Política de Seguridad de la Información

Confuturo 2021

Tabla de contenido

I. Introducción

La información es un activo y como tal está expuesto a riesgos y amenazas tales como: deterioro, adulteración, robo, divulgación no autorizada y extravío. Cada una de estas situaciones puede traducirse en pérdidas económicas, daño reputacional, incumplimientos normativos, sanciones por parte de los reguladores, vulneración de derechos de colaboradores, clientes o terceros, entre otros aspectos adversos.

La información es, junto con las personas, procesos y tecnología, uno de los activos más importantes de las organizaciones. Por su trascendental importancia para la toma de decisiones estratégicas y operación de sus procesos, la información debe ser resguardada y protegida de una serie de riesgos y amenazas a los cuales está expuesta, tales como desastres naturales, fraudes e ilícitos y ataques informáticos.

Estos riesgos y amenazas, provienen tanto del interior como del exterior de la organización y evolucionan a través del tiempo con la adopción de nuevas tecnologías y los cambios en el entorno, lo que demanda un monitoreo y gestión constantes.

Confuturo S.A. (en adelante, la Compañía), entiende esta necesidad y define una serie de lineamientos y directrices con el objetivo de proteger la información de sus procesos, clientes y colaboradores,

II. Propósito (Objetivo)

La presente política tiene como propósito establecer los criterios, directrices y obligaciones que deben guiar a las distintas áreas y estamentos de la organización en la gestión de la seguridad de los activos de información de la Compañía, a lo largo de todo su ciclo de vida, con el objetivo de garantizar niveles de confidencialidad, integridad y disponibilidad que permitan, mantener la continuidad del negocio, satisfacer la legislación y normativa vigente y, el cumplimiento de los estándares que la Compañía establezca al respecto.

Un debido cuidado de estos tres pilares de la seguridad de la información permitirá a la Compañía tomar decisiones oportunas con información fidedigna, asegurando la obtención de los resultados esperados.

También esta política busca asegurar que las definiciones sobre gestión de la Seguridad de la Información establecidas sean consideradas e incorporadas adecuadamente en los objetivos y procesos de negocios de la Compañía. En particular, con esta política se debe asegurar que:

a) Se desarrollen procedimientos de resguardo de información

b) Se capacite al personal de la Compañía en la protección de la información

c) Se fomente el cumplimiento de los principios de Conducta de Mercado, en especial se vele por el cumplimiento de la protección de la información de los clientes

d) Se implementen controles internos para verificar los adecuados niveles de protección

e) Se cuente con la tecnología adecuada para resguardar la información

f) Se identifiquen y manejen los riesgos y amenazas a la seguridad de la información, en los principios de confidencialidad, integridad y disponibilidad

g) Se establezcan planes de contingencia que permitan mitigar los riesgos y el impacto de cualquier filtración o uso indebido de la información.

III. Alcance

Esta política aplica a todos los activos de información de la Compañía, independientemente de la etapa del ciclo de vida en que se encuentren y de los dispositivos o instalaciones en los que se estén generando, capturando, usando, almacenando, transmitiendo o destruyendo. En consecuencia, involucra a todas las personas, procesos, infraestructura y sistemas de la Compañía que reciban, registren, procesen, preserven, transmitan o destruyan información de sus clientes, empleados, proveedores y de negocios, ya sea de manera interna o externalizada.

Esta política afecta entonces la actividad de todos los colaboradores de la Compañía, como así también a proveedores que, por la naturaleza de los servicios que nos prestan, tengan o puedan tener acceso a activos de información de la Compañía. La información que debemos prioritariamente resguardar y proteger corresponde a aquella relacionada con clientes, colaboradores, proveedores y la relacionada con la operación y gestión de los negocios de la Compañía.

IV. Principios

La presente política se basa en los siguientes principios o pilares:

- **Confidencialidad.** Es la propiedad, característica o atributo del activo de información que refleja que sólo debe ser expuesta a personas, entidades y procesos que necesiten acceso a esa información para poder realizar sus roles o funciones debidamente y, que por ello y para ello, cuenten con las autorizaciones correspondientes.

