Cirtel Comunicaciones SAS

MANUAL DE POLITICAS DE LA SEGURIDAD

COMPAÑÍA INTEGRAL DE RECURSOS
EN TELECOMUNICACIONES S.A.S
NIT 901130683-6

VIGENTE HASTA EL 31 DE DICIEMBRE DEL 2025

INDICE

1. **Presentación**
2. **Objetivo del Manual**
3. **Alcance**
4. **Marco Normativo y Referencial**
5. **Glosario de Términos**
6. **Principios Rectores de la Seguridad de la Información**
7. **Organización de la Seguridad**
8. **Clasificación de la Información**
9. **Políticas Generales de Seguridad**
    - 9.1 Control de Accesos
    - 9.2 Seguridad Física y Ambiental
    - 9.3 Seguridad en las Comunicaciones
    - 9.4 Seguridad en el Uso de Equipos
    - 9.5 Seguridad en la Gestión de Redes
    - 9.6 Gestión de Incidentes de Seguridad
    - 9.7 Respaldo y Recuperación de la Información
10. **Responsabilidades del Personal**
11. **Capacitación y Concientización**
12. **Auditorías y Revisión de la Política**
13. **Recomendaciones Generales**
14. **Canal de Contacto para Incidentes**
15. **Conclusión**

1. PRESENTACIÓN

En CIRTEL COMUNICACIONES S.A.S. reconocemos que la información es uno de nuestros activos más valiosos. Como empresa prestadora de servicios de telecomunicaciones, proteger la seguridad de la información no es solo un requisito legal, sino una responsabilidad directa con nuestros usuarios, aliados y colaboradores.

Este manual recoge nuestras políticas y lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información que gestionamos. Refleja el compromiso que tenemos con la protección de nuestros sistemas, datos y servicios.

Nuestra intención es que estas políticas sean comprendidas y aplicadas por todo el equipo de CIRTEL, y que se mantengan actualizadas frente a los cambios tecnológicos, normativos y operativos del entorno en el que trabajamos.

2. OBJETIVO DEL MANUAL

Este manual tiene como objetivo establecer las políticas de seguridad de la información que aplicamos en CIRTEL COMUNICACIONES S.A.S. para proteger nuestros sistemas, redes, servicios y datos, así como los de nuestros usuarios.

Buscamos garantizar un manejo responsable de la información en todos los niveles de la organización, prevenir riesgos asociados a accesos no autorizados, pérdidas o alteraciones, y asegurar la continuidad de nuestras operaciones.

Además, este documento nos permite dar cumplimiento a los requerimientos establecidos por la normativa vigente del sector TIC, especialmente en lo relacionado con la gestión de riesgos, el tratamiento de datos personales y la protección de la infraestructura tecnológica.

3. ALCANCE

Las políticas contenidas en este manual aplican a todos los procesos, áreas, sistemas y personas que hacen parte de CIRTEL COMUNICACIONES S.A.S., incluyendo personal interno, contratistas, aliados estratégicos y cualquier tercero que tenga acceso a nuestros activos de información.

Estas políticas deben ser consideradas en todas las actividades relacionadas con la operación técnica, administrativa y comercial de nuestros servicios, sin importar si se ejecutan de forma presencial o remota.

Incluimos aquí el tratamiento de datos personales, la protección de la infraestructura tecnológica, la gestión de incidentes, el acceso a los sistemas, el uso de redes, y cualquier otra acción que involucre información o tecnología bajo nuestra responsabilidad.

