TÉRMINOS DE REFERENCIA
"SERVICIO DE SUSCRIPCIÓN DE LICENCIA DE SOFTWARE DE CIBERSEGURIDAD PARA DNS DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES"

Órgano y/o Unidad Orgánica:	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
Actividad del POI	AOI00015400158: Administración de la Infraestructura Tecnológica
Meta presupuestal	057
Denominación de la Contratación:	SERVICIO DE SUSCRIPCIÓN DE LICENCIA DE SOFTWARE DE CIBERSEGURIDAD PARA DNS DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES.

1. FINALIDAD PÚBLICA

La Oficina de Tecnologías de la Información y Comunicaciones (OTIC) requiere Garantizar la disponibilidad, integridad, autenticidad y confiabilidad de los servicios digitales institucionales publicados a través del dominio trabajo.gob.pe, fortaleciendo la seguridad de los servicios de correo electrónico institucional, reduciendo el riesgo de suplantación de identidad (spoofing y phishing), mejorando la reputación digital del Ministerio de Trabajo y Promoción del Empleo y contribuyendo a la continuidad de los servicios digitales brindados a ciudadanos, empresas y entidades públicas.

La contratación de la suscripción de licencias de software de ciberseguridad para DNS permitirá implementar mecanismos avanzados de autenticación y protección del dominio institucional **trabajo.gob.pe** mediante el uso de estándares internacionales como SPF, DKIM, DMARC, BIMI, MTA-STS y TLS-RPT, reduciendo significativamente el riesgo de suplantación de identidad, fraude electrónico, phishing y uso indebido de la marca institucional.

2. OBJETIVO DE LA CONTRATACIÓN

2.1. Objetivo General

Contratar una suscripción de licencias de software de ciberseguridad para DNS seguro, autenticación de dominios y protección de marca digital, que permita fortalecer la seguridad del dominio institucional trabajo.gob.pe mediante la implementación, monitoreo y gestión de SPF, DKIM, DMARC, BIMI, MTA-STS, TLS-RPT y mecanismos de detección de suplantación de identidad digital.

2.2. Objetivos Específicos

- Incrementar la protección contra ataques de phishing y spoofing.
- Mejorar la reputación del dominio institucional.
- Aumentar la entregabilidad de correos legítimos.
- Implementar monitoreo permanente de dominios fraudulentos.
- Contar con reportes y métricas de seguridad del dominio.
- Fortalecer la postura de ciberseguridad institucional.

3. ALCANCES O DESCRIPCIÓN DEL SERVICIO

3.1. Alcance

El servicio deberá permitir autenticar el dominio trabajo.gob.pe para el envío legítimo de correos a las instituciones y evitar la suplantación de identidad, fortaleciendo los protocolos DMARC, SPF, DKIM y BIMI, e incorporar un módulo de protección de marca que monitoree y detecte dominios similares o fraudulentos que suplanten la identidad digital de la entidad.

3.2. Descripción del servicio

3.2.1. Consideraciones generales

a) El servicio debe permitir observar e identificar si el correo de la entidad está en cumplimiento con los protocolos de seguridad SPF, DMARC, DKIM, BIMI, MTA STS y TLS-RPT.
b) Deberá permitir visualizar picos de volumen de email.
c) El servicio deberá contar con un informe que detalle las IPs de envío.
d) Deberá mostrar la lista de servidores que envían y/o retransmiten correos en nombre del dominio de la entidad.
e) Deberá permitir identificar la fuente del correo electrónico mal intencionado para tomar una decisión.
f) Deberá permitir identificar los países en donde se encuentran los servidores que utilizan el dominio de la entidad.
g) Deberá procesar tanto reportes agregados como reportes forenses.
h) Deberá permitir configurar de manera ordenada los protocolos de seguridad SPF, DMARC, DKIM, BIMI, MTA STS y TLS-RPT.
i) Deberá permitir configurar BIMI incluir el logo certificado.
j) Deberá permitir delegar los protocolos SPF, DMARC, DKIM, BIMI, MTA STS y TLS-RPT para ser gestionado desde el propio sistema.
k) Deberá permitir activar políticas restrictivas asegurando sus fuentes de correos mediante la aplicación de protocolo de DMARC.
l) Deberá permitir la compresión del SPF a fin de evitar el exceso de lookups.
m) Deberá permitir gestionar tantos dominios como sean necesarios. Ya sean activos como inactivos.
n) Deberá permitir aplicar políticas para que los correos provenientes de fuentes no autorizadas sean identificados y puestos en cuarentena o rechazados según corresponda.
o) Deberá proveer reportes periódicos y automáticos sobre el nivel de exposición de la infraestructura de envío.
p) Deberá permitir detectar quién envía correos a nombre del dominio que no sea parte del servidor de correos.
q) Deberá permitir autorizar el envío de correos sólo a remitentes que pertenezcan a la institución o sean autorizados por ella.
r) Deberá contar con un sistema de prevención contra intrusos e inspección de todo tipo de tráfico.