- **Integridad.** Es la propiedad, característica o atributo del activo de información que refleja que se encuentra completa, es exacta y está libre de errores. Para lograr esta característica, la información solo puede ser registrada, modificada o eliminada por personas o procesos debidamente autorizados.

- **Disponibilidad.** Es la propiedad, característica o atributo del activo de información que refleja que debe ser accesible, en el formato apropiado, en el momento en que sea requerido por las personas, entidades o procesos debidamente autorizados para ello.

V. Referencias

Del mismo modo, la presente política se ajusta a lo dispuesto en las siguientes normas aplicables:

- Ley 19223 – Tipifica figuras penales relativas a la informática

- Ley 19628 – Protección de la vida privada
- Ley 20575 – Finalidad en el tratamiento de datos personales

Complementariamente, si bien la Compañía no las aplica íntegramente, también considera las siguientes normas o estándares internacionales como guías para su gestión:

- ISO/IEC 27001
- ISO/IEC 27002

VI. Definiciones (Glosario)

Colaborador. Todo empleado o persona que tenga un contrato de trabajo con la Compañía ya sea indefinido, a plazo fijo o a honorarios.

Información. Son datos que poseen significado y propósito.

Activo de Información. Son todos aquellos bienes que tienen valor para una organización, que interactúan con su información, principalmente almacenándola, transportándola o procesándola, independiente del formato en que éstos se encuentren.

Seguridad de la Información. Es la preservación de la confidencialidad, integridad y disponibilidad de la información, o en su defecto, de los activos de información.

Privilegios de acceso sobre la información. Corresponde al nivel de acceso que se otorga a cada colaborador, dependiendo de las actividades y tareas que deba desempeñar. Estos niveles de acceso pueden ser principalmente de (sólo de) visualización, ingreso y modificación, o eliminación de la información. Estos niveles de acceso se asignan para cada activo de información, sin embargo, por razones de eficiencia y simplicidad, éstos podrían asignarse en la forma de conjuntos o grupos, según sea el caso.

Cifrado de Información. El cifrado (coloquialmente llamado "encriptado"), se refiere a la conversión de datos desde un formato legible a un formato codificado, el cual sólo puede ser leído o procesado después de haber sido descifrado con una llave de cifrado para que vuelva a ser legible. Existen distintos mecanismos y tecnologías para cifrar la información y éstas se utilizan para proteger información de carácter sensible, reservado o confidencial.

Probabilidad. Posibilidad de ocurrencia de un evento que usualmente puede estimarse y expresarse de manera cuantitativa o cualitativa.

Impacto. La consecuencia o efecto de un evento determinado, que puede ser expresado tanto en términos cuantitativos como cualitativos. El impacto puede tener un carácter positivo o negativo.

Riesgo. Es la probabilidad de que ocurra un evento de cualquier tipo que genere un impacto, en el caso de una organización, sobre los objetivos que ésta tenga.

Control. Cualquier acción o medida que modifica (o mantiene) un riesgo.

Incidente. Es la materialización de un riesgo.

Incidente de Seguridad de la Información. Es todo aquel incidente operacional con impacto en los pilares de Seguridad de la Información (confidencialidad, integridad y disponibilidad), específicamente fuga, robo, uso, divulgación, acceso o intento de acceso no autorizado, daño, pérdida, destrucción o modificación no autorizada de información de la Compañía, además de la falla, indisponibilidad y/o daño a sistemas de información, servicios informáticos y/o de comunicaciones de la Compañía y, por cierto, cualquier violación o incumplimiento a la Política de Seguridad de la Información de la Compañía.

VII. Roles y Responsabilidades

Directorio. Provee las directrices para la administración de los riesgos asociados a la Seguridad de la Información al interior de la Compañía. Es responsable de aprobar esta política, la que deberá ser revisada anualmente o antes si hubiese necesidad.

Gerente General. Propone al Directorio cambios a esta política y designa al Presidente del Comité de Seguridad de la Información y al Oficial de Seguridad de la Información. Será función del Gerente General dirimir situaciones de conflicto donde el proceso de evaluación de riesgos dicte, de acuerdo a los reglamentos establecidos, implantar controles para los cuales no se cuente con las herramientas, procesos o presupuestos necesarios. De igual forma, también tendrá la función de dirimir situaciones de conflicto derivadas de decisiones del Comité de Seguridad de la Información (CSI) que pudieren afectar a estrategias de las áreas de negocio. Estas decisiones deberán ser comunicadas al CSI para que controle su aplicación.

