1. OBJETIVO

Establecer los lineamientos y obligaciones en lo referente a privacidad, seguridad de la información y ciberseguridad que deben tenerse en cuenta por parte de contratistas, aliados o proveedores, en adelante “Terceros”, que, con ocasión de una relación contractual, tengan acceso directo o indirecto a activos de información y ciberactivos de OCENSA.

2. PREMISAS Y PRINCIPIOS

OCENSA como parte de su compromiso frente a la protección de la confidencialidad, integridad y disponibilidad de activos de información y ciberactivos de la organización, ha definido dentro de su POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD, el siguiente principio rector:

Establecer lineamientos para la gestión de riesgos relacionados con Terceros y la cadena de suministro, promoviendo prácticas que contribuyan a preservar la seguridad de la información y la continuidad del negocio. Esto incluye la adopción de medidas razonables para conocer y mitigar posibles impactos derivados de las relaciones con Terceros (proveedores, contratistas y aliados), alineando su gestión con los principios de seguridad definidos por la organización.

Acorde a lo anterior, el presente documento establece las premisas y obligaciones mínimas en materia de seguridad de la información, privacidad y ciberseguridad que deberán cumplir los Terceros, que, con ocasión de una relación contractual, tengan acceso directo o indirecto a información, datos personales, sistemas, procesos o activos tecnológicos de OCENSA. Estas disposiciones se definen con base en un enfoque de gestión de riesgos, en la normatividad vigente y en buenas prácticas reconocidas, y tienen como finalidad proteger los activos de información de OCENSA, reducir riesgos legales, operativos y reputacionales, y asegurar un nivel adecuado de control sobre la cadena de suministro, basado en las siguientes premisas:

- Las obligaciones de seguridad, privacidad y ciberseguridad establecidas en el presente documento se definen bajo un enfoque de gestión de riesgos. Su aplicación será determinada según el tipo de servicio, criticidad del Tercero y nivel de riesgo asociado, asegurando un equilibrio entre control, eficiencia operativa y protección de los activos de información.

- Las disposiciones definidas como generales son de obligatorio cumplimiento para todo Tercero, independientemente de su naturaleza (tecnológico o no tecnológico), que tenga acceso directo o indirecto a información, datos personales, sistemas, procesos o activos de OCENSA.

- El Tercero es responsable de implementar y mantener las medidas necesarias para cumplir con las obligaciones aquí definidas y responderá por los actos u omisiones de su personal, subcontratistas y cadena de suministro, sin perjuicio de las responsabilidades legales y contractuales aplicables.

- El presente documento se fundamenta en la normatividad vigente aplicable y en estándares y buenas prácticas reconocidas de seguridad de la información, privacidad y ciberseguridad.

- La gestión de la seguridad en Terceros se concibe como un proceso continuo, integrado al ciclo de vida del Tercero, desde su selección y contratación hasta la operación, seguimiento, renovación y terminación. En este contexto, las obligaciones definidas deberán ser verificables, soportadas en evidencias razonables y sujetas a mecanismos de control, auditoría y mejora continua, permitiendo la toma de decisiones informadas a nivel táctico y estratégico.

- Es obligación del Tercero asegurar los soportes y evidencias correspondientes a la ejecución de los controles y el cumplimiento de las actividades derivadas de los requisitos de seguridad de la información y ciberseguridad, los cuales deben estar disponibles en cualquier momento que OCENSA lo requiera o decida hacer un monitoreo sobre este cumplimiento.

- Las obligaciones aquí definidas, así como las políticas, estándares o procedimientos asociados, podrán ser actualizadas, reforzadas o ajustadas por OCENSA en función de cambios normativos, tecnológicos, del entorno o en el perfil de riesgo.

- El presente documento y sus anexos serán parte integral del contrato y serán aplicables durante la vigencia del contrato y subsistirá aún después de su terminación, por el tiempo legalmente exigible.