s) Deberá contar con una gestión de reputación para el dominio protegido.
t) La plataforma deberá contar con doble factor de autenticación para los usuarios.
u) Deberá contar con gestión de permisos de administrador de cuenta, usuario de cuenta y usuario de solo lectura.
v) Deberá permitir la integración con API y SSO.
w) Deberá incluir un simulador de impacto de políticas de DMARC, permitiendo probar diferentes políticas sin afectar la entrega real de correos.
x) Deberá contar con un monitor de cambios DNS automático, que alerte sobre modificaciones que afecten los registros de SPF, DMARC, DKIM, BIMI, MTA STS y TLS-RPT.
y) Deberá soportar la migración de dominios, permitiendo mover configuraciones de autenticación entre distintos proveedores de DNS sin pérdida de seguridad.
z) Deberá detectar y alertar sobre intentos de suplantación mediante dominios homógrafos, utilizando caracteres visualmente similares.
aa) Deberá generar informes de compliance con regulaciones, como la protección de datos personales, mostrando el cumplimiento en términos de seguridad de correos electrónicos.
bb) El servicio deberá ofrecer un módulo de entrenamiento en seguridad para los usuarios, con lecciones sobre detección de phishing y correos maliciosos, basado en reportes forenses reales.
cc) Deberá contar con una herramienta que optimice automáticamente los registros SPF, sugiriendo correcciones para evitar problemas de lookups.
dd) El servicio debe incluir un monitor de reputación en tiempo real, permitiendo la visualización inmediata de cambios en la reputación de los servidores de correo.
ee) Deberá contar con una función que detecte y corrija automáticamente errores en la configuración DNS, proporcionando recomendaciones para su resolución.
ff) Deberá consolidar reportes agregados y forenses en un solo panel, con filtros avanzados para facilitar el análisis.
gg) El proveedor debe entregar un acceso a la plataforma de autentificación de dominio.
hh) El servicio deberá estar registrado a nombre de la entidad y ser entregado de manera virtual.

3.2.2. Autenticación de dominio

a) Debe soportar SPF (Sender Policy Framework).
b) Debe ser compatible con DKIM (Domain Keys Identified Mail).
c) Debe implementar y monitorear políticas DMARC (Domain-based Message Authentication, Reporting, and Conformance).
d) Debe gestionar múltiples dominios y subdominios.
e) Debe generar registros SPF y DKIM automáticamente.

f) Debe analizar los registros DNS para asegurar su correcta configuración.
g) Debe integrarse con proveedores de DNS para facilitar la actualización de registros.
h) Debe autenticar BIMI certificado con el logo del Ministerio de Trabajo y Promoción del Empleo y validado en https://mxtoolbox.com/SuperTool.aspx#
i) Debe implementar MTA-STS para evitar ataques de intercepción y la alteración de mensajes durante su tránsito.
j) Debe implementar TLS-RPT Supervisar la seguridad de las comunicaciones entre servidores, Detectar fallos en el cifrado, configuraciones incorrectas o problemas con certificados Facilitar la implementación del registro DNS requerido, Procesar y presentar los reportes en un formato claro y ayudar a mejorar la seguridad ajustando configuraciones según los problemas detectados.