Oficial de Seguridad de la Información (OSI). Preside el Comité de Seguridad de la Información. Es responsable de velar por la difusión y el cumplimiento de lo establecido en esta política y los reglamentos y procedimientos derivados de ésta a nivel de la Compañía. Debe proponer las modificaciones que sean necesarias para mantenerlos actualizados en relación con los estándares y normativas vigentes relativas a la seguridad de la información y verificar su cumplimiento al interior de la Compañía. Es también responsable de la adecuada y oportuna capacitación de los colaboradores, de la propuesta y evaluación periódica de los controles internos asociados al cumplimiento y de la oportuna identificación y gestión de los riesgos y amenazas de Seguridad de la Información en la Compañía. Será también responsable de escalar con el Gerente General las situaciones de conflicto entre los controles necesarios para obtener niveles de riesgo aceptables para un activo de información y los requerimientos o necesidades del negocio, en término de controles, procedimientos e inversiones necesarias para su implementación. Debe actuar como un asesor para las distintas áreas de negocio en el ámbito de seguridad y gestión de riesgos. En ausencia de un titular que cumpla este rol de manera exclusiva, el rol de Oficial de Seguridad de la Información recae en el Gerente de Riesgo y Finanzas.

Gerentes de Área. Asegurar la incorporación y aplicación de esta política y las directrices y guías sobre Seguridad de la Información en los procesos bajo su responsabilidad. Proponer cambios a esta política al Oficial de Seguridad de la Información.

Comité de Seguridad de la Información. Instancia presidida por el Oficial de Seguridad de la Información e integrada por miembros permanentes y miembros invitados que sesiona en forma periódica. Es el responsable de proponer cambios a la política de Seguridad de la Información al Directorio de la Compañía y, una vez aprobados, comunicarlos a la organización a través del Oficial de Seguridad de la Información. A su vez, debe establecer los reglamentos, manuales y procedimientos para el cumplimiento de las funciones que le son encomendadas, su ámbito de acción, conformación, funcionamiento, funciones y resoluciones. Sus responsabilidades se definen en el Reglamento del Comité de Seguridad de la Información (CSI).

El CSI deberá informar periódicamente al Comité de Auditoría del Directorio de toda situación de conflicto que haya requerido definición directa del Gerente General. Así como también, aquellas resoluciones que atendiendo a requerimientos del negocio haya tomado el Gerente General y que, informadas al CSI, requieran ser controladas.

Emitir reporte periódico al Comité de Auditoría del Directorio de los acuerdos tomados en las sesiones del CSI, y de las excepciones aprobadas por el Gerente General ante situaciones de conflicto, y el consiguiente seguimiento de aplicación de las mismas.

Especialista de Seguridad de la Información. Responsable de llevar a cabo los procesos y actividades propios del ámbito de Seguridad de la Información, asesorar a las áreas de negocio y apoyar la gestión del Oficial de Seguridad de la Información.

Dueño de Activos de Información. Es el colaborador, usualmente de la alta administración de la Compañía, quien, en función de su rol en la organización, tiene la responsabilidad sobre determinados activos de información. Debe velar por su adecuada protección al determinar qué usuarios pueden tener permisos de acceso a esos activos de información y con qué nivel de privilegios. Es responsable de administrar, autorizar el uso, regular o gestionar el activo de información. Junto con clasificar el activo, el dueño del activo propone el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Custodios de Activos de Información. Son los colaboradores o grupos de colaboradores a los cuales el dueño de la información entrega, total o parcialmente, la tenencia y protección de determinados activos de información que son de su responsabilidad. Habitualmente aunque no exclusivamente, el área de Plataforma Tecnológica asume la custodia de los activos de información de la Compañía que son capturados, generados, almacenados, procesados y transmitidos electrónica o digitalmente a través de la plataforma tecnológica que disponibiliza a la Compañía. Deberá mantener comunicación permanente con el dueño del activo para reportar los resultados de la aplicación de los controles.