2.1. ALCANCE

- Estas obligaciones y lineamientos aplican para los Terceros de Ocensa que tengan acceso directo o indirecto a activos de información (información y datos) y ciberactivos (activos tecnológicos) de OCENSA.
- Este documento define los controles en material de privacidad, seguridad de la información y ciberseguridad para Terceros de Ocensa. Estos controles serán extendidos a sus Subcontratistas (en caso de que Ocensa hubiese aprobado previamente la Subcontratación), y por lo cual, sin lugar a excepción, cualquier subcontrato incluirá y cumplirá los mismos controles obligatorios del contrato principal.
- Sirve como referente para evaluar la idoneidad de los Terceros en función de su desempeño en materia de Seguridad de la información y Ciberseguridad.

3. DESCRIPCIÓN

3.1. OBLIGACIONES GENERALES EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Los siguientes requerimientos aplican de manera transversal para todo contrato según el alcance definido en este documento:

Cumplimiento Regulatorio y Normativo

El Tercero se obliga a cumplir de manera estricta y permanente con toda la normatividad legal, reglamentaria y regulatoria aplicable, tanto de carácter nacional como internacional, relacionada con la prestación del servicio, incluyendo, sin limitarse a, normas sobre protección de datos personales, seguridad de la información, ciberseguridad, delitos informáticos, propiedad intelectual y uso adecuado de tecnologías de la información, según resulte aplicable al objeto contractual.

Asimismo, el Tercero se compromete a cumplir con las políticas, estándares, procedimientos, lineamientos y controles internos de OCENSA en materia de privacidad, gestión de información, seguridad de la información y ciberseguridad, los cuales le serán de obligatorio cumplimiento, incluyendo mas no limitándose a:

- SCI-POL-002 POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD
- SCI-STD-003 ESTANDAR SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD
- SCI-POL-001 POLITICA DECLARACION DE TRATAMIENTO DE DATOS PERSONALES
- SCI-STD-001 ESTANDAR TRATAMIENTO DE DATOS PERSONALES
- SCI-FOR-002 FORMATO ACUERDO DE TRANSMISION TRANSFERENCIA Y ACCESO DE DATOS PERSONALES

Protección y gestión de la información

Toda la información generada, modificada, transferida y almacenada dentro del desarrollo de los procesos y actividades de la organización y desarrollo del objeto contractual, es propiedad de OCENSA, salvo excepciones legales o contractuales en los que la propiedad es del Tercero y esto se encuentre claramente especificado a nivel contractual.

El Tercero se obliga a implementar, mantener y mejorar de forma continua medidas técnicas, organizativas y administrativas apropiadas para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de toda la información, datos personales, documentos, sistemas y activos de información de OCENSA a los que tenga acceso, directa o indirectamente, durante la ejecución del contrato. Dicha información será en todo momento propiedad exclusiva de OCENSA, o de los Terceros legítimos que éste determine, sin que el presente contrato implique cesión, licencia, transferencia o reconocimiento de derecho alguno a favor del Tercero, salvo lo estrictamente necesario para la correcta prestación del servicio y bajo instrucciones expresas de OCENSA.

El Tercero actuará únicamente como custodio y responsable de la protección y uso adecuado de la información, comprometiéndose a no copiarla, reproducirla, divulgarla, explotarla, analizarla, reutilizarla ni transferirla, total o parcialmente, para fines distintos a los previstos contractualmente. Asimismo, deberá restringir el acceso a la información conforme al principio de mínimo privilegio, garantizar su uso adecuado por parte de su personal y subcontratistas autorizados, y adoptar controles que prevengan fuga, pérdida, acceso no autorizado, alteración, destrucción o uso indebido, manteniendo dichas obligaciones vigentes incluso después de la terminación del contrato.

El Tercero deberá acatar los lineamientos de gestión de información de OCENSA y gestionar en los repositorios establecidos por OCENSA para tal fin.

El Tercero debe informar a cada uno de sus empleados o colaboradores debidamente autorizados, de los niveles de clasificación de la Información definidos por OCENSA y de la existencia de acuerdos de confidencialidad con OCENSA. Igualmente, el Tercero debe instruir a quién reciba la información o documentos, acerca de las medidas de protección y mecanismos para manejar la información y la obligatoriedad de no utilizarla sino para los temas necesarios para el desarrollo del acuerdo suscrito entre OCENSA y el Tercero quién será enteramente responsable por cualquier uso inadecuado de la información suministrada por OCENSA.

