POLÍTICA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD PLANOK

1. INTRODUCCIÓN

La presente Política de Seguridad de la Información y de Ciberseguridad, en adelante la "Política", establece los principios y directrices que **PLANOK** directores, ejecutivos y trabajadores deben asumir para garantizar la preservación de la confidencialidad e integridad de cualquier tipo de información que posea valor para la empresa, y la disponibilidad y resiliencia de las redes y los sistemas informáticos en que se almacene dicha información y en los que se apoyan los diferentes procesos de negocio.

PLANOK deberá desplegar todas las acciones para minimizar los riesgos y las ciberamenazas a los que están expuestos los activos de información, redes y sistemas informáticos de **PLANOK**, de manera que pueda cumplir su objeto social para con los clientes y otros grupos de interés.

La presente Política establece los lineamientos para identificar los activos de información críticos para **PLANOK**, así como para clasificarlos en función de su importancia, sensibilidad y valor. Considera, además, asignar a cada activo de información un propietario responsable de su protección y la gestión adecuada estará entregada a un custodio, quien velará por su integridad y confidencialidad.

Los activos de información de **PLANOK** abarcan una amplia gama de recursos, como bases de datos personales de clientes o terceros, información financiera, patentes, desarrollos, códigos fuentes, comunicaciones internas. La correcta gestión de estos activos es fundamental para mantener la confianza de los clientes y garantizar la continuidad de las operaciones de **PLANOK**.

2. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Esta Política tiene un alcance amplio y se aplica a directores, ejecutivos y trabajadores de **PLANOK** y a sus empresas relacionadas. **PLANOK SPA** las sociedades que forman parte del mismo grupo empresarial, por lo que cuando se haga mención de **PLANOK** se estará haciendo referencia a todas las empresas del grupo. Además, se aplica a todos aquellos que presten servicios a **PLANOK**, así como a los terceros que acceden, utilizan o manejan activos de información, redes o sistemas informáticos de **PLANOK**.

Por otra parte, esta Política se extiende a todos los activos de información, independientemente de su ubicación física o digital, dentro o fuera de las instalaciones de **PLANOK**, en Chile o en el extranjero, contenidos en dispositivos o alojados en servicios de internet en la nube, y que tengan un valor para **PLANOK.**

Los activos de información comprenden:

- **Información**:
- **Datos**: Toda información recopilada y mantenida en bases físicas o digitales que contienen datos de clientes, datos personales, datos de plataforma, información organizacional, y

cualquier otra información utilizada en las operaciones de **PLANOK**.

- **Documentación**: Esto comprende todos los documentos físicos o electrónicos que contienen información técnica sobre funcionamiento de sistemas y aplicaciones manuales de procedimientos, políticas internas, contratos, acuerdos de confidencialidad y cualquier otro documento que sea necesario para la gestión de la información de **PLANOK**.

- **Redes y Sistemas Informáticos**: Conjunto de dispositivos, servidores, ordenadores, portátiles, dispositivos móviles, unidades de almacenamiento, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas o aplicaciones que recopilan, almacenan, procesan, transmiten o comunican datos digitales.

3. OBJETIVO DE LA PRESENTE POLÍTICA

El objetivo de la presente Política es salvaguardar la información que posea valor para las operaciones de **PLANOK** y garantizar el cumplimiento normativo, protegiendo la confidencialidad e integridad de la información, y la disponibilidad y resiliencia de las redes y de los sistemas informáticos.

4. PRINCIPIOS DE LA PRESENTE POLÍTICA

Proteger la información no es solo una responsabilidad técnica, sino también una obligación ética y legal. **PLANOK** se rige por los siguientes principios en relación con la seguridad de la información y la ciberseguridad. Para efectos de lograr una correcta implementación de la presente Política, se requiere la comprensión sólida y el compromiso de todos quienes acceden a la información de sus principios básicos.