Comité de Gestión de Riesgos. Comité responsable de analizar todos los incidentes de riesgo operacional originados por fallas de personas, procesos, sistemas o eventos externos, proponiendo mitigaciones para fortalecer el ambiente de control de los procesos de la Compañía. En materias de Seguridad de la Información, responsable de tomar conocimiento de las gestiones realizadas y reportadas por el área de Seguridad junto con definir acciones a realizar dentro de este mismo ámbito. Al Comité de Gestión de Riesgos le corresponde, además, contribuir a la coordinación y coherencia de las decisiones y gestiones que adopten las diversas áreas o gerencias cuyo trabajo incide en la Seguridad de la Información, particularmente las encargadas de operaciones, riesgos y tecnologías de información.

Colaboradores. Es responsabilidad de cada uno de los colaboradores proteger proactivamente los activos de información de la Compañía, conociendo, comprendiendo y cumpliendo las directrices de esta política, como así también los procedimientos y normas sobre la Seguridad de la Información que dicte la Compañía.

Es también una obligación de los colaboradores reportar oportunamente cualquier riesgo no identificado (amenaza o vulnerabilidad) y los eventos sospechosos e incidentes que comprometan o puedan comprometer la Seguridad de la Información de la Compañía, de acuerdo al Procedimiento de Gestión de Incidentes de Riesgo Operacional.

En el caso de terceros que trabajen con la Compañía y tengan acceso a activos de información de ésta, es responsabilidad de los colaboradores de la Compañía poner en conocimiento de los terceros nuestras prácticas y normas de seguridad de la información y asegurarse de que éstas sean cumplidas por ellos y que existan los resguardos contractuales correspondientes, de acuerdo al Reglamento de Seguridad para Proveedores.

Todo colaborador es responsable de conocer, cumplir y hacer cumplir esta política.

VIII. Directrices y Lineamientos

La presente política debe ser revisada al menos con una periodicidad anual y aprobada por el Directorio de la Compañía. Sin embargo podrá ser modificada con anterioridad si existen cambios estratégicos, legales, regulatorios que lo ameriten o si el CSI lo estima necesario.

i. Marco Normativo de Gestión de Seguridad de la Información

Se define este Marco Normativo como la estructura documental utilizada para establecer y registrar las definiciones, directrices, acuerdos y compromisos en torno al ámbito de la Seguridad de la Información, de acuerdo con la siguiente estructura jerárquica:

1° Política
2° Reglamentos
3° Manuales de Procedimientos
4° Procedimientos, Estándares, y otros documentos

El Marco Normativo vigente está compuesto por los siguientes documentos:

a) Política de Seguridad de la Información
b) Reglamento del Comité de Seguridad de la Información
c) Reglamento de Gestión de Activos de Información
d) Reglamento de Gestión de Riesgos de Seguridad de la Información
e) Reglamento de Seguridad de la Información para Proveedores
f) Procedimiento de Clasificación de Activos de Información
g) Lineamientos para el Manejo de Información
h) Procedimiento de Gestión de Incumplimientos de Seguridad de la Información

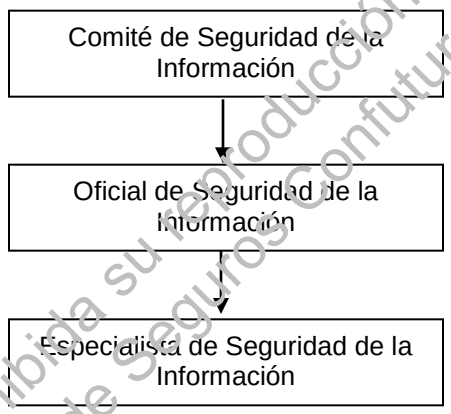
A su vez este marco normativo se complementa con otras normativas internas de la Compañía:

a) Reglamento Interno de Orden, Higiene y Seguridad

b) Código de Conducta
c) Manual de Cumplimiento
d) Política de Gestión de Riesgos
e) Manual de Gestión de Riesgos Operacionales
f) Otros procedimientos que emanan de los documentos ya mencionados

ii. Organización para la Gestión de la Seguridad de la Información

Para una adecuada Gestión de la Seguridad de la Información, la Compañía cuenta con una organización dedicada, la que se estructura de la siguiente manera:



En forma complementaria, el Oficial de Seguridad de la Información debe reportar en forma periódica al Comité de Gestión de Riesgos, con la intención de informar avances, gestiones, riesgos u otras situaciones que requieran la toma de conocimiento, toma de decisiones o bien la retroalimentación por parte de los Gerentes de la Compañía.