El Tercero será responsable ante OCENSA por cualquier daño o perjuicio que se derive del hecho de haber hecho uso no autorizado de la información o de la violación de los principios de integridad, disponibilidad o confiabilidad de esta.

Una vez finalice el periodo establecido para la prestación del servicio, el Tercero deberá hacer entrega de la información correspondiente en el formato y estructura acordada previamente entre las partes. Así mismo deberá entregar todas las copias de información que tenga en su poder.

Una vez finalizada la relación contractual, el Tercero deberá proceder con la devolución y/o eliminación de la información, dentro de un plazo no superior a 1 mes calendario o dentro del periodo de liquidación, incluyendo copias, respaldos o reproducciones de cualquier tipo, salvo que exista una obligación legal de conservación. En caso de que exista una obligación legal de conservación, deberá mantener la información bajo las mismas condiciones de seguridad y confidencialidad y por el tiempo estrictamente necesario, informando de ello a OCENSA. El Tercero emitirá certificación o constancia escrita de la devolución o eliminación dentro del plazo anteriormente estipulado y mantendrá la confidencialidad aun después de la terminación.

Tercero se obliga a cumplir las demás obligaciones estipuladas en la minuta contractual y relacionada con el manejo y confidencialidad de la información.

Las obligaciones de confidencialidad, seguridad de la información y protección de datos personales establecidas en el contrato y sus anexos permanecerán vigentes aun después de su terminación, sin limitación temporal, independientemente de la causa de finalización.

Privacidad y Datos personales

El Tercero se obliga a cumplir de manera estricta con la normativa vigente en materia de protección de datos personales, garantizando el respeto de los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. En desarrollo del contrato, el Tercero deberá abstenerse de realizar cualquier tratamiento[1] de datos personales que no se encuentre debidamente autorizado o que exceda el objeto contractual, y deberá implementar medidas técnicas, administrativas y organizativas razonables para prevenir accesos no autorizados, pérdida, alteración, divulgación o uso indebido de los datos personales a los que tenga acceso, manteniendo dichas obligaciones durante la vigencia del contrato y con posterioridad a su terminación.

En la medida en que, para la ejecución del contrato, el Tercero acceda, almacene, use, procese, transmita o administre datos personales por cuenta de OCENSA y siguiendo sus instrucciones, se entenderá que actúa en calidad de ENCARGADO DEL TRATAMIENTO, y OCENSA como RESPONSABLE, conforme a la legislación aplicable y lo establecido en la minuta del contrato. En dicha condición, el Tercero se obliga a tratar los datos personales únicamente conforme a las instrucciones documentadas de OCENSA, a no destinarlos a fines propios o distintos a los autorizados, a no transferirlos o comunicarlos a Terceros sin autorización previa y expresa, a garantizar la confidencialidad de su personal y a devolver o eliminar de forma segura los datos personales al finalizar el contrato, certificando dicho proceso cuando sea requerido.

El Tercero se obliga a cumplir las demás obligaciones estipuladas en la minuta contractual y relacionadas con el tratamiento de datos personales, así como lo estipulado en la POLITICA DECLARACION DE TRATAMIENTO DE DATOS PERSONALES, el ESTANDAR DE TRATAMIENTO DE DATOS PERSONALES y el Anexo ACUERDO DE TRANSMISIÓN, TRANSFERENCIA Y ACCESO DE DATOS

[1] Se entiende como tratamiento de datos personales el acceso, almacenamiento, uso, procesamiento, transmisión transferencia o administración de datos personales

Soluciones Tecnológicas, servicios Nube y Gestión de Datos

En caso de que el Tercero , como parte del alcance del contrato o como valor agregado, suministre, implemente o ponga a disposición de OCENSA cualquier solución tecnológica, incluyendo servicios en la nube (IaaS, PaaS, SaaS), aplicaciones, plataformas o infraestructura, se obliga a garantizar que dichas soluciones cumplan con requisitos mínimos de seguridad de la información, ciberseguridad y protección de datos personales, acordes con la naturaleza del servicio y el nivel de criticidad del mismo. El Tercero deberá asegurar que la solución se encuentre debidamente licenciada, configurada de forma segura, actualizada y sujeta a controles adecuados de acceso, disponibilidad, respaldo y monitoreo.