4. MARCO NORMATIVO Y REFERENCIAL

El presente manual se fundamenta en la aplicación de la normativa vigente y las mejores prácticas internacionales para garantizar la seguridad de la información en CIRTEL COMUNICACIONES S.A.S. Entre los principales marcos normativos y referenciales que orientan nuestras políticas se encuentran:

- **Ley 1581 de 2012**: Regula la protección de datos personales y garantiza el derecho a la privacidad.
- **Decreto 1377 de 2013**: Establece disposiciones para el tratamiento adecuado de datos personales.
- **Ley 1273 de 2009**: Tipifica los delitos informáticos y define medidas para proteger la información digital.
- **Normativas del Ministerio de Tecnologías de la Información y las Comunicaciones (TIC)** y la Comisión de Regulación de Comunicaciones (CRC), que establecen requisitos específicos para la seguridad en el sector de telecomunicaciones.
- **ISO/IEC 27001**: Estándar internacional para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), que promueve la confidencialidad, integridad y disponibilidad de la información.

Este marco garantiza que las políticas adoptadas cumplen con las obligaciones legales y estándares reconocidos, brindando confianza a nuestros usuarios, colaboradores y aliados estratégicos.

5. GLOSARIO DE TÉRMINOS

- **Activo de información:** Elemento o recurso que tiene valor para la organización, como datos, sistemas, equipos o infraestructura tecnológica.
- **Confidencialidad:** Propiedad que garantiza que la información solo sea accesible por personas autorizadas.
- **Disponibilidad:** Característica que asegura que la información y los sistemas estén accesibles y operativos cuando se requieran.
- **Integridad:** Propiedad que garantiza que la información no sea alterada de manera no autorizada.
- **Usuario:** Persona autorizada para acceder y utilizar los recursos de información de la organización.
- **Contraseña:** Clave secreta utilizada para autenticar la identidad de un usuario y controlar el acceso a sistemas o información.

- **Gestión de riesgos:** Proceso para identificar, evaluar y controlar los riesgos relacionados con la seguridad de la información.
- **Datos personales:** Información relacionada con una persona natural identificada o identificable.
- **Autenticación:** Proceso mediante el cual se verifica la identidad de un usuario o sistema.
- **Control de acceso:** Medidas implementadas para permitir o restringir el acceso a información o recursos.
- **Política de seguridad:** Conjunto de reglas y directrices para proteger la información y los sistemas.
- **Redes:** Conjunto de dispositivos y sistemas interconectados que permiten la comunicación y transmisión de datos.
- **Seguridad física:** Medidas para proteger los activos físicos contra accesos no autorizados o daños.
- **Respaldo (Backup):** Copia de seguridad de la información para su recuperación en caso de pérdida o daño.
- **Malware:** Software malicioso diseñado para dañar, comprometer o acceder sin autorización a sistemas o datos.
- **Firewall:** Sistema que controla y filtra el tráfico de red para proteger los recursos informáticos.
- **Phishing:** Técnica fraudulenta para obtener información confidencial mediante engaños.
- **Criptografía:** Técnica para proteger la información mediante el uso de códigos y cifrados.

6. PRINCIPIOS RECTORES DE LA SEGURIDAD DE LA INFORMACIÓN

En CIRTEL COMUNICACIONES S.A.S., la seguridad de la información es un pilar fundamental para garantizar la confianza de nuestros usuarios, aliados y colaboradores. Por ello, nuestras políticas se basan en los siguientes principios rectores que orientan todas las acciones y decisiones relacionadas con la protección de los activos de información:

- **Confidencialidad:** Se asegura que la información solo sea accesible a las personas o sistemas autorizados. Esto implica implementar controles y mecanismos que eviten la divulgación no autorizada de datos sensibles, como información personal, comercial o técnica.

- **Integridad:** Garantizamos que la información se mantenga precisa, completa y sin modificaciones no autorizadas durante todo su ciclo de vida. La integridad

asegura que los datos no se alteren accidentalmente o por acciones maliciosas, manteniendo su confiabilidad para la toma de decisiones.