Asimismo, el Oficial de Seguridad de la Información reportará regularmente al Comité de Auditoría, y con la frecuencia que éste determine, acerca del desempeño de sus tareas, el cumplimiento de su plan de trabajo y los desafíos o tareas pendientes en el área.

Los reportes mencionados deberán contribuir a la creciente integración de la función de Seguridad de la Información en la gestión del riesgo corporativo a nivel estratégico de la Compañía.

iii. Seguridad en la Gestión de Proyectos

Los distintos proyectos que lleve a cabo la Compañía con el fin de crear nuevos negocios, servicios, procesos o mejorar los existentes, deben contar con una revisión, análisis de riesgos y aprobación del área de Seguridad de la Información, realizada en conjunto con la Subgerencia de Riesgo Operacional. Del mismo modo, el área de Seguridad de la Información

debe actuar como un asesor para las distintas áreas de negocio en esta materia, entregando recomendaciones y sugerencias con el fin de anticipar y mitigar los riesgos que se presenten.

iv. Seguridad y Capacitación de los Recursos Humanos

La Compañía cuenta con procesos orientados a la capacitación de sus colaboradores, pasando por una inducción de carácter obligatorio para los nuevos ingresos dentro de su primer mes, al igual que una capacitación normativa anual, también de carácter obligatorio, para todos los colaboradores vigentes.

v. Gestión de Activos

Los activos de la Compañía deben ser debidamente inventariados y controlados, sean estos físicos o lógicos (no físicos), de acuerdo a la metodología y procedimientos establecidos por la misma. A su vez éstos deben contar con medidas de protección acordes a su importancia y criticidad.

Los distintos activos de información de la Compañía deben contar con dueños (responsables) definidos, quienes deben clasificar los activos de acuerdo a las definiciones internas de la Compañía, junto con proponer las medidas de protección necesarias para su resguardo.

vi. Control de Acceso

La Compañía entendiendo la importancia estratégica de su información, establece que el acceso a sus activos de información (información de procesos internos, clientes, colaboradores, proveedores y otros entes con que ésta interactúa) debe ser otorgado de acuerdo al principio restrictivo de la "necesidad de saber y conocer". Bajo este principio el acceso se otorga única y exclusivamente a los colaboradores que lo requieran para desempeñar sus funciones (actividades y tareas), encomendadas por la Administración de la Compañía, y específicamente en base a los privilegios de acceso a la información requeridos.

En el caso de información de clientes, adicionalmente, el acceso debe limitarse a las autorizaciones y obligaciones establecidas por la normativa vigente establecida por entes reguladores, y únicamente para los fines explícitos que la Compañía haya sido autorizada por los titulares de dicha información, velando por protegerla y resguardarla adecuadamente.

En consecuencia, la Compañía denegará el acceso a los activos de información que no se ajuste al principio antes mencionado.

vii. Cifrado como Medida de Protección de la Información

La Compañía entiende la necesidad de contar con mecanismos apropiados para proteger su información frente a las distintas amenazas y riesgos a los que está expuesta y en particular define la utilización de mecanismos de cifrado para proteger su información en reposo (almacenada) al igual que su información en tránsito (transferida interna y externamente), sujeto a las características, capacidades y limitaciones de la infraestructura tecnológica que posee.

viii. Seguridad Física y Ambiental

Los distintos edificios, centros o salas de cómputo (Datacenters) y dependencias de la Compañía, o aquellos servicios o recursos contratados externamente, deben contar con medidas de seguridad física operativas para resguardar su integridad y seguridad, de acuerdo a criterios establecidos en la normativa interna de ésta, normas a nivel nacional y normas de carácter laboral vigentes. Bajo este concepto de medidas de seguridad física se entenderán las puertas magnéticas y tarjetas de acceso, sistemas de extinción de incendios, señalética y vías de evacuación, entre otros.

