GRUPO

LÍNEA DIRECTA ASEGURADORA

POLITICA DE CIBERSEGURIDAD

Información importante sobre este documento

Nombre de la Política	**POLITICA DE CIBERSEGURIDAD**
Apartado del Código Ético de Grupo Línea Directa que desarrolla	**3, 4, 10, 14**
Apartado de otras Políticas que desarrolla	**Ninguna**
Normas que sustituye	**Política de Seguridad de la Información (junio 2022)**
Normas que deroga	**Ninguna**
Normas relacionadas	**Ninguna**
Unidad de negocio o función a la que afecta	**Todas las unidades de negocio del Grupo Línea Directa Aseguradora**
Personal al que afecta	**Todo el personal del Grupo Línea Directa Aseguradora y proveedores de servicios.**
Responsable principal de su vigilancia	**CISO (*Chief Information Security Officer*)**
Fecha de aprobación	**28 de enero de 2025**
Fecha de actualización	
Versión	**Versión 1**
Elaboración	**Ciberseguridad Corporativa**
Aprobación	**Consejo de Administración**

ÍNDICE

1. Propósito del documento

El Grupo Línea Directa (en adelante "Línea Directa" o "la Compañía") reconoce la importancia estratégica de sus activos tecnológicos y de información, que representan un elemento esencial en la generación y entrega de valor a sus clientes y partes interesadas. Asimismo, la ciberseguridad se encuentra posicionada en las dimensiones del plan de Sostenibilidad de la Compañía.

La presente Política establece los principios generales, las responsabilidades y la visión de Línea Directa con respecto a la seguridad de la información y ciberseguridad con el objetivo de proteger la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los sistemas que albergan información de la Compañía, garantizando el cumplimiento de normativas legales, contractuales y estándares internacionales relativos a ciberseguridad.

2. Objetivo de la Política

El objetivo de esta Política es establecer un marco integral para el gobierno y control de la ciberseguridad en Línea Directa que proporcione un nivel de madurez adecuado para gestionar las amenazas y riesgos de ciberseguridad de la Compañía.

3. Alcance

Este documento aplica a todo el personal de Línea Directa, así como a proveedores y terceras partes que accedan, procesen o manejen información de la Compañía, dando cobertura a todos los sistemas, aplicaciones, infraestructuras y activos que almacenen, transmitan o procesen información.

Asimismo, esta Política podrá ser complementada por las diferentes normas, procedimientos y estándares desarrollados por el departamento de Ciberseguridad Corporativa.

4. Principios generales

Línea Directa establece los siguientes principios fundamentales como la base efectiva para definir una estrategia de gestión de la seguridad de la información y ciberseguridad, así como para mitigar los riesgos asociados a las amenazas de ciberseguridad:

- **Confidencialidad**: garantizar que la información está adecuadamente protegida contra accesos no autorizados.

- **Integridad:** garantizar la exactitud, fiabilidad y completitud de la información, protegiéndola ante cambios no autorizados**.**

- **Disponibilidad:** garantizar el acceso a la información cuando se requiera por parte de las personas, procesos o sistemas autorizados.

- **Autenticidad:** garantizar la identidad de las entidades (usuarios, sistemas, etc.) y/o las fuentes de las que proviene la información, asegurando que dicha información es genuina y no ha sido alterada. Está relacionado con el principio de no repudio.

- **Trazabilidad:** garantizar el seguimiento de la información a lo largo de su ciclo de vida, permitiendo identificar su origen, modificaciones y accesos. Se asegura así que cualquier cambio o acceso a la información puede ser auditado y verificado.

5. Capacidades de Ciberseguridad

Los principios generales son desarrollan a través del siguiente conjunto de capacidades de ciberseguridad, alineadas con las mejores prácticas y estándares del mercado:

- **Gobernar:** Capacidades relacionadas con el alineamiento de los principios de ciberseguridad de la Compañía con todas las partes interesadas, gestionando adecuadamente las dependencias, y con los requisitos legales, normativos y contractuales; así como establecer, comunicar y priorizar adecuadamente las acciones en la gestión de amenazas y riesgos de ciberseguridad; definir y comunicar adecuadamente el contexto, las funciones, responsabilidades y competencias; establecer, comunicar e implementar la política y normativas de ciberseguridad, asegurando su cumplimiento y mantenimiento; supervisar los resultados de la gestión de riesgos de ciberseguridad y gestionar adecuadamente los riesgos de ciberseguridad de los proveedores TIC.
- **Identificar:** Capacidades relacionadas con la identificación, análisis y tratamiento de los riesgos y amenazas de ciberseguridad que puedan comprometer los procesos, servicios y activos de la Compañía, con especial foco en aquellos que son esenciales para Línea Directa.

