



Normativa para salvaguardar el secreto de las telecomunicaciones de abonados y usuarios

1ra Edición - Enero 2026

Índice

Contenido

1.	Introducción	3
2.	Objeto	3
3.	Ámbito de aplicación	3
4.	Contenido.....	3
4.1.	Definiciones	3
4.2.	Medidas de Protección.....	4
4.2.1.	Activos de Información Protegida.....	4
4.2.2.	Pautas Generales de Seguridad	5
4.2.3.	Estándares Mínimos de Seguridad	6
4.2.4.	Análisis y Gestión de Riesgos	6
4.2.5.	Medidas Técnicas.....	7
4.2.6.	Medidas Organizativas	8
4.3.	Organización interna	9
4.3.1.	Principio de corresponsabilidad.....	9
4.3.2.	Control Interno.....	10
4.4.	Obligaciones y responsabilidades	12
4.4.1.	Obligaciones de los trabajadores	12
4.4.2.	Obligaciones de los Proveedores	13
4.4.3.	Obligaciones específicas de las áreas.....	13
4.5.	Consecuencias de su incumplimiento	17
5.	Entrada en vigor	17
6.	Disposiciones complementarias	17

Versión	Responsable	Fecha	Aprobación Directorio
1	Gerencia de Regulación y Asuntos Públicos	Enero 2026	20 de enero 2026

1. Introducción

Integratel Perú S.A.A. (en adelante, “Integratel”), en su condición de concesionaria de servicios públicos de telecomunicaciones, está comprometida con garantizar la confidencialidad de las comunicaciones de sus abonados y usuarios.

Reafirmando dicho compromiso, se aprueba la presente Normativa para salvaguardar el Secreto de las Telecomunicaciones de Abonados y Usuarios (en adelante, la “Normativa”) para velar y regular el estricto cumplimiento de la legislación vigente sobre el secreto de las telecomunicaciones¹ (en adelante la “Legislación Vigente”) y los contratos de concesión que tiene celebrados Integratel con el Estado peruano.

2. Objeto

Establecer las normas, criterios, medidas de protección, obligaciones y responsabilidades que permitan a Integratel salvaguardar el derecho a la inviolabilidad y al secreto de las telecomunicaciones de sus abonados y usuarios.

3. Ámbito de aplicación

La presente Normativa es de observancia obligatoria para todos los miembros del Directorio y trabajadores de Integratel. Asimismo, alcanza a los Proveedores con los que Integratel se vincule y que tengan acceso a Activos de Información Protegida.

4. Contenido

4.1. Definiciones

- a) **Abonado:** persona natural o jurídica que ha celebrado un contrato de servicio de telecomunicaciones con Integratel.
- b) **Activos de Información Protegida:** activos críticos de información que se encuentran comprendidos dentro del ámbito de protección del Secreto de las Telecomunicaciones.
- c) **Áreas de Negocio Responsables:** aquellas áreas de Integratel que deciden sobre la finalidad, contenido y uso de los Activos de Información Protegida. Se encuentran vinculadas principalmente con operación y mantenimiento de las

¹ Constitución Política del Perú, Texto Único Ordenado de la Ley de Telecomunicaciones y su Reglamento, Resolución Ministerial N° 111-2009-MTC/03 - Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales y regula las acciones de supervisión y control, Ley 27336 - Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones, Código Penal y las que las modifiquen o complementen.

redes de telecomunicaciones, manejo de sistemas, facturación y servicio al cliente. Serán las responsables de los Activos de Información Protegida a su cargo.

- d) **Medidas de Protección:** medidas técnicas y organizativas de carácter preventivo o reactivo, físicas o lógicas, que deben ser adoptadas, tanto en la Planta Interna como Planta Externa, para evitar o mitigar el riesgo de vulneración al Secreto de las Telecomunicaciones.
- e) **MTC:** Ministerio de Transportes y Comunicaciones, quien es la autoridad competente para velar por el cumplimiento de las obligaciones relativas al Secreto de las Telecomunicaciones.
- f) **Planta Externa:** conjunto de construcciones, cables, instalaciones, equipos y dispositivos que se ubican fuera de los edificios de la Planta Interna hasta el terminal de distribución. Será aérea, cuando los elementos que conforman la Planta Externa estén fijados en postes o estructuras. Será subterránea, cuando los elementos que la conforman se instalan en canalizaciones, cámaras, ductos y conductos. Será inalámbrica, cuando los elementos que la conforman se instalan en estaciones de acceso para permitir las comunicaciones inalámbricas fijas o móviles.
- g) **Planta Interna:** conjunto de equipos o instalaciones que se ubican dentro de la edificación que alberga la central, cabecera o nodo del servicio de telecomunicaciones. Incluye los equipos de los sistemas de conmutación, sistemas de transmisión y sistemas informáticos (bases de datos, aplicativos, procesos).
- h) **Proveedores:** persona natural o jurídica que presta algún servicio a Integratel y que tenga o pueda tener acceso a Activos de Información Protegida de la Compañía.
- i) **Secreto de las Telecomunicaciones:** derecho fundamental de toda persona a que sus comunicaciones no sean vulneradas. Genera la obligación en Integratel de adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad de las comunicaciones que se cursen a través de sus redes. Se atenta contra este derecho cuando una persona que no es quien origina ni el destinatario de la comunicación, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, divulga, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación o de los medios que la soportan o transmiten, salvo las excepciones en la Legislación Vigente².
- j) **Usuario:** toda persona natural o jurídica que hace uso de los servicios públicos de telecomunicaciones ofrecidos por Integratel, sin ser necesariamente el abonado.