- **Confidencialidad**: La confidencialidad protege a la información contra del acceso no autorizado. Lo anterior significa que solo las personas autorizadas deben tener acceso a ciertos datos. Toda la información será utilizada exclusivamente por quienes se encuentren autorizados por **PLANOK**, para cumplir el objeto y finalidad para la cual es generada o recopilada, y no será revelada ni divulgada a terceros sin autorización previa, escrita y expresa de **PLANOK** o de sus titulares según corresponda.
- **Integridad**: La integridad asegura que la información no será alterada o destruida de manera no autorizada, lo anterior significa que los datos deben ser precisos y completos. Cualquier operación debe ser realizada por personas autorizadas y registradas adecuadamente.
- **Disponibilidad**: La disponibilidad consiste en que la información se encuentre disponible y utilizable cuando se necesite. Es fundamental que los datos y los servicios estén disponibles para los usuarios autorizados en todo momento, sin interrupciones.
- **Autenticación:** La autenticación es el proceso de verificación de la identidad de un usuario o dispositivo antes de permitirle el acceso a un sistema o información.
- **Autorización**: Una vez autenticado, el sistema debe verificar si el usuario tiene los derechos necesarios para acceder a ciertos recursos o realizar determinadas operaciones.
- **No repudio:** El no repudio garantiza que una persona no pueda negar la autoría de una acción realizada en un sistema.
- **Evaluación de riesgos:** La evaluación de riesgos es el proceso de identificar, analizar y evaluar

las amenazas potenciales a la seguridad de la información, de modo de poder priorizar las medidas de seguridad y asignar recursos de manera eficiente.

- **Gestión de riesgos:** Todos los riesgos identificados contarán con un propietario del riesgo, quien deberá proponer un plan de tratamiento de los riesgos identificados y asegurar la ejecución del plan para mitigar los mismos. El propietario del riesgo será el propietario del activo y a su vez será la persona designada por el Gerente de Innovación, Tecnología, Ciberseguridad y Datos. Se entiende por propietario del riesgo quien tiene la responsabilidad y la autoridad para gestionar el riesgo.
- **Seguridad y privacidad por defecto y desde el diseño**: Los sistemas informáticos y aplicaciones deben diseñarse, implementarse y gestionarse teniendo en cuenta la seguridad y la privacidad de los datos personales que procesan. Dichos proyectos deberán pasar por una evaluación provista por el área de TI, quien realizará una prueba de seguridad en base al estándar OWASP con el fin de evitar posibles amenazas o incidentes.
- **Responsabilidad**: Toda persona que ocupa un cargo, función o posición en **PLANOK** incluyendo directores, ejecutivos principales, trabajadores y todos aquellos que presten servicios como proveedores, asesores, así como los terceros a quienes se les comuniquen, acceden, utilicen o manejen activos de información de **PLANOK** son responsables de cumplir con las leyes sobre tratamiento de protección de datos personales, las políticas y procedimientos de seguridad de la información que **PLANOK** elabore.

5. GOBIERNO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- **Responsabilidades**

La Gerencia General tiene la responsabilidad de liderar y respaldar la implementación de la Política de la Seguridad de la Información y Ciberseguridad y del resto de las políticas y/o procedimientos afines. Para tales efectos, deberá proporcionar los recursos necesarios, establecer objetivos y supervisarlos regularmente para evaluar su eficacia. Además, la Gerencia General debe garantizar que se establezca un marco de gestión de riesgos de seguridad de la información, asignar roles y responsabilidades claras dentro de la organización.

- **Gestión de la Seguridad de la Información y la Ciberseguridad:**

La Gerencia de Innovación, Tecnología, Ciberseguridad y Datos encabeza la Gestión de la Seguridad de la Información de **PLANOK** supervisar y monitorear las actividades relacionadas con la Política de Seguridad de la Información. Le caben las siguientes acciones concretas:

- Identificar las mejores prácticas sobre Seguridad de la Información y Ciberseguridad.
- Monitorear el debido cumplimiento de esta Política y velar por la implementación de otras políticas o procedimientos que permitan el cumplimiento de las normas Seguridad de la Información y Ciberseguridad.
- Fomentar una cultura de seguridad de la información en toda la organización y coordinar las capacitaciones para que los trabajadores conozcan las normas sobre Seguridad de la Información y Ciberseguridad, conforme al plan de capacitaciones que **PLANOK** elaborará y comunicará.

- Coordinar la identificación y clasificación de activos de información y asegurarse de que se asignen propietarios responsables y custodios.
- Realizar evaluaciones de riesgos y gestionar las vulnerabilidades y amenazas identificadas implementando medidas de mitigación adecuadas.
- Actuar como punto focal para la gestión de incidentes de seguridad de la información, coordinando la respuesta a incidentes, investigando y documentando los incidentes, y tomando medidas correctivas para evitar futuras incidencias.