- **Disponibilidad:** Los sistemas, servicios y la información deben estar disponibles y operativos para los usuarios autorizados cuando lo necesiten. Esto implica prevenir interrupciones, planificar la continuidad del negocio y contar con planes de recuperación ante desastres para minimizar el impacto de fallas o incidentes.
- **Responsabilidad:** Todos los colaboradores, contratistas y terceros con acceso a la información deben actuar con responsabilidad y cumplir con las políticas y procedimientos establecidos. La seguridad es un compromiso colectivo que requiere la colaboración de toda la organización.
- **Legalidad:** Cumplimos con todas las leyes, normativas y regulaciones aplicables en materia de seguridad de la información, protección de datos personales y telecomunicaciones. Esto garantiza que nuestras prácticas estén alineadas con los requisitos legales vigentes y se respeten los derechos de los usuarios.
- **Transparencia:** Promovemos una cultura de comunicación abierta y clara sobre las políticas y prácticas de seguridad, facilitando la comprensión y el cumplimiento por parte de todos los involucrados.
- **Mejora Continua:** Reconocemos que las amenazas y tecnologías evolucionan constantemente. Por ello, mantenemos un proceso permanente de revisión, auditoría y actualización de nuestras políticas, controles y procedimientos, para fortalecer la protección de la información y adaptarnos a los cambios del entorno.
- **Minimización:** Solo recopilamos, almacenamos y procesamos la información estrictamente necesaria para cumplir con nuestras funciones, reduciendo la exposición a riesgos y protegiendo la privacidad de los usuarios.
- **Seguridad por Diseño:** Incorporamos prácticas de seguridad desde la planificación y desarrollo de proyectos, sistemas y procesos, garantizando que la protección sea parte integral de todas las operaciones.

Estos principios son la base para construir un entorno seguro, confiable y resiliente que permita a CIRTEL COMUNICACIONES S.A.S. cumplir con sus objetivos estratégicos y operativos, protegiendo los activos de información y fortaleciendo la confianza de todos los grupos de interés.

7. ORGANIZACIÓN DE LA SEGURIDAD

En CIRTEL COMUNICACIONES S.A.S., la seguridad de la información es responsabilidad de toda la organización, pero para asegurar su adecuada gestión se ha establecido una estructura clara con roles y responsabilidades definidos:

- **Alta Dirección:**
  La alta dirección tiene el compromiso y liderazgo para promover la cultura de seguridad en toda la empresa. Es responsable de aprobar las políticas de seguridad, asignar recursos y supervisar su cumplimiento.
- **Responsable de Seguridad de la Información:**
  Designado por la dirección, esta persona coordina la implementación, seguimiento y actualización de las políticas y controles de seguridad. Además, actúa como enlace entre las distintas áreas y reporta a la alta dirección sobre el estado de la seguridad.
- **Comité de Seguridad de la Información:**
  Grupo interdisciplinario conformado por representantes de áreas clave (tecnología, operaciones, recursos humanos, legal, entre otras) que se reúne periódicamente para evaluar riesgos, revisar incidentes y proponer mejoras en la gestión de seguridad.
- **Usuarios y Colaboradores:**
  Todos los empleados, contratistas y terceros con acceso a los recursos de información tienen la obligación de cumplir con las políticas, reportar incidentes y participar en programas de capacitación y concientización.
- **Área de Tecnología:**
  Responsable de implementar y mantener los controles técnicos de seguridad, como gestión de accesos, protección de redes, respaldo de información y respuesta ante incidentes técnicos.
- **Área de Recursos Humanos:**
  Encargada de incluir en los procesos de selección, inducción y capacitación aspectos relacionados con la seguridad de la información, así como de gestionar la confidencialidad mediante acuerdos y cláusulas contractuales.

Esta estructura organizacional busca garantizar una gestión integral y coordinada de la seguridad de la información, alineada con los objetivos estratégicos de CIRTEL COMUNICACIONES S.A.S., y permite una respuesta rápida y eficiente ante cualquier evento que pueda afectar la confidencialidad, integridad o disponibilidad de la información.