4.2. Medidas de Protección

4.2.1. Activos de Información Protegida

² Como excepción, las comunicaciones o sus instrumentos sólo podrán ser abiertos, incautados, interceptados o intervenidos por mandato motivado del juez con las garantías previstas en la Legislación Vigente.

Los Activos de Información Protegida son los siguientes:

- a) El contenido de cualquier comunicación, de voz o de datos, en tiempo real o histórico, cursado a través de las redes de telecomunicaciones u otros medios que la tecnología permita.
- b) La identificación en tiempo real o histórico de las celdas que brindan cobertura a una línea telefónica.
- c) El origen, destino, realización, curso o duración de una comunicación.
- d) La información del tráfico o consumo de datos de internet de un Abonado o Usuario.
- e) Los datos codificados y decodificados de los registros de llamadas, en tiempo real o histórico.
- f) El detalle de los mensajes de texto (SMS y MMS) entrantes y salientes, en tiempo real o histórico.
- g) El registro en tiempo real o histórico de las asignaciones de direcciones IP asociadas al servicio de acceso a Internet del Abonado o Usuario, que asegure trazabilidad.
- h) Los documentos en soporte físico o digital y bases de datos que contengan la información referida anteriormente, así como aquellos que fueran elaborados para la prestación de servicios de telecomunicaciones.
- i) Cualquier otra información que determine y formalice el MTC u autoridad competente.

La lista precedente no es exhaustiva ni limitativa. Ante alguna duda sobre el ámbito de protección del Secreto de las Telecomunicaciones, deberá solicitarse el apoyo al área de Regulación.

4.2.2. Pautas Generales de Seguridad

Ante los Activos de Información Protegida, Integratel deberá tener en cuenta las siguientes pautas generales de seguridad:

- a) **Autenticación:** implica contar con mecanismos para corroborar que una entidad (persona, dispositivos, servicios y/o aplicaciones) tiene efectivamente la identidad que pretende. Incluye verificar que no se trata de un caso de usurpación de identidad o reproducción no autorizada de una comunicación anterior.
- b) **No repudio:** implica contar con la capacidad de evitar que una entidad (persona, dispositivos, servicios y/o aplicaciones) pueda negar haber realizado una acción en etapas posteriores. Supone la creación de pruebas que podrían ser utilizadas para demostrar la falsedad de un argumento.
- c) **Confidencialidad:** implica contar con mecanismos para que los Activos de Información Protegida no se divulguen o pongan a disposición de individuos, entidades y procesos no autorizados.

- d) **Control de Acceso:** implica contar con mecanismos y sistemas para asegurar que solo el personal o los dispositivos autorizados puedan acceder a los locales, ambientes, elementos de red, información almacenada en bases de datos, flujos de información, sistemas, aplicaciones u otros servicios de información con acceso restringido, tanto en la Planta Interna como Planta Externa.
- e) **Alarmas de Seguridad:** implica contar con sistemas y/o elementos de seguridad pasivos para detectar una intrusión, mediante la generación de una señal de alerta o advertencia.

4.2.3. Estándares Mínimos de Seguridad

Las Medidas de Protección a adoptarse deberán cumplir como mínimo con los estándares establecidos en la Norma Técnica Peruana NTP-ISO/IEC 27001. Asimismo, deberán guiarse de las recomendaciones vigentes en materia de seguridad de la información en las telecomunicaciones de entidades especializadas como la Unión Internacional de Telecomunicaciones, entre otras.

4.2.4. Análisis y Gestión de Riesgos

Para determinar las Medidas de Protección idóneas que correspondan a los Activos de Información Protegida, se deben realizar análisis de riesgos de seguridad de manera periódica para los entornos objetivo.