- **Propietarios, custodios y usuarios de activos de información:**

- **Propietario de activos de información**: Cada activo de información debe tener un propietario designado, que sea responsable de su protección y gestión adecuadas. El propietario del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso. Los propietarios tienen la responsabilidad de:
    - Identificar y clasificar los activos de información bajo su propiedad, asegurándose de comprender su importancia y sensibilidad.
    - Establecer controles de seguridad adecuados para proteger los activos de información, basados en las evaluaciones de riesgos y los requisitos de seguridad.
    - Definir los requisitos de acceso y autorización para los activos de información, asegurándose de que sólo se otorguen los privilegios necesarios para la ejecución de sus funciones.
    - Colaborar con otros propietarios de activos de información y garantizar una gestión coherente y eficaz de los activos de información en toda la organización.

- **Custodio**: Se entiende por **custodio** al encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

- **Usuarios o Trabajadores:** Quien genere, obtenga, transforme, conserve o utilice la información para propósitos propios de su labor.

- Sin perjuicio de lo anterior, todos tienen responsabilidades en la seguridad de la información y deben cumplir con esta Política y los procedimientos que de ella deriven. Esto incluye:

- Conocer y cumplir la Política y procedimientos de seguridad de la información y ciberseguridad de **PLANOK**, incluida la clasificación de los activos de la información y el manejo adecuado de la información.
- Participar en programas de capacitación y concientización sobre seguridad de la información para comprender los riesgos y las mejores prácticas de seguridad.
- Informar cualquier incidente de seguridad o vulnerabilidad detectada a seguridad@planok.com y cooperar en la resolución de dichos incidentes.
- Utilizar los activos de información de manera responsable y asegurarse de protegerlos contra pérdidas, robos o daños físicos.

6. PLAN DE MEDIDAS DE SEGURIDAD MÍNIMAS:

Las medidas de seguridad de la información implementadas son aplicables a todos quienes interactúan con información que posea un valor para **PLANOK**, y consideran a lo menos:

- **Acuerdos de Confidencialidad y Cláusulas de Seguridad:** En los acuerdos de confidencialidad se define claramente la responsabilidad de los directores, ejecutivos, trabajadores, prestadores de servicios o aliados comerciales, para proteger la información confidencial y cumplir con las políticas de seguridad de la información de **PLANOK**.
- **Gestión de sesiones:** Se trata de controles para gestionar y controlar las sesiones de usuario, incluyendo el cierre automático de sesiones inactivas, el registro de actividad de inicio de sesión y la detección de actividades sospechosas.
- **Control de Acceso, autenticación y revocación de acceso:** Los directores, ejecutivos, trabajadores y prestadores de servicios o aliados comerciales deben acceder solo a los recursos y datos necesarios para llevar a cabo sus funciones. Para lo anterior, se ha desarrollado un procedimiento para gestionar los permisos de acceso a los activos de información, asegurando que los usuarios tengan los derechos y privilegios adecuados según sus funciones y responsabilidades. Además, se revisarán y actualizarán regularmente los derechos de acceso para evitar privilegios innecesarios o no autorizados. En ese mismo procedimiento se establecen las reglas para revocar el acceso a quienes hayan dejado de pertenecer a la empresa, o ya no sean prestadores de servicios ni aliados comerciales. Se debe mantener implementado y operativo un sistema autenticación segura y multifactorial y el uso de contraseñas seguras.
- **Capacitación y Sensibilización**: Se cuenta con un plan de capacitación dirigido a directores, ejecutivos, trabajadores, prestadores de servicios o aliados comerciales sobre las políticas de seguridad de **PLANOK** y las mejores prácticas para proteger la información confidencial, según la función desarrollada en **PLANOK**, incluyendo la detección de software malicioso, el manejo seguro de archivos adjuntos y enlaces, y las prácticas recomendadas para evitar infecciones.
- **Revisión de Prácticas de Seguridad:** Se considera la realización de 1 a 2 auditorías anuales para verificar que los a directores, ejecutivos, trabajadores, prestadores de servicios o aliados comerciales cumplen con las políticas de seguridad y las medidas acordadas. También, se considera la evaluación proactiva que tiene como objetivo detectar o identificar amenazas o vulnerabilidades en aplicaciones web y móviles (Ethical Hacking). Los resultados de estas evaluaciones ayudan a la empresa a planificar qué hacer para responder y gestionar el riesgo.
- **Cifrado y Protección de Datos:** Se considera el cifrado respecto de aquellos datos sensibles que **PLANOK** considere necesario, sea que se trate de información en tránsito o reposo.
- **Separación de entornos de desarrollo, prueba y producción.** Los ambientes de Desarrollo, Pruebas y Producción de **PLANOK** deberán estar separados para reducir riesgos de acceso no autorizado o cambios en el entorno operacional. Se definen los ambientes como