3.2.3. Monitoreo y reportes

a) Debe generar informes DMARC en formato XML y PDF.
b) Debe proporcionar reportes de rua y ruf para monitorear el tráfico de correo electrónico.
c) Debe ofrecer desglose de resultados de autenticación por país, proveedor y servidor.
d) Debe permitir la visibilidad completa de los intentos fallidos de suplantación.
e) Debe analizar reportes para identificar fuentes legítimas y no legítimas de correos electrónicos.
f) Debe identificar y eliminar fuentes no autorizadas de correos electrónicos.
g) Debe generar reportes automatizados de salud del dominio por correo electrónico.
h) Debe detectar problemas de entregabilidad en correos legítimos.
i) Debe visualizar en tiempo real las amenazas y correos no autenticados.
j) Debe permitir la exportación de reportes en CSV y PDF.
k) Políticas y Seguridad:
l) Debe permitir configurar políticas DMARC flexibles como none, quarantine y reject.
m) Debe soportar la aplicación de políticas personalizadas para subdominios.
n) Debe auditar los cambios en las configuraciones y políticas de seguridad.
o) Debe identificar servicios en la nube autorizados y no autorizados que envían correos en nombre del dominio.
p) Debe realizar seguimiento y análisis de IPs de envío no autorizadas.
q) Debe monitorear falsificaciones y correos no alineados.
r) Debe soportar políticas de subdominio independiente.
s) Debe implementar políticas DMARC de impacto cero (modo none) para observar resultados sin interferir en la entrega de correos.

t) Debe proteger contra la suplantación de identidad en envíos de terceros.
u) Protección de Marca y Certificaciones:
v) Debe implementar BIMI (Brand Indicators for Message Identification) para mejorar la visibilidad de la marca.
w) Debe permitir la certificación de la marca visual en bandejas de entrada compatibles.
x) Debe prevenir la suplantación de dominios de alto perfil.
y) Gestión de Reputación:
z) Debe mejorar la reputación del dominio al implementar políticas estrictas de autenticación.
aa) Debe identificar y eliminar direcciones IP que afecten negativamente la reputación del dominio.
bb) Debe monitorear la reputación del dominio y ajustar automáticamente la configuración para mejorar la entregabilidad.
cc) Debe soportar análisis de IPs bloqueadas y listas negras.
dd) Debe validar periódicamente direcciones IP autorizadas para asegurar la autenticación consistente.
ee) Facilidad de Uso y Configuración:
ff) Debe proporcionar una interfaz intuitiva y amigable para configurar y gestionar políticas SPF, DKIM, DMARC y BIMI.
gg) Debe ofrecer plantillas automáticas para la creación de registros DNS.
hh) Debe implementar un asistente paso a paso con recomendaciones basadas en buenas prácticas.
ii) Debe configurar alertas automáticas para cambios críticos en la política de autenticación.
jj) Debe actualizar automáticamente los registros de autenticación con un solo clic.
kk) Debe permitir la programación de reportes y alertas periódicas.
ll) Debe soportar múltiples usuarios con roles y permisos personalizados.
mm) Debe configurar alertas de detección de intentos de ataque.
nn) Debe detectar automáticamente problemas en la infraestructura de correos.
oo) Debe integrar plataformas de gestión de correos electrónicos y sistemas de terceros.
pp) Debe almacenar un historial de cambios y auditorías accesibles desde la consola.
qq) Debe ofrecer documentación detallada y tutoriales integrados.

3.2.4. Seguridad de la información

a) El servicio debe cifrar los datos en reposo y en tránsito.
b) El servicio debe gestionar de manera segura las credenciales y claves DKIM.
c) El servicio debe implementar autenticación multifactor (MFA) para usuarios administrativos.

d) El servicio debe soportar IP whitelisting para limitar el acceso a ubicaciones seguras.
e) Debe gestionar usuarios con autenticación segura.
f) Debe cumplir con normativas de seguridad como la de protección de datos personales.
g) El servicio debe realizar auditorías de seguridad sobre el uso de la plataforma.
h) El servicio deberá almacenar reportes de manera segura en la nube.