- **Proteger:** Capacidades relacionadas con la protección de los activos identificados según su criticidad ante amenazas y riesgos de ciberseguridad a través de:

    - El diseño y construcción de productos y servicios digitales seguros.

    - La implementación de mecanismos de control de acceso basados en la identidad y en el principio de necesidad de conocer.

    - La protección de las comunicaciones tanto internas como externas.

    - El control de las operaciones de los activos.

- La gestión de las claves criptográficas.
- El fomento de una cultura adecuada en materia de ciberseguridad.

- **Detectar:** Capacidades relacionadas con la detección de amenazas y vulnerabilidades de ciberseguridad a través de:
  - La vigilancia de los productos y servicios digitales.
  - La monitorización de las comunicaciones.
  - La supervisión de la infraestructura tecnológica.
  - La detección y clasificación de ciberamenazas y eventos adversos, tanto internos como externos, que puedan impactar en los activos de Línea Directa.

- **Responder:** Capacidades relacionadas con el establecimiento, gestión y pruebas de los planes de respuesta ante la materialización de amenazas de ciberseguridad y la comunicación con las partes interesadas, incluyendo aquellas exigidas por legislación, regulación o contratos.

- **Recuperar:** Capacidades relacionadas con la resiliencia de los activos de Línea Directa para recuperarse del impacto ante eventos adversos de ciberseguridad y volver lo antes posible a la situación normal e identificar lecciones aprendidas para evitar la reproducción futura de dichos eventos.

Todas estas capacidades se implementarán a través de una Estrategia de ciberseguridad que defina y despliegue el marco de actuación de la Compañía alineado con las mejores prácticas del mercado.

6. Modelo de Gobierno

La Compañía contará con un Equipo Técnico de Resiliencia Operativa Digital configurado como un equipo de expertos que dan apoyo al Comité Permanente de Riesgos y que reportará trimestralmente a la Comisión de Auditoría y periódicamente al Consejo. Entre sus competencias, se incluyen:

- Proponer y monitorizar la estrategia de resiliencia operativa digital y supervisar la Estrategia de ciberseguridad, su avance y el grado de madurez de la Compañía.
- El estado de amenazas de ciberseguridad y los riesgos relacionados con las TIC.

La función de la Ciberseguridad reside en el departamento de Ciberseguridad Corporativa a través del CISO (*Chief Information Security Officer*), enmarcado dentro del área de Tecnología y Ciberseguridad de Línea Directa.

7. Responsabilidades

Línea Directa establece las siguientes responsabilidades en materia de ciberseguridad:

7.1 Consejo de Administración

- Aprobar y supervisar la Estrategia de ciberseguridad de la Compañía, así como la Política y la misión de ciberseguridad.
- Asumir la responsabilidad última de gestionar el riesgo relacionado con las TIC de la Compañía.
- Asignar y revisar periódicamente la adecuación del presupuesto y recursos designados para satisfacer las necesidades de la Estrategia de ciberseguridad y de la resiliencia operativa digital.
- Mantenerse actualizado y contar con conocimientos y capacidades suficientes para comprender y evaluar el riesgo relacionado con las TIC y las amenazas de ciberseguridad, y su posible impacto en la Compañía.

7.2 Dirección de Tecnología y Ciberseguridad

- Promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la implantación de los principios generales de ciberseguridad.
- Fomentar una cultura de ciberseguridad en la Compañía.
- Establecer canales de comunicación para mantenerse informado de los incidentes graves relacionados con las TIC y sus repercusiones, así como de las medidas de respuesta, recuperación y corrección.
- Aprobar el documento de especificación del alcance de las pruebas de penetración basadas en amenazas.

7.3 Departamento de Ciberseguridad Corporativa

- Implantar mecanismos de detección de actividades anómalas y definir umbrales de alerta y escalado, así como planes de respuesta y gestión de incidentes de ciberseguridad.
- Planificar y gestionar la definición y ejecución de pruebas avanzadas de penetración basadas en amenazas sobre los sistemas en producción con una periodicidad de tres años.
- Definir un plan de recuperación ante incidentes de ciberseguridad que incluya los escenarios de incidentes de ciberseguridad que se consideren más relevantes para Línea Directa.