- Ambiente de Desarrollo (DEV): Es el ambiente en donde se implementan cambios y nuevas funcionalidades en el software. Generalmente se incluye el uso herramientas de desarrollo como IDEs, distintas versiones de librerías, software de control de versiones y/o plataformas online.
- Ambiente de Pruebas (Testing & QA): Es el ambiente en donde se realizan pruebas manuales y chequeos automatizados para verificar el correcto funcionamiento de la aplicación para todos los casos de prueba definidos.

- Ambiente de Producción: Es el ambiente en donde se aloja la versión probada del software en donde los usuarios finales podrán interactuar directamente con ella.

- **Procedimiento de reacción ante brechas e incidentes:**

- **Notificación de brechas e incidentes:** Contamos con un plan de acción claro en caso de una violación de seguridad. Esto incluye notificar a las partes afectadas, al cliente y a la autoridad del control si fuere del caso, y a tomar medidas para mitigar los daños.
- **Plataformas Seguras: PLANOK** utiliza plataformas y servicios seguros para compartir información confidencial, certificados de seguridad SSL, sistemas de seguridad perimetral que controlan y monitorean el tráfico entrante y saliente, y para prevenir ataques externos no autorizados. Se realizan revisión de las plataformas, versiones, actualizaciones, protocolos, estándares, soluciones antivirus y antimalware actualizadas y eficaces en todos los sistemas y dispositivos, aplicación oportuna de parches críticos y la realización de pruebas de seguridad posteriores a la implementación.
- **Eliminación de la información: PLANOK** elimina la información cuando se cumple el objetivo tenido a la vista para su obtención.
- **Procedimientos de respaldo y recuperación de datos en caso de pérdida de datos: PLANOK** cuenta con un sistema de respaldo diario de los datos con plazos de retención.
- **Planes de continuidad del negocio y resiliencia en caso de desastres o interrupciones: PLANOK** cuenta con un sistema DRP que mantiene sincronizados los datos de forma diaria para poder operar ante cualquier incidente grave de disponibilidad.
- **Medidas específicas respecto de proveedores de servicios y aliados comerciales**
    - **Informe de Brechas e Incidentes: PLANOK** exige a sus proveedores de servicios y aliados comerciales, mediante cláusulas incorporadas en acuerdos o convenios, informar cualquier brecha o incidente de seguridad de manera inmediata.
    - **Evaluación de Riesgos: PLANOK** realizará una evaluación inicial de seguridad para los proveedores de servicios y aliados comerciales con el objeto de determinar si se ajustan a las medidas de seguridad según el nivel de riesgo del tratamiento, o si se deben tomar medidas de resguardos especiales, siendo válidas para estos efectos las certificaciones en materia de seguridad de la información o ciberseguridad que puedan acreditar.

7. POLÍTICAS QUE FORMAN PARTE INTEGRANTE DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Forman parte del Sistema de Seguridad de la Información y Ciberseguridad todas las políticas que PLANOK ha elaborado al efecto.

8. CONSECUENCIAS DEL INCUMPLIMIENTO DE LAS POLÍTICAS Y PROCEDIMIENTOS QUE FORMAN PARTE DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Toda infracción o incumplimiento a esta política y las que forman parte integrante del sistema de seguridad de la información y ciberseguridad y que se identifican en el punto anterior, será sancionado conforme a lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad de **PLANOK** o con el término del contrato por alguna de las causales que establece el Código del Trabajo en el artículo 160, sin perjuicio de las acciones judiciales que puedan dirigirse contra el

transgresor para hacer efectiva su responsabilidad tanto civil como penal.