ix. Seguridad en las Comunicaciones y Operaciones

Para el correcto funcionamiento de sus procesos internos la información de la Compañía debe fluir a través de las redes internas y externas de comunicaciones en forma segura, por ello ésta considera de vital importancia contar con mecanismos y controles efectivos en la mitigación de los riesgos propios de la operación diaria, como son (y no limitado exclusivamente a) cláusulas en contratos, acuerdos de confidencialidad y procedimientos operativos para el tratamiento de la información, sumado a otros requerimientos, restricciones y normativas vigentes emanados de entes reguladores.

x. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

La Compañía cuenta con sistemas de información que dan soporte a una serie de procesos internos y planes estratégicos de las distintas unidades de negocio. Ésta entiende la necesidad de contar con sistemas que sean mantenidos, renovados o reemplazados, según se requiera y, del mismo modo, contar con mecanismos de seguridad en los procesos de mantención, adquisición y desarrollo de sistemas, que permitan identificar riesgos oportunamente y mitigarlos. Adicionalmente, la plataforma tecnológica debe contemplar definiciones y requerimientos de seguridad para mantener la estabilidad de la operación, pero por sobre todo niveles de riesgo aceptables de acuerdo a las definiciones de la Compañía.

xi. Relación con los Proveedores Tecnológicos

Deben existir procesos acordados y establecidos para gestionar la relación con proveedores tecnológicos y los servicios prestados a la Compañía, que permitan alcanzar una calidad homogénea, respetando los niveles de seguridad definidos por la ésta, que estén en concordancia con las definiciones establecidas en la Política de Compras y otras normativas internas relacionadas con la contratación y adquisición de productos o servicios.

xii. Gestión de Incidentes de Seguridad de la Información

Los incidentes de seguridad son eventos no esperados, que resultan o pueden resultar en un daño para la organización. Por ello, la Compañía define un proceso para la gestión de incidentes que cuenta con los canales de comunicación que permitan reportar y comunicar eventos de este tipo, al igual que equipos para dar respuesta y gestionarlos correctamente.

Este proceso y las gestiones respectivas estarán alineadas con las definiciones de Gestión de Incidentes de Riesgo Operacional y la Gestión de Riesgo a nivel Corporativo, en general.

xiii. Gestión del Cumplimiento Normativo

La Compañía debe actuar conforme a compromisos efectuados. Entiéndanse estos como acuerdos contractuales celebrados, definiciones internas, normativas nacionales e internacionales, tributarias, laborales, medioambientales y propias de la industria en que se desempeña.

En adición, la Compañía toma las medidas y resguardos necesarios en sus procesos, información y operación para dar cumplimiento especialmente a los requerimientos de entes reguladores externos.

xiv. Relación con Otras Normativas de la Compañía

Lo establecido en esta política prevalecerá respecto de toda otra normativa interna de la Compañía que se refiera a los activos de información y que pudiera ser considerada contraria a aquella. Las demás normativas se deberán interpretar y aplicar de un modo consistente con lo dispuesto en esta política.

A su vez, y en el contexto de la gestión de riesgos, la función de Seguridad de la Información se adhiere a las definiciones y lineamientos establecidos en la Política de Gestión de Riesgos y la Gestión de Riesgo Operacional de la Compañía.

El Oficial de Seguridad de la Información es el responsable, con el apoyo de la Administración de la Compañía, de generar, conseguir aprobación y controlar el cumplimiento de las obligaciones y directrices de esta política, las que deben ser consideradas e incorporadas en otras normativas internas y en los procedimientos que regulan el funcionamiento de los procesos de negocio de la Compañía.

IX. Faltas al Marco Normativo de Seguridad de la Información

Para incentivar el cumplimiento del marco normativo de Seguridad de la Información, éste debe ser informado, comunicado a los colaboradores y contemplado dentro del Reglamento Interno de Orden, Higiene y Seguridad de la Compañía y en los contratos de trabajo.