- Aplicar mecanismos que limiten el acceso a los activos de información y activos TIC de la Compañía y establecer a tal fin un conjunto de políticas, procedimientos y controles que se centren en los derechos de acceso y garanticen una buena administración de los mismos.
- Velar por la seguridad de los activos digitales de Línea Directa.
- Revisar anualmente la Estrategia de ciberseguridad, Política de ciberseguridad, así como las normas y procedimientos incluidos en el Cuerpo normativo de ciberseguridad de la compañía; o ante cualquier cambio relevante, ya sea interno o externo, con el objetivo de proteger los principios generales de ciberseguridad.
- Desarrollar los contenidos de concienciación y formación específicos relacionados con la gestión de la ciberseguridad y del riesgo tecnológico, así como la formación específica necesaria para el área de ciberseguridad y la gestión del riesgo TIC.

7.4 Empleados y colaboradores

- Cumplir con todas las políticas, procedimientos y normas derivadas de la presente Política.
- Participar en las iniciativas de formación y concienciación en ciberseguridad.
- Proteger la información y los activos, preservando el acceso y previniendo cualquier tipo de filtración o comunicación no necesaria, y usándola solamente para los propósitos autorizados.
- Clasificar la información de acuerdo con la normativa de clasificación y manejo de información.
- Reportar lo antes posible los potenciales incidentes, brechas o violaciones de seguridad que detecten.
- Preservar las credenciales de acceso, no revelándolas a terceros y utilizándolas únicamente para acceder a las aplicaciones corporativas.

7.5 Propietarios de los datos y los sistemas

- Definir los niveles de clasificación de sus activos de información.
- Autorizar y revisar periódicamente los derechos de acceso y roles a los sistemas y datos de su propiedad.
- Garantizar la aplicación de controles de seguridad adecuados.
- Participar en evaluaciones de riesgos y revisiones de seguridad.

- Colaborar en la definición de las medidas y necesidades de seguridad de los sistemas y los datos y los requisitos de recuperación.
- Apoyar las investigaciones de incidentes de seguridad.
- Garantizar el cumplimiento de las políticas de seguridad de sus activos.

7.6 Consecuencias del incumplimiento

Cualquier vulneración de la presente política o de las normas y procedimientos que la desarrollen podrá dar lugar a la adopción de medidas conforme a la normativa que sea de aplicación.

8. Misión de la ciberseguridad

Línea Directa tienen por misión garantizar los principios generales de ciberseguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) asumiendo los siguientes compromisos:

8.1 Cumplimiento Normativo

- **Cumplimiento Normativo de Ciberseguridad**: se desarrollará y publicará un Cuerpo Normativo de Ciberseguridad alineado con las principales regulaciones aplicables basado en los estándares y mejores prácticas del mercado, según las necesidades de la Compañía.
- **Revisión y actualización**: se revisará el Cuerpo Normativo al menos una vez al año, así como cuando se producen incidentes graves relacionados con las TIC o cambios relevantes en la Compañía.

8.2 Gestión de Riesgos de ciberseguridad

- **Identificación de riesgos de ciberseguridad**: se identificarán las vulnerabilidades, amenazas y riesgos de ciberseguridad en los sistemas y en la información manejada por los mismos.
- **Evaluación, análisis y mitigación de riesgos de ciberseguridad**: se definirán criterios para la identificación y evaluación de riesgos de ciberseguridad, definiendo planes de acción para remediar y mitigar las debilidades identificadas y la priorización de las medidas que las mitiguen.

8.3 Ciberseguridad en Terceros

- **Evaluación previa**: se definirán requisitos de ciberseguridad para terceros TIC antes de establecer relaciones contractuales.

- **Contratos y acuerdos**: se garantizará la incorporación de cláusulas relacionadas con medidas de ciberseguridad en los contratos con proveedores TIC.

- **Supervisión continua**: se realizará una monitorización, reportes de cumplimiento y evaluación del desempeño de terceros TIC garantizando el cumplimiento de lo establecido a nivel contractual en materia de ciberseguridad.

- **Plan de respuesta a incidentes de terceros**: se definirán procedimientos específicos para gestionar incidentes de ciberseguridad que involucren a proveedores TIC.

8.4 Gestión de Activos de ciberseguridad

- **Inventario de activos de ciberseguridad**: se definirá y mantendrá actualizado un registro de activos relacionados con el ámbito de la ciberseguridad.

- **Protección de activos**: se implementarán medidas de ciberseguridad durante el ciclo de vida de los activos identificados y registrados dentro del inventario (planificación, desarrollo, implementación y mantenimiento/operación).

- **Etiquetado y clasificación de información:** se definirán reglas para identificar y clasificar los activos de información de la Compañía.

- **Controles de información:** se implementarán controles específicos de ciberseguridad, basados en los mecanismos de etiquetado y clasificación de la información.