Toda infracción o incumplimiento de esta Política por parte todos aquellos que presten servicios a **PLANOK** como contratistas, proveedores, asesores, así como los terceros que acceden, utilizan o manejan activos de información, dará lugar a la aplicación de las sanciones o consecuencias de acuerdo con lo previsto en los respectivos contratos, sin perjuicio de las acciones judiciales que puedan dirigirse para hacer efectiva la responsabilidad tanto civil como penal.

9. PREVENCIÓN DE DELITOS INFORMÁTICOS

La gestión adecuada de la seguridad de la información y ciberseguridad mejora los procesos corporativos, evita el acceso no autorizado a información que posee valor para **PLANOK**, y crea un entorno de control que previene conductas delictivas de los trabajadores en el ámbito informático.

En este sentido, todo el que ocupa un cargo, función o posición en **PLANOK** incluyendo a directores, ejecutivos y trabajadores, proveedores o asesores, así como los terceros que acceden, utilizan o manejan activos de información de **PLANOK**, tienen prohibido cometer conductas ilícitas a través de medios informáticos o en contra de sistemas informáticos. Dichas conductas se encuentran sancionadas en la Ley N°21.459, que establece normas sobre delitos informáticos, los cuales se describen a continuación.Para poder comprender de mejor manera, la ley se encarga de definir los siguientes conceptos:

- **Datos informáticos:** Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.
- **Sistema informático:** Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
- **Prestadores de servicios:** Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

Delitos tipificados en la ley:

- **Ataque a la integridad de un sistema informático, artículo 1 Ley Nº 21.459 (sabotaje informático):** Se refiere a la obstaculización o impedimento del normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos
- **Acceso ilícito, artículo 2° ley 21.459:** Se refiere al acceso a un sistema informático sin autorización o excediendo la autorización que se posea y superando barreras técnicas o medidas tecnológicas de seguridad. La pena se agrava si el acceso fuera realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático. También se castiga la divulgación de la información a la cual se accedió de manera ilícita.
- **Interceptación ilícita, artículo 3° ley 21.459:** Interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático o entre

dos o más de aquellos. También captar, sin contar con la debida autorización, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos

- **Ataque a la integridad de los datos informáticos (sabotaje de datos), artículo 4° ley 21.459:** Alterar, dañar o suprimir indebidamente datos informáticos, siempre que con ello se cause un daño grave al titular de estos mismos.
- **Falsificación informática, artículo 5° ley 21.459**: Introducir, alterar, dañar o suprimir indebidamente datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.
- **Receptación de datos informáticos, artículo 6° ley 21.459:** Se sanciona al que, conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas de acceso ilícito, interceptación ilícita y falsificación informática.
- **Fraude informático, artículo 7° ley 21.459:** Manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero. Para los efectos de este delito se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta ya descrita, facilita los medios con que se comete el delito.
- **Abuso de los dispositivos, artículo 8° ley 21.459:** Sanciona al que para la perpetración de los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos y delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos.
- **Agravantes**: Conforme a lo establecido en el artículo 10 de la Ley 21.459, se considerarán como agravantes para los delitos contemplados en la misma ley, cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función. El efecto que tiene esta circunstancia agravante es el de aumentar en un grado la pena prevista ante la comisión de uno de los delitos contemplados en la Ley 21.459.

10. COMUNICACIÓN DE LA POLÍTICA

Para asegurar la efectiva implementación de esta Política, es fundamental que todos quienes utilizan información de valor para **PLANOK** la conozcan y adhieran a ella.

La información relacionada a la presente Política estará disponible en las redes de comunicación internas y externas y se difundirá y capacitará sobre buenas prácticas, controles, obligaciones y prohibiciones para prevenir la comisión de infracciones a la presente política, ley sobre protección de datos personales y delitos informáticos.

11. VIGENCIA DE LA PRESENTE POLÍTICA Y FECHA DE PUBLICACIÓN

La presente Política entrará en vigencia a contar de la fecha de su publicación y se comunicará a

través de procesos de capacitación, folletos y charlas informativas al interior de cada una de las áreas de **PLANOK**.

La fecha de publicación de la presente Política es: 28 de abril de 2025.