3.2.5. Integración con servicios externos

a) El servicio debe integrar servicios de correo como Zimbra, Gmail, Google Workspace y Yahoo Mail.
b) Debe identificar servicios de terceros que envían correos en nombre del dominio.
c) Debe integrarse con plataformas de monitoreo de seguridad y sistemas SIEM.
d) El servicio deberá proporcionar una API para automatizar el monitoreo y análisis de reportes DMARC.
e) Deberá ser compatible con proveedores de DNS como Cloudflare, GoDaddy, y AWS Route 53.

3.2.6. Optimización de entregabilidad

a) Debe mejorar la entregabilidad al identificar y resolver problemas de autenticación.
b) Debe analizar correos legítimos bloqueados para ajustar las políticas sin impactar la comunicación.
c) Debe recomendar ajustes automáticos para mejorar las tasas de entregabilidad.
d) Debe proteger contra la falsificación de direcciones de correo.
e) Debe identificar y resolver problemas de alineación de correos.
f) Debe proporcionar un análisis detallado de dominios que fallan la autenticación.

3.2.7. Recuperación ante incidentes

a) El servicio deberá alertar y bloquear fuentes no autorizadas en tiempo real.
b) Debe generar reportes de incidentes con recomendaciones para resolver fallos de autenticación.
c) Deberá ofrecer soporte para la recuperación de credenciales DKIM comprometidas.
d) Deberá detectar anomalías en patrones de envío de correos.
e) Debe bloquear automáticamente fuentes sospechosas de envío.
f) Deberá mitigar ataques de phishing dirigidos.
g) Deberá contar con planes de recuperación ante desastres.
h) Deberá realizar copias de seguridad de la información crítica.

3.2.8. Protección de marca y monitoreo de dominios

a) El servicio deberá incluir un módulo de protección de marca (Brand Protection) que monitoree de forma continua el uso indebido de la identidad digital y del nombre de dominio institucional trabajo.gob.pe en internet.
b) Deberá detectar automáticamente dominios similares, fraudulentos o de suplantación (typosquatting, dominios homógrafos y variaciones de extensión o TLD alternativos) que imiten al dominio institucional, por ejemplo trabajo.io, trabajo.live, trabajo.store, trabajo.org, trabajo.net, trabajo.info, trabajo.co, trabajo.online, trabajo.com, trabajo.site, trabajo.biz, trabajo.app y trabajo.xyz, entre otros.
c) Deberá aplicar técnicas de descubrimiento que incluyan, como mínimo, la generación de variantes por extensión o TLD alternativo (alt_tld), sustitución y omisión de caracteres, y permutaciones del nombre de dominio.
d) Deberá asignar a cada dominio detectado una puntuación de riesgo (score) y un nivel de riesgo categorizado (Alto, Medio y Bajo), que permita priorizar la atención de las amenazas más críticas.
e) Para cada dominio sospechoso deberá mostrar, como mínimo, la técnica de generación utilizada, el origen, el estado de su servicio web, la existencia de registros MX (correo), la presencia de certificado SSL/TLS, la antigüedad del dominio y el estado del contenido publicado.
f) Deberá permitir filtrar los dominios detectados por nivel de riesgo y por estado (activos o inactivos), facilitando el análisis del analista de seguridad.
g) Deberá identificar dominios que cuenten con servicio web activo, registros MX configurados y/o certificado SSL válido, por representar un mayor potencial de uso malicioso (suplantación de portales o envío de correos fraudulentos).
h) Deberá mantener un historial de escaneos que registre la fecha, hora, tipo de análisis (manual o automático), cantidad de dominios hallados y cantidad de dominios activos, así como el estado de cada escaneo.
i) Deberá permitir ejecutar análisis de marca bajo demanda (escaneo manual) y de manera programada o automática, con capacidad de refrescar los resultados.
j) Deberá contar con capacidades de descubrimiento de activos digitales expuestos asociados a la entidad (Attack Surface y Dark Exposure), así como inteligencia de amenazas (Threat Intel) relacionada con el dominio protegido.
k) Deberá ofrecer monitoreo en tiempo real con generación de alertas ante la aparición de nuevos dominios similares, cambios en su estado o incremento en su nivel de riesgo.
l) Deberá permitir la gestión de la superficie de exposición de marca a nivel ejecutivo (Executive Risk) y de cadena de suministro digital (Supply Chain), según corresponda.