Los Activos de Información Protegida, junto a los servicios, procesos, aplicaciones, sistemas, redes, ambientes, equipos y otros que los albergan, forman parte del entorno objetivo de los referidos análisis de riesgos de seguridad.

Las Áreas de Negocio Responsables, dentro del marco de sus funciones operativas y en su condición de propietarias de los Activos de Información Protegida y de los riesgos de seguridad vinculados, tienen la responsabilidad de impulsar la realización de análisis de riesgos para los entornos objetivo, para lo que deben:

- Identificar los principales riesgos de vulneración de los Activos de Información Protegida, a su cargo.
- Evaluar los riesgos considerando su probabilidad, así como su impacto cualitativo y/o cuantitativo, para posteriormente priorizarlos con el apoyo de indicadores y métricas.
- Gestionar la implementación de las Medidas de Protección frente a los riesgos identificados.
- Realizar un seguimiento de la evolución de los riesgos y de los planes de acción frente a los mismos.

El área de Seguridad brindará soporte a las Áreas de Negocio Responsables para la realización de los análisis de riesgos de seguridad que correspondan.

Este soporte abarcará tres frentes fundamentales: **Seguridad Física**, enfocada en la protección de personas, instalaciones y activos tangibles; **Seguridad Lógica**, orientada a salvaguardar sistemas, redes y accesos tecnológicos; y **Seguridad de la información**, centrada en garantizar la confidencialidad, integridad y disponibilidad de la información.

Este enfoque integral permitirá a las Áreas de Negocio Responsables identificar y gestionar de manera más efectiva las vulnerabilidades y amenazas identificadas.

4.2.5. Medidas Técnicas

En función a los riesgos identificados en el análisis de riesgos indicado en el numeral anterior, las Áreas de Negocio Responsables deben adoptar e implementar medidas de control de carácter técnico para la protección de los Activos de Información Protegida. Estas medidas deben ser determinadas por el área de Seguridad, y deben poder garantizar un nivel de seguridad adecuado al riesgo identificado.

Las medidas técnicas que se detallan a continuación no deben ser entendidas como únicas, siendo las Áreas de Negocio Responsables las llamadas a adoptar, implementar y/o coordinar con las áreas competentes las medidas de protección complementarias que resulten apropiadas en cada caso, según determine el área de Seguridad:

- a) Sistemas de control de acceso en puertas internas y externas para garantizar que sólo el personal debidamente autorizado, acceda a locales, ambientes, elementos de red, información almacenada en bases de datos, flujos de información, sistemas, aplicaciones u otros servicios de información con acceso restringido, tanto en Planta Interna como Planta Externa. Además, deben permitir detectar accesos no autorizados, registrar y revisar eventos críticos realizados por los usuarios en los sistemas.
- b) Sistemas de identificación de trabajadores o personal autorizado, así como sus niveles de acceso (gestión de accesos y gestión de privilegios). Para la Planta Interna se empleará tarjetas magnéticas y/o sistemas biométricos u otros identificadores cuyo nivel de seguridad y confiabilidad sea similar o superior.
- c) Mecanismos de seguridad física o electrónica en puertas, ventanas, perímetros y en ambientes internos o externos, para detectar y demorar actos malintencionados, como intrusiones, hurtos y/o robos de Activos de Información Protegida, hasta la llegada de los elementos de respuesta. Los siguientes elementos de la Planta Externa y Planta Interna contarán con mecanismos de seguridad mínimos, tales como:
 - (i) Planta Externa:
 - Los armarios contarán con cerraduras y/o candados físicos o electrónicos, platinas de seguridad con cerradura, entre otros.
 - Las cajas de distribución contarán con cerraduras con llave, entre otros; siempre que la tecnología lo permita y no sea limitante para brindar servicios a los abonados y usuarios.
 - Las cámaras subterráneas contarán con soldadura de tapas, contratapas, tapas especiales con grava, entre otros mecanismos de seguridad.
 - (ii) Planta Interna:
 - Los repartidores principales (MDF) contarán con cerraduras y/o candados físicos o electrónicos, contactos magnéticos, entre otros.
 - Los sistemas de conmutación y transmisión contarán con cerraduras y/o candados físicos o electrónicos, contactos magnéticos, sensores de movimiento, cámaras de videovigilancia, entre otros.