8. CLASIFICACIÓN DE LA INFORMACIÓN

Para garantizar un manejo adecuado y seguro de la información, en CIRTEL COMUNICACIONES S.A.S. clasificamos la información en función de su sensibilidad, valor y riesgos asociados. Esta clasificación permite aplicar controles específicos según el nivel de protección requerido:

- **Información Pública:**
  Datos e información que pueden ser divulgados sin restricción, ya que no generan riesgos para la empresa ni para terceros. Ejemplos incluyen materiales de marketing, información institucional y comunicados oficiales.
- **Información Interna:**
  Información que es exclusiva para uso interno de CIRTEL y no debe ser compartida fuera de la organización. Su divulgación no autorizada podría afectar la operación o la imagen de la empresa. Incluye políticas internas, procedimientos y datos administrativos.
- **Información Confidencial:**
  Información sensible que requiere protección estricta debido a su impacto en la empresa o en terceros en caso de acceso o divulgación no autorizada. Incluye datos personales de clientes, información financiera, contratos, y documentación técnica.
- **Información Restringida:**
  Información crítica con acceso limitado solo a personal autorizado y con estrictos controles de seguridad. La divulgación o pérdida de esta información podría causar daños significativos a la empresa o a sus usuarios. Ejemplos incluyen claves de acceso, planes estratégicos y datos en proceso de investigación.

La correcta clasificación de la información facilita la aplicación de medidas de seguridad apropiadas, como controles de acceso, cifrado, almacenamiento seguro y procedimientos de destrucción cuando sea necesario. Todos los colaboradores deben manejar la información respetando su clasificación y reportar cualquier incidente o sospecha de vulneración.

9. POLÍTICAS GENERALES DE SEGURIDAD

En CIRTEL COMUNICACIONES S.A.S., se establecen las siguientes políticas para proteger la seguridad de la información y los recursos tecnológicos de la organización:

9.1 Control de Accesos

- El acceso a los sistemas, aplicaciones y datos debe ser autorizado únicamente para usuarios con permisos necesarios para cumplir sus funciones.

- Se debe utilizar autenticación segura, preferiblemente con contraseñas robustas y renovaciones periódicas.
- Los privilegios de acceso se asignarán con base en el principio de menor privilegio, limitando las autorizaciones al mínimo necesario.
- Se mantendrán registros de accesos para auditoría y monitoreo.

9.2 Seguridad Física y Ambiental

- Los centros de datos, salas de servidores y áreas con equipos críticos deben contar con controles físicos que limiten el acceso solo a personal autorizado.
- Se implementarán medidas para proteger los equipos contra incendios, inundaciones, cortes de energía y otros riesgos ambientales.
- Se mantendrá un ambiente seguro que prevenga daños accidentales o intencionales a los activos de información.

9.3 Seguridad en las Comunicaciones

- Toda comunicación de datos deberá estar protegida contra interceptaciones o modificaciones no autorizadas, mediante el uso de cifrado y protocolos seguros.
- Se deben aplicar controles para proteger las redes internas y externas, incluyendo el uso de firewalls y sistemas de detección de intrusos.
- Se evitará la transmisión de información sensible por canales no seguros.

9.4 Seguridad en el Uso de Equipos

- Los dispositivos y equipos de la empresa deben ser utilizados exclusivamente para fines autorizados y dentro del marco de las políticas establecidas.
- Se prohibirá la instalación de software no autorizado que pueda comprometer la seguridad.
- Los equipos deberán mantenerse actualizados con parches y antivirus vigentes.

9.5 Seguridad en la Gestión de Redes

- La infraestructura de red debe ser configurada y mantenida para proteger la confidencialidad, integridad y disponibilidad de la información.
- Se implementarán controles para monitorear y detectar actividades sospechosas o no autorizadas en la red.
- El acceso remoto debe realizarse mediante métodos seguros, como VPNs o conexiones cifradas.

9.6 Gestión de Incidentes de Seguridad

- Se establecerán procedimientos para la identificación, reporte, análisis y respuesta oportuna a incidentes de seguridad de la información.
- Todo incidente debe ser documentado y evaluado para tomar acciones correctivas y preventivas.
- Se fomentará la cultura de reporte inmediato para minimizar el impacto y evitar recurrencias.