3.2.9. Reportes e indicadores de compromiso (IOC) defensivos

a) Deberá permitir la exportación de reportes de los dominios similares e indicadores detectados en múltiples formatos estándar, como mínimo: PDF, CSV, JSON y HTML.
b) Deberá generar indicadores de compromiso (IOC) en formatos compatibles con plataformas de seguridad, incluyendo, como mínimo: IOC para SIEM, lista de bloqueo (Blocklist) y reglas para firewall (Firewall).
c) Los reportes e IOC generados deberán poder integrarse con las plataformas de monitoreo de seguridad y SIEM de la entidad para reforzar las medidas defensivas.
d) Deberá permitir la programación y descarga periódica de reportes de protección de marca, facilitando las auditorías y el seguimiento del nivel de exposición del dominio institucional.
e) Deberá consolidar en un único panel (dashboard) los dominios similares detectados, su nivel de riesgo y el historial de escaneos, con opciones de filtrado avanzado para el análisis.
f) Deberá contar con un módulo de inteligencia que incluya, como mínimo, las siguientes herramientas adicionales: SenderGraph para el análisis y visualización de las fuentes de envío del dominio; DMARC Autopilot para la gestión y ajuste automático de las políticas DMARC; Dominios Similares para la detección y monitoreo de dominios similares o fraudulentos que suplanten la identidad digital de la entidad; y Fleet Threat Intel para la inteligencia de amenazas relacionada con el dominio protegido.

3.2.10. Consola de administración

a) Deberá contar con un Dashboard que permita mostrar el volumen de correos autenticado y no autenticado.
b) Deberá contar con un panel de configuración de políticas DMARC que permita establecer, modificar y monitorear políticas en modo de monitoreo, cuarentena o rechazo.
c) Deberá ofrecer herramientas de validación de registros SPF y DKIM para verificar si están configurados correctamente y detectar posibles problemas.
d) Deberá incluir un sistema de reportes detallados en tiempo real que visualice los correos autenticados, no autenticados y los intentos de suplantación.
e) Deberá contar con un módulo de alertas automatizadas que notifique sobre problemas críticos, como intentos de spoofing o configuraciones incorrectas.
f) Deberá incluir un visor de registros históricos de tráfico de correo para analizar tendencias y evaluar la evolución de la seguridad del dominio.
g) Deberá permitir la gestión simultánea de múltiples dominios desde una sola consola con opciones de configuración individualizadas para cada dominio.

h) Deberá contar con herramientas de simulación de políticas DMARC para evaluar el impacto de los cambios antes de implementarlos en producción.
i) Deberá ofrecer soporte para la implementación de MTA-STS y BIMI con guías de configuración integradas y monitoreo de cumplimiento.
j) Deberá incluir un sistema de gestión de usuarios y roles que permita asignar permisos específicos a diferentes equipos o administradores.
k) Deberá contar con una API para integrar la consola con herramientas externas y automatizar procesos de análisis y configuración.
l) Deberá permitir la exportación de informes en formatos estándar como CSV o PDF, facilitando auditorías y análisis adicionales.
m) Deberá ofrecer visualizaciones gráficas y estadísticas intuitivas para facilitar la comprensión de datos y métricas clave sobre autenticación de correos.
n) Deberá incluir un sistema de monitoreo continuo de seguridad que detecte cambios en los registros DNS que puedan comprometer la autenticación.
o) Deberá contar con compatibilidad multiidioma para facilitar su uso por equipos globales y en diversos contextos.
p) Deberá ofrecer cifrado avanzado para la transmisión de datos y garantizar la seguridad de la información gestionada en la plataforma.