- Las estaciones base celulares contarán con perímetros de material noble o malla eslabonada terminada con concertina galvanizada de doble navaja en espiral, contactos magnéticos y alarmas de intrusión, entre otros.
 - Los ambientes internos o externos desde los cuales se puede acceder a los Activos de Información Protegida almacenados en soportes físicos e informáticos deberán tener solidez física en todo el perímetro y no podrán tener zonas vulnerables que puedan derribarse fácilmente y facilitar su acceso. Además, contarán con cerraduras o candados físicos o electrónicos, contactos magnéticos y alarmas de intrusión, entre otros, según la criticidad de los Activos de Información Protegida.
- d) Mecanismos o sistemas para registrar, consolidar y reportar el 100% de los trabajos realizados en la Planta Interna (MDF, conmutación, transmisión) y en la Planta Externa que permitan verificar presencial o remotamente el detalle de los trabajos realizados. En el caso de la Planta Externa se utilizarán los registros de Órdenes de Trabajo y evidencias fotográficas que se añaden a los expedientes de obra. Aleatoriamente se podrán realizar inspecciones a obras para validar en sitio la ejecución.
- e) Centro de Control de Seguridad Integral y centros de control periféricos desde los cuales se monitoree permanentemente los sistemas de seguridad electrónica instalados en los locales y ambientes restringidos de la Planta Interna y, de ser caso, Planta Externa (oficinas, edificios, etc.) que requieran Medidas de Protección.
- f) Sistemas de seguridad lógica para proteger los equipos informáticos empleados para los procesos de facturación, tasación, bases de datos, entre otros, los cuales contarán con contraseñas de acceso, firewalls, software de detección y protección en tiempo real contra códigos maliciosos.
- g) Sistemas de seguridad de red para proteger el acceso, el uso y la integridad de la red, así como la confidencialidad de los Activos de Información Protegida frente a ataques maliciosos, a través de mecanismos, tales como: autenticación, control de conexión de red y cifrado en los sistemas principales, entre otros.

En caso se identifique indicios o registre antecedentes de vulneración de las medidas técnicas de seguridad implementadas, el Área de Negocio Responsable en coordinación con el área de Seguridad, deberá adoptar medidas de seguridad adicionales que permitan minimizar dicho riesgo.

4.2.6. Medidas Organizativas

Las medidas técnicas anteriormente descritas, deben ser complementadas con medidas organizativas, apropiadas para garantizar un nivel de seguridad adecuado al riesgo identificado.

Las Áreas de Negocio Responsables deben adoptar e implementar medidas de control de carácter organizativo para la protección de los Activos de Información Protegida. Estas medidas deben ser determinadas por las áreas de Regulación y Seguridad y deben poder garantizar un nivel de seguridad adecuado al riesgo identificado.

Las medidas organizativas que se detallan a continuación no deben ser entendidas como únicas. Las Áreas de Negocio Responsables tienen la responsabilidad de adoptar e implementar medidas complementarias que resulten apropiadas en cada caso, según determinen las áreas de Regulación y Seguridad:

- a) Manuales internos de procedimientos de Seguridad Lógica, Seguridad de la Información, Seguridad Física, etc., los mismos que deben ser aplicables a trabajadores y Proveedores, según corresponda.
- b) Programa de Inspecciones en la Planta Interna y Planta Externa y/o en los ambientes internos o externos de manera independiente a las acciones de control realizadas periódicamente, que se lleven a cabo para verificar el cumplimiento de las medidas adoptadas para salvaguardar el Secreto de las Telecomunicaciones. En la Planta Externa, las inspecciones se realizarán sobre muestras. Los registros de las citadas inspecciones estarán a disposición de los inspectores autorizados del MTC, en caso sea solicitado.
- c) Programa de mantenimiento de los sistemas y elementos de seguridad electrónico instalados en los ambientes restringidos para asegurar su adecuado funcionamiento y de esa manera, evitar o mitigar el riesgo de vulneración a los Activos de Información Protegida.
- d) Cláusulas en los contratos con Proveedores, que obliguen a éstos, a establecer las medidas y procedimientos razonables para evitar o mitigar el riesgo de vulneración del Secreto de las Telecomunicaciones.
- e) Acuerdos de confidencialidad con cada uno de los trabajadores que participen de la gestión comercial y/u operativa y/o que tengan acceso a Activos de Información Protegida, previendo en dichos acuerdos, la obligación de no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración del Secreto de las Telecomunicaciones y la confidencialidad de los Activos de Información Protegida, aún después de extinguido el vínculo laboral, sin perjuicio de las consecuencias civiles y penales derivadas de su incumplimiento. El Área de Negocio Responsable, tiene a su cargo verificar dicho cumplimiento en cualquier momento.
- f) En los contratos con Proveedores, Integratel exigirá a su vez, la suscripción de Acuerdos de Confidencialidad con el personal que éstos tuvieran a su cargo y que tenga acceso a Activos de Información Protegida. Dichos acuerdos, entre el proveedor y su personal, preverán la obligación de no divulgar cualquier información que pudiera facilitar o coadyuvar a la vulneración del Secreto de las Telecomunicaciones y la confidencialidad de los Activos de Información Protegida, aún después de extinguido el vínculo laboral o contractual, sin perjuicio de las consecuencias civiles y penales derivadas de su incumplimiento. El Área de Negocio Responsable, tiene a su cargo verificar dicho cumplimiento en cualquier momento.