Asimismo, el Tercero deberá garantizar la reversibilidad y portabilidad de la información, asegurando que, al finalizar el contrato o cuando OCENSA lo requiera, los datos puedan ser extraídos**,** transferidos o migrados en formatos estándar y utilizables, sin afectación a su integridad ni a la continuidad del servicio. El Tercero deberá informar y acordar previamente con OCENSA la localización de los datos, incluyendo países o regiones donde se almacenen o procesen, y no podrá modificar dicha localización sin notificación y autorización de OCENSA.

Para servicios clasificados como críticos o de alto impacto, el tercero deberá garantizar la trazabilidad, integridad, consistencia y auditabilidad de la información, mediante la implementación de mecanismos formales que aseguren:

- Registro completo y consistente de eventos (logs) con identificadores técnicos que permitan reconstruir la trazabilidad de las operaciones, así como su preservación, retención definida e inmutabilidad.
- Extracciones certificadas y verificables cuando sean requeridos por Ocensa como parte de la ejecución de controles, análisis forenses o auditorias, incluyendo controles de integridad (hash), consistencia (conteos), identificación única, contexto temporal, evidencia de inmutabilidad (IPE/manifest, sellado de tiempo) y capacidad de exportación de la información.
- Definición y disponibilidad de un catálogo de logs y reportes
- Disponibilidad de reportes y consultas auditables, certificadas, controladas y versionadas.
- Documentación técnica actualizada, incluyendo diccionario de datos, definición de eventos/estados y guías de interpretación para auditoría.
- Mecanismos de validación y reconciliación de la información, que permitan verificar la consistencia entre datos, eventos y extracciones.

El tercero deberá permitir la verificación, auditoría y validación de estos controles por parte del contratante, así como cumplir con los tiempos y condiciones definidos para la entrega de información.

En todo caso, la implementación, uso o puesta en producción de cualquier solución tecnológica o servicios Cloud, deberá contar con la validación previa y expresa del área de Tecnología de OCENSA, quien evaluará aspectos de arquitectura, seguridad, compatibilidad y riesgos, como condición obligatoria para su implementación y uso.

Cumplimiento de estándares y certificaciones de seguridad

El proveedor deberá cumplir con prácticas y estándares reconocidos de seguridad de la información, acordes con la clasificación de criticidad del servicio (de acuerdo con el PROCEDIMIENTO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS).

Para proveedores clasificados como de alto impacto, especialmente aquellos que involucren el procesamiento, almacenamiento o transmisión de información en entornos de nube, el proveedor deberá contar y mantener vigentes certificaciones o informes de aseguramiento independientes tales como SOC 2 Tipo II e ISO 27001, que evidencien la implementación y operación efectiva de controles de seguridad.

El proveedor deberá garantizar que las certificaciones o informes de aseguramiento (SOC, ISO u otros) cubran integralmente el servicio contratado, incluyendo infraestructura, plataformas, aplicaciones, procesos operativos y controles de protección de la información. El proveedor deberá suministrar los informes completos que permitan validar el alcance, controles implementados y exclusiones, así como declarar explícitamente los componentes cubiertos y no cubiertos. En caso de existir elementos fuera del alcance, el proveedor deberá presentar controles equivalentes.

Para proveedores clasificados como medios, se podrá requerir evidencia de controles de seguridad implementados, certificaciones parciales o evaluaciones equivalentes, según la naturaleza del servicio.

Subcontratación y Cadena de Suministro

Teniendo en cuenta que la minuta del contrato prohíbe la cesión y subcontratación parcial o total del contrato, salvo que exista autorización previa y expresa de parte de OCENSA, solo en estos casos se entenderá autorizado el acceso a la información por parte del o los Terceros en cuestión.