3.2.11. Condiciones de Ejecución

La ejecución del servicio de autenticación de dominio deberá realizarse garantizando el cumplimiento de estándares internacionales de seguridad, la continuidad operativa de los servicios de correo institucional y la protección integral del dominio trabajo.gob.pe, bajo las siguientes condiciones:

- El servicio deberá implementarse en coordinación con la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones (OGETIC), asegurando la compatibilidad con la plataforma de correo electrónico institucional y con los servidores DNS utilizados por la entidad.
- Toda la configuración y gestión deberá realizarse a nombre de la entidad contratante, manteniendo la titularidad total del dominio, los registros DNS y los certificados asociados.
- El contratista deberá aplicar protocolos y prácticas de seguridad alineadas a las normas ISO/IEC 27001, ISO/IEC 27032 e ISO/IEC 27035, así como a la Ley N.º 29733 – Ley de Protección de Datos Personales y su reglamento.
- La ejecución del servicio deberá realizarse sin interrumpir las operaciones de correo electrónico institucional ni afectar la entregabilidad de los mensajes legítimos.
- El proveedor deberá garantizar la confidencialidad, integridad y disponibilidad de los datos manejados durante la implementación y operación del servicio.

4. REQUISITOS DEL PROVEEDOR

El proveedor deberá acreditar:

4.1. Requisitos mínimos

- Empresa jurídica.
- Contar con Registro Nacional de Proveedores vigente.
- No contar con impedimento para contratar con el estado, según Artículo 30° de la Ley General de Contrataciones Públicas.
- Debe contar con Certificación ISO 27001 e ISO 9001.

4.2. Experiencia del postor

La experiencia del postor en la especialidad tales como Servicio de autenticación de dominio y/o servicio de protección avanzada de correos y/o servicio de protección de marca digital (Digital Risk Protection) servicios o compras de soluciones antimalware o antivirus y/o similares, los cuales se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de diez (10) contrataciones.

4.3. Personal clave.

Como mínimo:
Un (01) Especialista en autenticación de dominio.

- Título en Ingeniería: de Sistemas y/o Computación y Sistemas, y/o de Sistemas e Informática, y/o Informática, y/o Electrónica, y/o Redes y/o Telecomunicaciones y/o Computación y/o Redes y Comunicaciones y/o afines.
- Experiencia profesional mínima de dos (02) años en servicios, tales como: Servicio de antispam, servicios de autenticación de dominios y/o similares la cual será validada con una constancia de trabajo.
- Certificación oficial del fabricante vigente de la plataforma de autenticación del dominio.
- Certificaciones y/o constancias de capacitación en las siguientes materias, los cuales se acreditarán con copia simple de los certificados y/o constancias correspondientes: Fundamentos de Ciberseguridad, Fundamentos de Cómputo Forense, Fundamentos de Ethical Hacking, Gestión de la Ciberseguridad, Gestión de un CyberSOC y Peritaje e Informática Forense.

Actividades:

- Realizar el diagnóstico técnico inicial del dominio institucional y sus registros DNS.
- Elaborar un informe de línea base que identifique el estado actual de SPF, DKIM, DMARC, BIMI, MTA-STS y TLS-RPT.

- Configurar y validar los registros DNS del dominio para asegurar la autenticación correcta de los correos institucionales.
- Implementar las políticas de autenticación en modo de monitoreo y luego en modo restrictivo.
- Validar la correcta alineación entre los registros SPF, DKIM y DMARC.
- Configurar y activar el logo certificado BIMI de la entidad.
- Implementar alertas automáticas ante cambios o anomalías en los registros DNS.
- Supervisar continuamente el funcionamiento de los protocolos de autenticación implementados.
- Analizar los reportes DMARC (rua y ruf) para detectar intentos de suplantación o fuentes no autorizadas.
- Monitorear la reputación del dominio y de las IPs de envío.
- Brindar soporte técnico ante incidencias o alertas detectadas durante la vigencia del contrato.
- Entregar la carta de activación del servicio y los accesos administrativos a nombre de la Entidad.
- Garantizar la confidencialidad, integridad y disponibilidad de la información procesada.

5. PLAZO Y LUGAR DE EJECUCIÓN DEL SERVICIO

5.1. Plazo de implementación

La implementación se realizará en un plazo de hasta diez (10) días calendarios desde el día siguiente de notificada la Orden de Servicio o suscripción de Contrato.