- **Eliminación segura**: se establecerán mecanismos para la destrucción segura de información que serán de aplicación según su nivel de clasificación.

8.5 Gestión de vulnerabilidades y parcheado

- **Identificación de vulnerabilidades**: se desplegarán herramientas y procesos para el escaneo periódico que permita la detección y tratamiento de vulnerabilidades.

- **Evaluación de vulnerabilidades**: se priorizarán y evaluarán las vulnerabilidades según su criticidad, garantizando que se dispone de las capacidades tanto técnicas como personales para recopilar y analizar dicha información.

- **Plan de parcheado**: se dispondrá de mecanismos que permitan la aplicación de actualizaciones y parches de seguridad en los activos y sistemas de la Compañía.

- **Monitorización, validación y mejora continua**: se realizará una verificación posterior al parcheo y se definirá un proceso de supervisión continua para identificar nuevas vulnerabilidades.

- **Pruebas de penetración**: se llevarán a cabo pruebas de penetración basadas en amenazas y pruebas de penetración avanzadas sobre sistemas que sustenten funciones esenciales o importantes.

8.6 Gestión de accesos

- **Control de identidades**: se definirán requisitos de control de accesos a los sistemas de información alineados con la clasificación de la información que contienen y al perfil de riesgo del activo TIC.

- **Autenticación y autorización**: se implementarán mecanismos de autenticación fuerte para el acceso remoto a la red, el acceso de usuarios privilegiados y el acceso a activos TIC que soporten funciones críticas, importantes o de acceso público.

- **Principio de mínimo privilegio**: se restringirá y controlará la asignación y uso de derechos de acceso privilegiado y se basarán en el principio de necesidad de conocer.

- **Gestión de cuentas privilegiadas y no privilegiadas**: se definirán procedimientos formales para altas, bajas y modificaciones de usuarios.

- **Monitorización de accesos**: se implementarán registros de acceso a los sistemas y datos que permitan la trazabilidad de las acciones de los usuarios. Adicionalmente, se revisarán periódicamente los derechos de acceso por parte de los responsables de los activos.

8.7 Concienciación y formación en ciberseguridad

- **Programas de formación**: se desarrollarán programas y acciones formativas en materia de ciberseguridad aplicables tanto a empleados, proveedores TIC como a la Dirección y tendrán un nivel de complejidad acorde con las atribuciones de sus funciones.

- **Simulacros y ejercicios**: se realizarán ejercicios y campañas periódicas de simulaciones de ataques sobre los empleados y usuarios externos de la Compañía con el fin de concienciar y formar en materia de ciberseguridad.

- **Campañas de sensibilización**: se desarrollarán campañas de sensibilización en materia de ciberseguridad tanto para empleados como para proveedores TIC con el fin de reforzar buenas prácticas y generar una cultura de ciberseguridad.

8.8 Cifrado y criptografía

- **Gestión de claves**: se definirán procedimientos seguros para la generación, almacenamiento, métodos de reemplazo de claves en caso de pérdida, compromiso o daño, y eliminación de claves criptográficas.
- **Cifrado de datos sensibles**: se definirán e implementarán métodos de cifrado de la información tanto en tránsito como en reposo.
- **Revisión de algoritmos criptográficos**: se realizarán revisiones periódicas de las técnicas criptográficas conforme las mejores prácticas, avances tecnológicos y amenazas emergentes.

8.9 Gestión de amenazas

- **Identificación de amenazas**: se llevará a cabo una identificación proactiva de amenazas de ciberseguridad basada en fuentes fiables de información e inteligencia, que se complementarán con el uso de herramientas de detección temprana.
- **Análisis y respuesta de amenazas**: se realizarán evaluaciones del impacto potencial de cada amenaza identificada previamente para definir planes que permitan gestión, respuesta y mitigación.

8.10 Gestión de Incidentes

- **Detección y notificación**: se definirán mecanismos para identificar y reportar incidentes tanto internamente como a terceras partes implicadas y a organismos supervisores, identificando los roles y el personal responsable de llevar a cabo dichas acciones.
- **Análisis y priorización**: se evaluará el alcance y severidad de los incidentes, registrando toda la información necesaria para su posterior análisis.
- **Respuesta a incidentes**: se definirán planes de acción para contener y dar respuesta a los incidentes y permitan recuperar la disponibilidad e integridad de los sistemas afectados en el menor tiempo posible.
- **Lecciones aprendidas**: se realizarán análisis post incidente para mejorar los controles y procesos afectados, así como para identificar patrones y mejorar los planes de respuesta.