con el fin de determinar la validez y legalidad de estos, éstos deberán estar debidamente convalidados ante el Ministerio de Educación Nacional.

Nota: El personal técnico descrito anteriormente, será verificado durante el proceso de selección.

6 APROBACIONES

Aprobaciones	Nombre y cargo	Firma
Aprobó	Iván Hernando Pardo	
Revisó	Darío Oswaldo Mosquera Tribales	
Elaboró	Zulay A. Salinas T	