4.3. Organización interna

4.3.1. Principio de corresponsabilidad

Los trabajadores deben preservar la seguridad de los Activos de Información Protegida que Integratel pone a su disposición, en consonancia con los criterios, requisitos, procedimientos y tecnologías de seguridad definidas por las normativas de seguridad de Integratel y la Legislación Vigente. Al mismo tiempo, los trabajadores deben utilizar los Activos de Información Protegida estrictamente para el desempeño de las actividades propias de su puesto de trabajo y tareas asignadas, según corresponda.

El Área del Negocio Responsable, en su condición de propietaria de los Activos de Información Protegida, es propietaria a su vez, del riesgo asociado del Activo de Información Protegida. Tiene la responsabilidad y autoridad última de gestionar ese riesgo y aceptar el riesgo residual. El Área de Negocio Responsable se apoyará en

las áreas de Seguridad y Regulación para realizar las tareas orientadas a garantizar la seguridad de este, según corresponda.

4.3.2. Control Interno

Para asegurar un adecuado cumplimiento de la presente Normativa por parte de Integratel, los Directores de todas las Áreas de Negocio deberán asegurar dentro de las responsabilidades de su equipo a cargo, las siguientes, pudiendo ser asumidas por más de un Responsable Interno:

- **Planificación y cumplimiento normativo**

Planificar, supervisar y evaluar la implementación de controles que garanticen el cumplimiento de la Normativa dentro de su área, incluyendo la adecuada incorporación de dichos requisitos en los contratos con Proveedores.

- **Gestión documental**

Documentar, conservar y mantener accesible toda evidencia que acredite el cumplimiento de las obligaciones establecidas en la Normativa.

- **Análisis de riesgos**

Impulsar y coordinar la ejecución de análisis de riesgos relacionados con la vulneración del Secreto de las Telecomunicaciones y de los Activos de Información Protegida, abarcando procesos, sistemas, ambientes, equipos y componentes tanto de Planta Interna como Externa. Mantener actualizada la matriz de riesgos correspondiente.

- **Implementación de medidas de protección**

Coordinar con el área de Seguridad la implementación, mejora o mantenimiento de Medidas de Protección internas, asegurando que estas se ajusten a los riesgos identificados y que se mantenga un nivel de seguridad adecuado.

- **Gestión presupuestal**

Gestionar los recursos y presupuestos necesarios para implementar, reforzar o mantener las Medidas de Protección relacionadas con los Activos de Información Protegida del área.

- **Gestión de ambientes y sistemas restringidos**

Identificar, registrar y mantener actualizada la relación de ambientes y sistemas de acceso restringido que almacenan Activos de Información Protegida, informando oportunamente al área de Seguridad sobre cualquier cambio.

- **Concientización interna y con Proveedores**

Promover la cultura de protección del Secreto de las Telecomunicaciones dentro del área y entre los Proveedores, asegurando que conozcan y comprendan la presente Normativa.

- **Comunicación con Regulación y Seguridad**

Informar a las áreas de Regulación y Seguridad sobre controles implementados, sus modificaciones, los responsables operativos de los activos y cualquier otra información necesaria para cumplir con requerimientos regulatorios o de inspección.

- **Participación en foros y coordinación operativa**

Participar activamente en los foros o espacios de coordinación convocados por las áreas de Regulación y Seguridad para asegurar la correcta articulación de las funciones de control.

- **Inspecciones y verificaciones de campo**

Realizar inspecciones periódicas en Planta Interna, Planta Externa y ambientes relacionados, llevando registro de sus resultados y gestionando acciones correctivas frente a las incidencias detectadas.

- **Supervisión de trabajos en Planta**

Implementar mecanismos de registro, consolidación y reporte que permitan verificar el detalle del 100% de los trabajos ejecutados en Planta Interna y Externa.

- **Simulacros de inspección del MTC**

Coordinar y participar en simulacros que permitan evaluar la capacidad operativa del área frente a inspecciones opinadas e inopinadas del MTC, considerando diversos escenarios de riesgo.

- **Investigación de incidentes**

Colaborar en actividades de investigación relacionadas con incidentes de seguridad de las telecomunicaciones en coordinación con las áreas de Seguridad y Regulación.