9.7 Respaldo y Recuperación de la Información

- Se realizarán copias de seguridad periódicas y confiables de la información crítica, garantizando su integridad y disponibilidad.
- Los respaldos deben almacenarse en lugares seguros y, preferiblemente, en ubicaciones diferentes a los sistemas principales.
- Se desarrollarán y probarán planes de recuperación ante desastres para asegurar la continuidad de las operaciones.

RESPONSABILIDADES DEL PERSONAL

En CIRTEL COMUNICACIONES S.A.S., todos los miembros del equipo tienen un papel fundamental en la seguridad de la información. Las responsabilidades principales incluyen:

- **Conocimiento y cumplimiento:** Cada empleado, contratista o tercero debe conocer y cumplir las políticas y procedimientos de seguridad establecidos en este manual.
- **Confidencialidad:** Proteger la información a la que se tiene acceso, evitando su divulgación no autorizada.
- **Uso adecuado de recursos:** Utilizar los sistemas, equipos y recursos tecnológicos solo para fines autorizados y conforme a las políticas internas.
- **Reportes de incidentes:** Informar de manera inmediata cualquier incidente, vulnerabilidad o sospecha de amenaza relacionada con la seguridad de la información.
- **Participación en capacitación:** Asistir a las sesiones de formación y concientización para mantener actualizados los conocimientos en materia de seguridad.

- **Colaboración:** Trabajar en conjunto con las áreas responsables para implementar y mantener las medidas de seguridad.

Cada colaborador es responsable de actuar con diligencia y compromiso para proteger los activos de información y contribuir a un entorno seguro y confiable.

11. CAPACITACIÓN Y CONCIENTIZACIÓN

En CIRTEL COMUNICACIONES S.A.S., reconocemos que la seguridad de la información no depende únicamente de la tecnología, sino fundamentalmente del factor humano. Por esta razón, consideramos imprescindible desarrollar y mantener un programa continuo de capacitación y concientización que permita a todos los colaboradores, contratistas y terceros entender los riesgos asociados, conocer las políticas vigentes y aplicar las mejores prácticas en su trabajo diario.

Importancia de la capacitación
La capacitación es clave para fortalecer la cultura de seguridad, reducir errores humanos y prevenir incidentes que puedan comprometer la confidencialidad, integridad o disponibilidad de la información. Los temas abordados deben estar alineados con las amenazas actuales y las necesidades específicas de la organización, adaptándose a los cambios tecnológicos y normativos.

Temas prioritarios para las capacitaciones:

- **Políticas y procedimientos de seguridad:** Explicación detallada de las políticas internas, responsabilidades, y el impacto de su incumplimiento.
- **Gestión de contraseñas y control de accesos:** Cómo crear y manejar contraseñas seguras, la importancia de la autenticación multifactor y las reglas para el acceso a sistemas.
- **Identificación y prevención de amenazas comunes:** Concientización sobre phishing, ingeniería social, malware, ransomware y otras técnicas utilizadas por atacantes.
- **Protección de datos personales:** Cumplimiento de la normativa vigente en protección de datos y el manejo responsable de información sensible.
- **Reportes de incidentes:** Procedimientos para la detección, reporte y respuesta oportuna ante incidentes de seguridad.
- **Uso adecuado de los recursos tecnológicos:** Buenas prácticas para el uso de equipos, software y redes, evitando riesgos innecesarios.

- **Continuidad del negocio y recuperación ante desastres:** Rol del personal en asegurar la disponibilidad y recuperación de la información en situaciones de emergencia.

Cronograma anual de capacitaciones:
Para garantizar una cobertura adecuada y sostenida en el tiempo, se recomienda realizar al menos cuatro sesiones formativas anuales, distribuidas estratégicamente para abordar temas relevantes según la evolución de amenazas y proyectos internos. Este cronograma puede ajustarse a necesidades específicas, pero un ejemplo podría ser:

- **Primer trimestre:** Introducción a las políticas de seguridad y manejo de contraseñas.
- **Segundo trimestre:** Prevención de ataques de ingeniería social y phishing.
- **Tercer trimestre:** Protección de datos personales y cumplimiento normativo.
- **Cuarto trimestre:** Reporte de incidentes, continuidad del negocio y mejores prácticas generales.