En caso de autorizarse la subcontratación, y en especial aquellos contratos categorizados como riesgo medio y alto (de acuerdo con el PROCEDIMIENTO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS) o con tratamiento y gestión de datos personales, el Tercero deberá garantizar que dichos Terceros subcontratados cumplan, como mínimo, con las mismas obligaciones de seguridad de la información o equivalentes, protección de datos personales, ciberseguridad y confidencialidad establecidas en el contrato y en este anexo, siendo el Tercero responsable directo y solidario por cualquier incumplimiento, incidente o daño ocasionado por su cadena de suministro.

Asimismo, el Tercero se obliga a implementar mecanismos razonables de evaluación, control y supervisión de riesgos asociados a su cadena de suministro, incluyendo la selección diligente de subcontratistas, la gestión de accesos, la revocación oportuna al finalizar la relación contractual y la notificación inmediata a OCENSA de cualquier evento que pueda afectar la seguridad, continuidad o integridad de la información. Las obligaciones aquí previstas subsistirán aun después de la terminación del contrato.

Continuidad de los Servicios

El Tercero se obliga a adoptar medidas razonables para asegurar la continuidad, disponibilidad y resiliencia de los servicios objeto del contrato, implementando medidas técnicas, organizativas y operativas razonables para prevenir interrupciones, fallas o degradaciones que puedan afectar a OCENSA.

Para ello, deberá contar con mecanismos y estrategias de contingencia/continuidad, respaldo y recuperación, acordes con la naturaleza y criticidad del servicio, que permitan restablecer la operación ante eventos que puedan afectarla. El Tercero deberá probar y mantener actualizados dichas estrategias de forma periódica y notificar oportunamente a OCENSA cualquier evento que pueda comprometer la continuidad del servicio.

Gestión de Incidentes de Seguridad

El Tercero deberá contar con mecanismos para la gestión de incidentes de seguridad de la información y ciberseguridad, que permita la identificación, análisis, contención, erradicación, recuperación y reporte de eventos que afecten o puedan afectar la confidencialidad, integridad o disponibilidad de la información de los servicios de OCENSA.

El Tercero se obliga a notificar a OCENSA sin dilación indebida y, en todo caso, dentro de las veinticuatro (24) horas siguientes a tener conocimiento, sobre cualquier incidente de seguridad que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de los datos, información o los servicios contratados o a los cuales tiene acceso. El CONTRATISTA deberá adoptar de manera inmediata las medidas técnicas, administrativas y organizativas necesarias para contener, gestionar y remediar el incidente, así como colaborar plenamente con OCENSA en la investigación de los hechos, el análisis de sus causas, la implementación de acciones correctivas y el cumplimiento de las obligaciones legales o regulatorias aplicables. En todo caso, el CONTRATISTA será responsable de los incidentes que se originen por el incumplimiento de las obligaciones de seguridad, confidencialidad o privacidad establecidas en el presente documento, en el contrato o en la normativa aplicable.

Premisas para el Acceso a la Información y Recursos de OCENSA

El Tercero deberá utilizar los recursos de información y tecnología de OCENSA exclusivamente para los propósitos necesarios para el cumplimiento del objeto contractual suscrito.

El Tercero se obliga a gestionar los accesos e identidades de su personal y de cualquier Tercero autorizado que participe en la ejecución del contrato, garantizando que el acceso a la información, sistemas y recursos de OCENSA se otorgue únicamente a personas debidamente autorizadas, conforme a los principios de mínimo privilegio y temporalidad.

Todo acceso a los recursos tecnológicos y servicios de OCENSA y otorgados al Tercero debe ser:

- Justificado, documentado y aprobado
- Limitado, temporal y proporcional a la necesidad del servicio.
- Se debe aplicar el principio de mínimo privilegio

El Tercero se obliga a notificar de forma inmediata todas las novedades que se presenten (especialmente ante cambios de rol o desvinculación del personal con acceso a información y recursos de la organización) a fin de revocar de forma oportuna dichos accesos y será responsable por cualquier uso indebido, no autorizado o negligente de las credenciales y accesos otorgados en el marco del contrato.