- **Supervisión**

Ejecutar acciones periódicas de supervisión y control que permitan validar tanto el cumplimiento normativo como la efectividad de las Medidas de Protección implementadas.

- **Gestión con Proveedores**

- ✓ Verificar que se haya puesto a disposición de los Proveedores la versión vigente de la presente Normativa.,
- ✓ Supervisar el cumplimiento de las medidas técnicas y organizativas exigidas por la presente Normativa dentro de su ámbito contractual.
- ✓ Supervisar la existencia de acuerdos de confidencialidad entre los Proveedores y su personal con acceso a información protegida.

- **Actualización normativa**

Colaborar con el área de Regulación en la revisión y mejora continua de la presente Normativa.

- **Gestión de accesos**

Supervisar periódicamente la vigencia, necesidad y trazabilidad de los permisos de acceso físico y lógico relacionados con Activos de Información Protegida, solicitando su revocación cuando ya no sean requeridos.

- **Gestión de incidentes y notificaciones**

Reportar de manera inmediata al área de Seguridad cualquier incidente, sospecha o anomalía que pueda comprometer el Secreto de las Telecomunicaciones o los Activos de Información Protegida.

4.4. Obligaciones y responsabilidades

4.4.1. Obligaciones de los trabajadores

Todos los trabajadores de Integratel, independientemente del área en la que se desempeñen, se encuentran obligados a preservar la seguridad, confidencialidad e integridad de los Activos de Información Protegida de Integratel, en línea con la presente Normativa.

Los trabajadores de Integratel están obligados a:

- Salvaguardar los Activos de Información Protegida encontrándose impedidos de sustraer, interceptar, interferir, cambiar, alterar, desviar el curso, publicar, revelar, divulgar, utilizar, tratar de conocer o facilitar que un proveedor y/o tercero realice dichas acciones o trate de conocer la existencia, el contenido de cualquier comunicación o de los medios que lo soportan y/o transmitan. Se encuentran impedidos³ de entregar y/o facilitar Activos de Información Protegida a terceros (incluidos cónyuges o familiares).
- Conocer y cumplir la presente Normativa, procedimientos que de ella se deriven, así como las Políticas, Normativas, Reglamentos, Instrucciones y/o Manuales de Seguridad que se vinculen.
- En caso aplique, asegurar que los contratos con los Proveedores que accedan o puedan acceder a Activos de Información Protegida contengan las cláusulas sobre Secreto de las Telecomunicaciones, establecidas por el área de Regulación. Asimismo, deberán asegurar que los Proveedores que accedan o puedan acceder a Activos de Información Protegida suscriban los Acuerdos de Confidencialidad con su personal.
- Informar a su superior inmediato cualquier infracción relativa a la violación del Secreto de las Telecomunicaciones o incumplimiento a lo dispuesto en la presente Normativa por parte de trabajadores y/o Proveedores. Este a su vez, informará a las áreas de Seguridad y Regulación.
- Notificar lo antes posible a su superior inmediato, cualquier incidente, vulnerabilidad u eventos sospechosos que pudiera ser un riesgo real o potencial a la seguridad de los Activos de Información Protegida. Este a su vez, informará a las áreas de Seguridad y Regulación.
- Acceder y utilizar únicamente los Activos de Información Protegida a los que se tiene acceso autorizado para los fines establecidos.
- Asistir a los cursos de capacitación organizadas por Integratel.

³ Se exceptúa de este impedimento a los trabajadores de Integratel que tengan como parte de sus funciones deban atender solicitudes de levantamiento de secreto de las telecomunicaciones.

- El incumplimiento de la obligación de salvaguardar el Secreto de las Telecomunicaciones será considerado una falta laboral grave y será causal de terminación del contrato de trabajo. Ello, sin perjuicio de las responsabilidades civiles y penales correspondientes.

4.4.2. Obligaciones de los Proveedores

Los Proveedores están obligados a preservar la seguridad, confidencialidad e integridad de éstos, en línea con las obligaciones que dispone la presente Normativa y sus respectivos contratos.