Evaluación y seguimiento:
Cada sesión incluirá evaluaciones para medir el nivel de comprensión y retención de los participantes. Los resultados permitirán identificar áreas de mejora y ajustar los contenidos futuros.

Estas actividades complementan la formación, fortaleciendo la capacidad de prevención, detección y respuesta frente a incidentes y asegurando la mejora continua del sistema de gestión de seguridad de la información.

12. AUDITORÍAS Y REVISIÓN DE LA POLÍTICA

Para garantizar la efectividad y vigencia de las políticas de seguridad de la información, en CIRTEL COMUNICACIONES S.A.S. se implementa un proceso sistemático de auditorías y revisión continua que incluye los siguientes aspectos:

Auditorías internas y externas:

- Se programan auditorías periódicas para evaluar el cumplimiento de las políticas, procedimientos y controles establecidos.
- Las auditorías internas son realizadas por personal capacitado dentro de la organización, mientras que las auditorías externas pueden ser contratadas para ofrecer una visión imparcial y especializada.
- Durante las auditorías se revisan aspectos técnicos, administrativos y operativos relacionados con la seguridad de la información.

Evaluación de riesgos y controles:

- Los resultados de las auditorías permiten identificar vulnerabilidades, incumplimientos o áreas de mejora.
- Se revisan los controles existentes para determinar su eficacia y pertinencia frente a los riesgos actuales.

Revisión y actualización de la política:

- La política de seguridad de la información es un documento vivo que debe adaptarse a los cambios tecnológicos, normativos y organizacionales.
- Se establece un proceso formal para la revisión periódica, al menos una vez al año, o cuando se presenten eventos significativos que justifiquen una actualización (nuevas amenazas, cambios regulatorios, incidentes graves, entre otros).
- Los cambios en la política se comunican oportunamente a todos los colaboradores y partes interesadas.

Mejora continua:

- Con base en los hallazgos de auditorías y evaluaciones, se diseñan e implementan planes de acción para corregir deficiencias y fortalecer la seguridad.
- Se promueve una cultura de mejora continua que permita anticipar riesgos y adaptar las medidas de protección de manera proactiva.

Documentación y seguimiento:

- Todos los informes, resultados y acciones derivadas de las auditorías se documentan y archivan para su consulta y seguimiento.
- Se da seguimiento a las recomendaciones hasta su completa implementación.

Este proceso asegura que las políticas de seguridad de la información mantengan su relevancia y eficacia, contribuyendo a proteger los activos de información y apoyar los objetivos estratégicos de CIRTEL COMUNICACIONES S.A.S.

13. RECOMENDACIONES GENERALES

Para fortalecer la seguridad de la información en CIRTEL COMUNICACIONES S.A.S., se establecen las siguientes recomendaciones generales que deben ser adoptadas por todo el personal y áreas de la organización:

- **Cumplimiento estricto de políticas:** Todas las personas deben acatar las políticas y procedimientos establecidos para evitar riesgos y garantizar un manejo adecuado de la información.
- **Uso responsable de recursos tecnológicos:** Los equipos, sistemas y redes deben ser utilizados exclusivamente para actividades autorizadas y de acuerdo con las mejores prácticas de seguridad.
- **Protección de contraseñas:** Se debe mantener la confidencialidad de las credenciales de acceso y evitar compartirlas o anotarlas en lugares inseguros.
- **Manejo cuidadoso de la información confidencial:** La información sensible debe ser almacenada, transmitida y eliminada siguiendo los controles definidos según su clasificación.
- **Reporte inmediato de incidentes:** Cualquier anomalía, acceso no autorizado o sospecha de vulneración debe ser comunicada de forma rápida para tomar acciones oportunas.
- **Actualización constante:** Mantener los sistemas, aplicaciones y dispositivos con las últimas actualizaciones y parches de seguridad.
- **Evitar riesgos en la red:** No conectar dispositivos externos no autorizados, evitar descargar software o archivos sospechosos y usar conexiones seguras.
- **Concientización permanente:** Participar activamente en las campañas y programas de formación para estar siempre informados sobre las amenazas y buenas prácticas.
- **Colaboración entre áreas:** Fomentar la comunicación y cooperación para identificar riesgos, implementar controles y responder eficientemente ante incidentes.