5.2. Plazo del servicio

El servicio a contratar tendrá una vigencia de trescientos sesenta y cinco (365) días calendario y entrará en vigor a partir del día siguiente de culminada la implementación del servicio.

5.3. Lugar

El servicio se ejecutará en las instalaciones de la Sede Central del Ministerio de Trabajo y Promoción del Empleo (MTPE), ubicada en la ciudad de Lima, Av Salaverry N° 655, Jesús María.

6. PRODUCTO O ENTREGABLE A OBTENER

El contratista deberá entregar:

Entregable Único

Dentro de los cinco (05) días calendario de implementado el servicio, el contratista deberá presentar un Informe de la instalación, configuración y puesta en producción de la solución de ciberseguridad DNS, el cual deberá contemplar lo siguiente:

- Acta de conformidad del servicio, emitido por la Oficina General de Estadística y Tecnologías de la Información y Comunicaciones del MTPE.
- Informe detallado de la instalación y despliegue.

- Carta de activación del servicio a nombre de la entidad y por el periodo contratado.
- Relación de contactos para atención de incidentes y cuadro de escalamiento para atenciones comerciales y de reclamos, indicando números de teléfonos, nombres completos y correos electrónicos.

Los entregables serán presentados a través de la Mesa de partes virtual en https://mesadigital360.trabajo.gob.pe/account/login o a través de la ventanilla de la Mesa de Partes de la Oficina de Atención al Ciudadano y Gestión Documentaria, sito en Av. Salaverry N° 655, primer piso Jesús María, en el horario de 8:00 a 16:30 horas.

7. CONFORMIDAD DEL SERVICIO

La conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas. La conformidad será otorgada por la Oficina de Tecnologías de Información y Comunicaciones.

De existir observaciones, LA ENTIDAD las comunica a EL PROVEEDOR, indicando claramente el sentido de estas, otorgándole un plazo para subsanar el cual no debe ser mayor al 30% del plazo del entregable correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL PROVEEDOR no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar a EL PROVEEDOR periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

8. FORMA DE PAGO

El pago se efectuará en una sola armada, previa emisión de la conformidad correspondiente, con la presentación del comprobante de pago y demás documentos exigidos por la normativa vigente.

9. PENALIDADES:

9.1. **Penalidad por mora:** En este caso incluye lo siguiente:

En caso de retraso injustificado en la ejecución de las prestaciones objeto de la contratación, se aplicará automáticamente una penalidad por mora, por cada día de retraso y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40

Penalidades por mora: se aplicará al contratista la penalidad establecida en el artículo 120 del Reglamento de la Ley General de Contrataciones Públicas.

9.2. **Otras penalidades:**

Supuesto	Penalidad
Incumplimiento del plazo de implementación	0.5% del monto contractual por día.
No presentación de informes requeridos	0.1% del monto contractual por día.

10. SEGURIDAD DE LA INFORMACIÓN

El contratista deberá mantener absoluta reserva y confidencialidad respecto de toda la información, documentación, configuraciones, datos y demás elementos a los que tenga acceso durante la ejecución del servicio en el Centro de Datos del Ministerio de Trabajo y Promoción del Empleo.

La información, informes, documentos técnicos, registros, fotografías, diagramas, configuraciones o cualquier otro dato obtenido, generado o proporcionado durante la ejecución del servicio no podrán ser divulgados, reproducidos, transferidos ni utilizados para fines distintos al cumplimiento de las obligaciones contractuales, antes, durante o después de culminada la prestación del servicio, salvo autorización expresa de la Entidad.

Asimismo, el contratista deberá cumplir con la Política de Seguridad de la Información vigente del MTPE, así como con las disposiciones relacionadas con Seguridad Digital, Ciberseguridad y Protección de Datos Personales emitidas por la Presidencia del Consejo de Ministros y la Autoridad Nacional de Protección de Datos Personales.

En caso de detectarse cualquier evento, incidente o vulneración que pudiera comprometer la seguridad de la información, la disponibilidad de los servicios tecnológicos o la infraestructura crítica del Centro de Datos, el contratista deberá comunicarlo de manera inmediata al Oficial de Seguridad y Confianza Digital del Ministerio y al área usuaria correspondiente.

11. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es responsable por la calidad ofrecida y por los vicios ocultos por un plazo no menor de un (1) año contado a partir de la conformidad otorgada por la Entidad. El contrato puede establecer excepciones para bienes fungibles y/o perecibles, siempre que la naturaleza de estos bienes no se adecue a este plazo.

12. RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes podrá resolver el contrato, de conformidad con lo establecido en la Ley N.° 32069 – Ley General de Contrataciones Públicas, su

Reglamento aprobado mediante Decreto Supremo N.° 009-2025-EF y la Directiva N.° 005-2025-MTPE/4, que regula la contratación de bienes y servicios bajo la modalidad de contratos menores en el Ministerio de Trabajo y Promoción del Empleo – Unidad Ejecutora 001 – Oficina General de Administración.

Constituyen causales de resolución contractual las siguientes:

a) Caso fortuito o fuerza mayor que imposibilite la continuación de la contratación.
b) Incumplimiento de las obligaciones contractuales por causa atribuible al contratista.
c) Hecho sobreviniente al perfeccionamiento del contrato menor, distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuidad de la contratación.
d) Incumplimiento de la cláusula anticorrupción y antisoborno.
e) Presentación de documentación falsa, adulterada o con información inexacta en cualquier etapa del proceso de contratación o durante la ejecución contractual.
f) Configuración de la condición de terminación anticipada establecida en el contrato menor u Orden de Servicio.
g) Asimismo, constituye causal de resolución contractual la presentación de información falsa o inexacta en la Declaración Jurada de Prohibiciones e Incompatibilidades prevista en la Ley N.° 31564 – Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público.

En caso de verificarse el incumplimiento de los impedimentos establecidos en el artículo 5 de la referida Ley, corresponderá la aplicación de las sanciones y medidas previstas en la normativa vigente, incluida la inhabilitación para contratar o prestar servicios al Estado, de corresponder.

13. ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del contrato o de la formalización de la Orden respectiva, el Contratista declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de EL MTPE.

Asimismo, el Contratista se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, el Contratista se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito.

En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.
Adicionalmente, el Contratista se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con EL MTPE.

Finalmente, el incumplimiento de las obligaciones establecidas en este acápite, durante la ejecución contractual, otorga a la entidad contratante el derecho de resolver total o parcialmente el contrato.

El Contratista declara conocer los principios, deberes y prohibiciones establecidas en la Ley Nº 27815, Ley del Código de Ética de la Función Pública y otras normas vinculadas a la materia; por lo que su conducta se encuentra acorde a las disposiciones de dicha Ley y normas conexas. En ese sentido, declara someterse a las consecuencias que se deriven de la realización de acciones u omisiones que la vulneren o transgredan.

14. SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resolverán mediante conciliación, con excepción de aquellas que versen sobre nulidad de contrato, conforme a lo dispuesto en el numeral 81.3 del artículo 81 de la Ley N.° 32069, Ley General de Contrataciones Públicas

Sin perjuicio de lo anterior, en caso de no arribar a un acuerdo conciliatorio, las controversias surgidas durante la ejecución del contrato serán resueltas en la vía arbitral o a través de la jurisdicción ordinaria, según el acuerdo de las partes. A falta de acuerdo, dichas controversias serán sometidas a la jurisdicción de los jueces y tribunales del Distrito Judicial de Lima.

15. GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato/orden de servicio u compra y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación se recomienda los siguientes riesgos:

Riesgo	Probabilidad	Impacto	Mitigación
Configuración incorrecta DMARC	Media	Alta	Validación previa y pruebas
Interrupción de correo institucional	Baja	Muy Alta	Implementación gradual
Pérdida de registros DNS	Baja	Alta	Respaldo previo
Falso positivo de	Media	Alta	Política DMARC progresiva

Riesgo	Probabilidad	Impacto	Mitigación
rechazo de correos			
Compromiso de credenciales administrativas	Baja	Alta	MFA obligatorio
Aparición de dominios fraudulentos	Alta	Media	Monitoreo continuo Brand Protection
Caída de plataforma SaaS	Baja	Alta	SLA y redundancia del fabricante