Para ello, los Proveedores se obligan a cumplir con las siguientes obligaciones:

- Aceptar y cumplir con las cláusulas contractuales relacionadas a Secreto de las Telecomunicaciones incluidas en los contratos que celebre con Integratel.
- Difundir la presente Normativa entre todo su personal que acceda o pueda acceder a los Activos de Información Protegida, de modo que puedan conocer las obligaciones que les aplican. Los Proveedores deberán poder acreditar ante Integratel el cumplimiento de esta obligación.
- Suscribir Acuerdos de Confidencialidad con su personal, estableciendo la obligación de no divulgar información que pueda facilitar la vulneración y la confidencialidad de los Activos de Información Protegida, incluso después de extinguido el vínculo laboral, sin perjuicio de las consecuencias civiles y penales derivadas de su incumplimiento. El modelo de Acuerdo de Confidencialidad forma parte integrante del contrato suscrito entre Integratel y el proveedor.
- Mantener un archivo físico y/o digital con los Acuerdos de Confidencialidad suscritos con su personal, que tenga o pueda tener acceso a los Activos de Información Protegida, pudiendo ser requeridos por Integratel en cualquier momento.
- Facilitar inspecciones, investigaciones o auditorías por parte de Integratel para verificar el cumplimiento de las medidas de protección en sus respectivos ámbitos de actuación.
- Brindar capacitaciones continuas (al menos semestralmente) a su personal que acceda o pueda acceder a Activos de Información Protegida.
- No compartir con terceros los Activos de Información Protegida. Previa solicitud expresa debidamente sustentada, Integratel podrá de manera excepcional autorizar dicha compartición.

4.4.3. Obligaciones específicas de las áreas

4.4.3.1. Gerente General y Comité de Dirección

Son responsabilidades del Gerente General y de los Directores de Integratel impulsar el cumplimiento de la presente Normativa en todas sus áreas.

4.4.3.2. Personas

Son responsabilidades del área de Personas las siguientes:

- Designar como mínimo a un Responsable Interno, con la finalidad de asegurar la implementación y cumplimiento de la presente Normativa dentro del área. Dicha designación será comunicada a las áreas de Regulación y Seguridad.
- Incluir en todos los contratos de trabajo con los trabajadores, cláusulas que los obliguen a salvaguardar el Secreto de las Telecomunicaciones, de acuerdo con la presente Normativa. Dichas cláusulas precisarán que esta obligación regirá aún después de extinguido el vínculo laboral, así como las consecuencias civiles y penales de su incumplimiento.
- Entregar a todas las personas que ingresen a practicar o laborar en Integratel, un ejemplar de la presente Normativa.
- Mantener un registro de toma de conocimiento de todos los trabajadores, mediante el cual estos declaren que han tomado conocimiento de la presente Normativa, y se obligan a cumplirla. Este registro deberá ser actualizado cada vez que se actualice la presente Normativa.
- Mantener actualizado el Reglamento Interno de Trabajo, en consonancia con la presente Normativa.
- Establecer medidas disciplinarias en caso de incurrir en incumplimientos a la presente Normativa.
- Participar en las investigaciones sobre incumplimientos a la presente Normativa y sancionar los casos que así se determinen.

4.4.3.3. Regulación y Legal

Son responsabilidades del área de Regulación las siguientes:

- Asesorar a todas las áreas de Integratel y ejercer las facultades de interpretación que sean requeridas de esta Normativa.
- Redactar y aprobar cláusulas contractuales destinadas a asegurar la protección del Secreto de las Telecomunicaciones, en consonancia con la presente Normativa.
- Colaborar con el área de Personas en la actualización del Reglamento Interno del Trabajo en lo que corresponda a la protección del Secreto de las Telecomunicaciones.
- Preparar el informe anual sobre medidas implementadas para salvaguardar el Secreto de las Telecomunicaciones, consolidando la información remitida por las distintas Áreas de Negocio Responsables y remitirlo oportunamente al MTC y al OSIPTEL. Dicho informe anual debe contener lo exigido por la Legislación Vigente, así como en los contratos de concesión de los que Integratel es parte. Las modificaciones al informe anual presentado deberán

ser comunicadas al MTC semestralmente en los términos indicados en la Legislación Vigente.

- Coordinar con las Áreas de Negocio Responsables, aquellas inspecciones que realice el MTC u otras entidades competentes.
- Organizar capacitaciones en materia de Secreto de las Telecomunicaciones a los trabajadores, las cuales serán coordinadas con el área de Seguridad y Personas.
- Mantener actualizada la presente Normativa.
- Informar a todas las Áreas del Negocio cuando exista una modificación de la presente Normativa.

Son responsabilidades del área Legal las siguientes:

- Incorporar y actualizar los modelos de contratos que utiliza el área de Compras, así como los otros modelos de contratos que correspondan con las cláusulas de Secreto de las Telecomunicaciones que el área de Regulación apruebe.
- Asesorar al área de Seguridad e impartir pautas para la atención de las solicitudes judiciales del levantamiento del Secreto de las Telecomunicaciones.
- Aprobar los modelos de carta de respuesta para la atención de pedidos de las autoridades con relación al levantamiento del Secreto de las Telecomunicaciones.