Adoptar estas recomendaciones contribuye a crear un entorno seguro y confiable para proteger los activos de información, garantizar la continuidad del negocio y fortalecer la confianza de nuestros usuarios, aliados y colaboradores.

14. CANAL DE CONTACTO PARA INCIDENTES

Para garantizar una respuesta rápida y eficiente ante cualquier incidente relacionado con la seguridad de la información, CIRTEL COMUNICACIONES S.A.S. ha establecido un canal de contacto directo y accesible para todo el personal, aliados y usuarios.

Canal oficial:

- **Correo electrónico:** ingenieria@cirtel.com.co

- **Teléfono:** +57 316 3758574

Procedimiento para reporte de incidentes:

1. **Detección:** Cualquier empleado, contratista o usuario que identifique un posible incidente debe reportarlo inmediatamente a través de los canales oficiales.
2. **Registro:** El incidente será documentado para permitir su seguimiento y gestión.
3. **Análisis:** El equipo responsable evaluará la gravedad y el alcance del incidente para definir las acciones correctivas y preventivas.
4. **Comunicación:** Se informará oportunamente a las áreas involucradas y, si es necesario, a la alta dirección y entidades regulatorias.
5. **Resolución y cierre:** Una vez mitigado el incidente, se documentarán las lecciones aprendidas para fortalecer las medidas de seguridad.

Confidencialidad y protección:
Se garantiza la confidencialidad de la información proporcionada en los reportes y se protege a los denunciantes contra cualquier tipo de represalia.

Este canal de contacto es fundamental para mantener la integridad y continuidad de nuestros servicios, así como para proteger los datos de nuestros usuarios y la infraestructura tecnológica de la empresa.

Denuncias y Reportes

CIRTEL COMUNICACIONES S.A.S. promueve un ambiente de transparencia y responsabilidad, por lo que facilita la presentación de denuncias y reportes relacionados con irregularidades o vulneraciones a las políticas de seguridad.

- Las denuncias pueden referirse a incidentes como accesos no autorizados, fraudes, uso indebido de recursos o cualquier conducta que afecte la seguridad de la información.
- Se exhorta a todos los colaboradores y terceros a reportar cualquier sospecha o evidencia de incumplimiento sin temor a represalias.
- Todos los reportes serán tratados con estricta confidencialidad y serán investigados de manera objetiva y oportuna.
- El equipo responsable dará seguimiento a cada denuncia hasta su resolución, comunicando las acciones tomadas según corresponda.

Este mecanismo es vital para fortalecer la protección de los activos de información y promover un ambiente laboral ético y seguro.

15. CONCLUSIÓN

En CIRTEL COMUNICACIONES S.A.S., la seguridad de la información es un compromiso integral que involucra a todos los miembros de la organización. Este manual establece las bases para proteger nuestros activos de información, asegurar la continuidad de nuestros servicios y cumplir con las normativas vigentes del sector TIC.

La aplicación constante y responsable de las políticas aquí descritas nos permitirá minimizar riesgos, responder de manera eficaz ante incidentes y mantener la confianza de nuestros usuarios, aliados y colaboradores. Además, la capacitación, el control y la mejora continua son pilares fundamentales para adaptarnos a un entorno tecnológico dinámico y en constante evolución.

Reafirmamos el compromiso de CIRTEL con la protección de la información como un activo estratégico, garantizando así un servicio confiable y seguro para todos.