El acceso remoto a los recursos de OCENSA debe hacerse mediante métodos seguros (VPN corporativa, autenticación multifactorial, cifrado de comunicaciones). En caso de servicios contratados en el que se requiera una conexión directa hacia los recursos de OCENSA, el Tercero deberá contar con una conexión segura y dedicada, garantizando en todo momento la disponibilidad, capacidad y seguridad de dicha conexión.

El Tercero será responsable de garantizar que los equipos de cómputo, dispositivos móviles u otros activos tecnológicos que suministre a su personal para la ejecución del servicio cuenten con medidas básicas de seguridad de la información, incluyendo la eliminación de privilegios administrativos para

usuarios finales, controles de acceso adecuados, control de aplicaciones mecanismos de protección contra software malicioso, gestión de parches y actualizaciones, firewall activo y restricciones sobre dispositivos externos. Asimismo, el Tercero deberá asegurar que todo el software instalado o utilizado en dichos equipos sea legal, original y debidamente licenciado, manteniéndolo actualizado conforme a las recomendaciones del fabricante.

El Tercero adoptará medidas para prevenir el uso no autorizado, la pérdida, el robo o el acceso indebido a la información de OCENSA desde estos equipos, siendo responsable por los incidentes de seguridad o contingencias legales que se deriven del uso inadecuado o del incumplimiento de las obligaciones aquí establecidas.

El suministro de equipos de cómputo por parte de OCENSA a Terceros y de las herramientas de seguridad y respaldo de información, se podrá dar para casos excepcionales, en donde se identifique la gestión de información altamente sensible y sea necesario el control total sobre la misma.

Así mismo OCENSA se reserva el derecho de solicitar y tener el control y administración de los equipos de cómputo asignados por el Tercero en caso de que se identifique información altamente sensible dentro del alcance del contrato

El Tercero se obliga a acatar las demás responsabilidades que devengan del acceso y uso de los recursos y activos de información descritas en el ESTANDAR DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Cultura y corresponsabilidad

El Tercero debe fomentar al interior de su organización una cultura de seguridad y corresponsabilidad entre todos los colaboradores, promoviendo comportamientos seguros, éticos y alineados con las políticas establecidas. Para esto ha de implementar prácticas y mecanismos de capacitación y sensibilización en Privacidad, Seguridad de la información y ciberseguridad.

Así mismo debe asegurar el conocimiento por parte de sus empleados y Terceros que intervienen en la prestación del servicio de la POLÍTICA Y EL ESTÁNDAR DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE OCENSA.

Derecho de verificación y auditoría

OCENSA se reserva, y el Tercero reconoce recíprocamente, el derecho de verificar y/o auditar en cualquier momento y de manera previamente informada, directamente o a través de Terceros debidamente autorizados, el cumplimiento de las obligaciones establecidas en el contrato, el presente documento y demás anexos por parte del Tercero. El Tercero deberá mantener disponibles para verificación evidencias razonables de cumplimiento. OCENSA podrá solicitar al Tercero evidencias, reportes, certificaciones, autoevaluaciones o resultados de auditorías relacionadas con seguridad de la información, protección de datos personales y ciberseguridad. El Tercero se compromete a remediar las situaciones identificadas en los tiempos acordados, de acuerdo con la criticidad y riesgos asociados.

3.2. OBLIGACIONES ADICIONALES EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Adicional a los requerimientos generales descritos anteriormente y que aplican de manera transversal, para aquellos contratos categorizados como riesgo *medio y alto* (De acuerdo con el PROCEDIMIENTO DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS) *y con tratamiento de datos personales*, se deberá diligenciar el anexo **VERIFICACIÓN CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS,** el cual será parte integral del contrato.