4.4.3.4. Seguridad

Son responsabilidades del área de Seguridad las siguientes:

- Designar como mínimo a un Responsable Interno desde las funciones de seguridad (Seguridad Lógica, Seguridad de la Información, Seguridad Física, etc.) que se encargará de dar soporte u orientación a las Áreas de Negocio. Dicha designación será comunicada al área de Regulación.
- Atender los requerimientos de las autoridades judiciales en materia de levantamiento del Secreto de las Telecomunicaciones. Dicha designación será comunicada al área de Regulación.
- Difundir con todas las áreas de la Compañía instrucciones o procedimientos de acceso a ambientes restringidos que albergan Activos de Información Protegida.
- Proponer al área de Regulación, la incorporación de cláusulas de seguridad en los contratos con Proveedores de servicios críticos (red, planta interna y externa, facturación, sistemas) para asegurar medidas de protección idóneas en sus respectivos ámbitos de actuación y mitigar así, los riesgos de los Activos de Información Protegida.

- Participar con las áreas de Regulación y Personas, en la elaboración y difusión de contenidos en materia de seguridad del Secreto de las Telecomunicaciones, para la capacitación de los trabajadores.
- Implementar un programa de mantenimiento de los sistemas y elementos de seguridad electrónica instalados en los locales y ambientes que contengan Activos de Información Protegida, para asegurar su adecuado funcionamiento.
- Gestionar los sistemas de control de accesos físicos y lógicos a los locales, ambientes o sistemas restringidos que contengan Activos de Información Protegida.
- Mantener permanentemente actualizada la lista de ambientes internos y externos que albergan Activos de Información Protegida y que son de acceso restringido, así como la lista de los responsables que aprueban los accesos a dichos ambientes.
- Implementar un programa de inspecciones, con una periodicidad de tres meses, de forma aleatoria y sobre muestras, a los ambientes internos y/o externos para verificar o auditar, si fuera el caso, el cumplimiento de las medidas de protección por parte de trabajadores y Proveedores que prestan servicios de operación y mantenimiento de las redes de telecomunicaciones, manejo de sistemas, facturación y servicio al cliente y que tienen acceso a los Activos de Información Protegida, así como para verificar la correcta ejecución de las labores que se les hubiera encomendado, debiendo mantener un registro de dichas inspecciones.
- Realizar coordinaciones con el Poder Judicial, Ministerio Público y Policía Nacional del Perú, sobre temas relativos al levantamiento del Secreto de las Telecomunicaciones, con conocimiento del área de Regulación.

4.4.3.5. TI

Son responsabilidades del área de TI las siguientes:

- Designar como mínimo a un Responsable Interno, con la finalidad de asegurar la implementación y cumplimiento de la presente Normativa dentro del área. Dicha designación será comunicada a las áreas de Regulación y Seguridad.
- Administrar los mecanismos y sistemas de seguridad aplicables a las tecnologías de la información.
- Gestionar la implementación de medidas de seguridad aplicables a los Activos de Información Protegida en su ámbito de responsabilidad, en coordinación con el área de Seguridad.
- Gestionar la generación y almacenamiento de los registros de acceso a los Activos de Información Protegida.
- Velar por el cumplimiento de las normativas y controles de seguridad en los contratos con Proveedores.

4.4.3.6. Compras

Son responsabilidades del área de Compras las siguientes:

- Designar como mínimo a un Responsable Interno, con la finalidad de asegurar la implementación y cumplimiento de la presente Normativa dentro del área. Dicha designación será comunicada a las áreas de Regulación y Seguridad.
- Poner a disposición de los Proveedores, un ejemplar de la presente Normativa y comunicar las actualizaciones de ésta de manera oportuna.

4.4.3.7. Auditoría Interna

El área de Auditoría Interna efectuará las verificaciones que considere pertinentes para constatar el correcto cumplimiento de los aspectos contenidos en la presente Normativa.

4.5. Consecuencias de su incumplimiento

El incumplimiento de la presente Normativa constituye una falta grave que puede afectar directamente la continuidad operativa de Integratel. Puede derivar en sanciones administrativas, incluyendo responsabilidades penales e incluso la revocación de la concesión de telecomunicaciones.

5. Entrada en vigor

La presente Normativa entrará en vigor a partir de la fecha de su aprobación por el Directorio. El área de Regulación será responsable de su custodia, seguimiento y actualización, en coordinación con las áreas involucradas, cuando así se requiera.

6. Disposiciones complementarias

Dentro de un plazo de 30 días hábiles desde la aprobación de la presente Normativa, las áreas de Regulación y Seguridad aprobarán el listado de los Activos de Información Protegida con sus respectivos responsables, debiendo ser éstos debidamente informados.

* * * *