Por otro lado el incumplimiento de la política, reglamentos y procedimientos, debe ser sancionado considerando las definiciones establecidas en el Reglamento Interno de Orden, Higiene y Seguridad, las normas legales y reglamentos aplicables.

Cualquier situación no contemplada en esta política, será abordada por el Oficial de Seguridad de la Información y validada con el Comité de Seguridad de la Información y Comité de Gestión de Riesgos, según corresponda.

X. Modificaciones y actualizaciones

1) **Noviembre / 2018** – Preparada por el Comité de Seguridad de la Información. Aprobada por el Directorio el mes de diciembre de 2018.

2) **Noviembre / 2019** – El documento es actualizado por el Gerente de Operaciones y Tecnologia, Fue aprobado por el Comité de Seguridad de la Información el 24.10.19. Se presentó al Comité de Auditoria el 03.12.19 y fue ratificada por el Directorio en la sesión realizada el mes de diciembre de 2019.

   Al respecto, el documento presenta las siguientes modificaciones:

   a) En el capítulo II, se modifica la definición de Integridad y Comité de Seguridad de la Información.
   b) Se modifica el detalle de integrantes del CSI y sus responsabilidades.
   c) En el Capítulo III, se actualiza el Propósito.
   d) En el Capítulo V, se actualizan las Directrices, incluyendo los apartados Marco Normativo de Gestión de la Seguridad de la Información y Organización para la Gestión de la Seguridad de la Información.
   e) Además, se elimina el numeral iii. Colaboradores, información que es traslada al Capítulo VI. Roles y Responsabilidades.
   f) En el Capítulo VI, se modifican las responsabilidades del Oficial de Seguridad.

3) **Agosto / 2020** – El documento es actualizado por el Gerente de Operaciones y Tecnología / Oficial de Seguridad de la Información, Fue aprobado por el Comité de Seguridad de la Información. Se presentó al Comité de Auditoria el 03/09/20 y fue ratificada por el Directorio en la sesión realizada el mes de septiembre de 2020.

      a) Se reorganiza el contenido de la Política, en los apartados Propósito, Alcances, Definiciones, Roles y Responsabilidades y Directrices y Lineamientos.
      b) En el apartado Roles y Responsabilidades, se incorpora el rol del Especialista de Seguridad de la Información.
      c) En el apartado Directrices y Lineamientos, se incorpora el título Propiedad de los Activos de Información.
      d) Se homologa estructura del Marco Normativo con el resto de la Compañía.

4) **Octubre / 2021** – El documento es actualizado por el Oficial de Seguridad de la Información, Fue aprobado por el Comité de Seguridad de la Información. Se presentó al Comité de Auditoria el mes de octubre del 2021 y fue ratificada por el Directorio en la sesión realizada el mes de octubre de 2021.

e) Se complementa la introducción y definiciones del documento.
f) Se incorporan los apartados **Principios** y **Referencias**.
g) En el apartado **Roles y Responsabilidades** se complementa el rol del Comité de Gestión de Riesgos.
h) Dentro del ítem **VIII Directrices y Lineamientos**, se incorporan los apartados: **Seguridad de los Recursos Humanos**, **Cifrado como Medida de Protección de la Información**, **Seguridad Física y Ambiental**, **Seguridad en las Comunicaciones y Operaciones**, **Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información**, **Relación con los Proveedores Tecnológicos**, **Gestión de Incidentes de Seguridad de la Información**, **Gestión del Cumplimiento Normativo**.
i) Dentro del ítem **VIII Directrices y Lineamientos**, los apartados **Propiedad de los Activos de Información**; **Clasificación de los Activos de Información**; **Acceso, Registro y Uso de Información** y **Asignación de Privilegios Sobre la Información** se reemplazan y sus definiciones se incorporan dentro de los nuevos apartados **Gestión de Activos** y **Control de Acceso**.
j) Se complementa el apartado **Relación con Otras Normativas de la Compañía**, en relación a la gestión de riesgos y la relación con Riesgo Operacional.
k) Se modifica dependencia del subproceso de Seguridad de la Información, acorde con el cambio de dependencia de dicha función en la Compañía.