En caso de que el contrato incluya el tratamiento de **datos personales sensibles o de menores de edad, información clasificada o reservada**, adicional a lo estipulado en las OBLIGACIONES GENERALES del presente documento y el anexo de VERIFICACIÓN CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS, el Tercero deberá tener en cuenta los siguientes requisitos de seguridad de obligatorio cumplimiento:

- El Tercero garantizará la confidencialidad estricta de esta información, obligación extensiva a sus empleados, contratistas, subcontratistas y Terceros autorizados, durante la vigencia del contrato y con posterioridad a su terminación.
- El Tercero implementará medidas técnicas, organizacionales y administrativas proporcionales al riesgo, acordes con la naturaleza sensible de la información tratada, incluyendo como mínimo controles de acceso, cifrado, monitoreo, gestión de vulnerabilidades, respaldo de información y continuidad del servicio.
- El Tercero garantizará que todos los equipos de cómputo, dispositivos portátiles o estaciones de trabajo desde los cuales se acceda, procesen, almacene o gestione datos personales sensibles o de menores de edad, información clasificada o reservada cumplirán, como mínimo, con los siguientes requisitos:

  Control de acceso y autenticación
  - Acceso restringido mediante usuarios individuales e intransferibles.
  - Política de uso de contraseñas robustas
  - Autenticación multifactor (MFA) para el acceso a sistemas
  - Bloqueo automático de sesión por inactividad.
  - Restricción de uso de cuentas genéricas o compartidas.

  Protección del dispositivo
  - Sistemas operativos legales, licenciados y soportados por el fabricante.
  - Cifrado del disco duro o del medio de almacenamiento.
  - Restricción de permisos de administrador local o privilegios elevados para los usuarios finales en los equipos de cómputo.
  - Controles para la Instalación únicamente de software autorizado.

  Protección contra malware y amenazas
  - Instalación y actualización permanente de antivirus / EDR o XDR.
  - Protección activa contra malware, ransomware y accesos no autorizados.
  - Escaneos periódicos y monitoreo de comportamiento sospechoso.

  Gestión de actualizaciones y vulnerabilidades
  - Aplicación oportuna de parches de seguridad del sistema operativo y aplicaciones.
  - Restricción de uso de software obsoleto o sin soporte.
  - Gestión de vulnerabilidades críticas.

Conectividad y redes

- Acceso remoto únicamente mediante canales seguros y cifrados (VPN).
- Prohibición de herramientas de acceso remoto no autorizadas.
- Prohibición de acceso a información desde redes públicas o no confiables sin protección.
- Firewall habilitado y mecanismos de protección de red del sistema

Uso de dispositivos externos

- Restricción o control del uso de USB, discos externos u otros medios removibles. En caso de autorización, estos deberán estar cifrados.
- Prohibición de copias no autorizadas de información.

Registro, monitoreo y trazabilidad

- Registro de accesos, actividades y eventos relevantes.
- Conservación de logs conforme a la criticidad del tratamiento.
- Capacidad de trazabilidad ante incidentes.

Uso exclusivo y controlado

- Los equipos utilizados para el tratamiento de datos sensibles o de menores de edad deberán estar bajo control exclusivo del Tercero.
- Prohibición de uso de equipos personales no autorizados (BYOD), salvo autorización expresa del Tercero y cumplimiento evidenciable de los mismos controles de seguridad mencionados anteriormente.

3.3. DOCUMENTOS DE REFERENCIA

- SCI-POL-002 POLITICA DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD
- SCI-STD-003 ESTANDAR SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD
- SCI-POL-001 POLITICA DECLARACION DE TRATAMIENTO DE DATOS PERSONALES
- SCI-STD-001 ESTANDAR TRATAMIENTO DE DATOS PERSONALES
- SCI-FOR-002 FORMATO ACUERDO DE TRANSMISION TRANSFERENCIA Y ACCESO DE DATOS PERSONALES
- SCI-FOR-003 FORMATO VERIFICACIÓN CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN TERCEROS

4. CONTROL DE ACTUALIZACIONES

VERSIÓN	FECHA	DESCRIPCIÓN
0	30/04/2026	Creación del Estándar

EVELIN JIMENEZ
Profesional Sr de control y seguridad de la información
Revisó

OLFER LEON
Experto Ciberseguridad
Revisó

YULIETH ANGARITA
Jefe de Tecnología
Aprobó