TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las amenazas que vulneran la seguridad de la información y ciberseguridad pueden afectar considerablemente la reputación de Concesionara Panamericana S.A.S. (en adelante Panamericana o La Compañía), así como sus activos de información más importantes. Conscientes de las consecuencias, y como respuesta a su compromiso en la preservación de los pilares de Seguridad de la información y Ciberseguridad se incluyen los aspectos que deben tenerse en cuenta por parte de todos los trabajadores para que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (Confidencialidad); que esté protegida contra modificaciones no autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad), que sea utilizada para los propósitos que fue obtenida (Privacidad) y que se deje el rastro de los eventos que ocurren al tener acceso a la información (Auditabilidad).

Por lo tanto, los trabajadores de Panamericana deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las instrucciones, procedimientos y formatos; en el entendido que la Alta Gerencia tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de Seguridad de la Información y Ciberseguridad, de acuerdo con las responsabilidades asignadas dentro de La Compañía en relación con este tema.

2. OBJETIVOS

2.1. Objetivo General

Establecer las directrices y los lineamientos relacionados con el manejo seguro de los activos de información, enmarcado en el estándar internacional de seguridad (v gr. ISO 27001) y en normas de entes reguladores (SIC - Ley 1581 de 2012 y sus decretos reglamentarios o posteriores que las deroguen o modifiquen), con la finalidad de proteger a Panamericana frente a situaciones que representen riesgo para la Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de La Compañía y/o los prestados a través de terceros.

2.2. Objetivo Específicos

- Establecer los lineamientos para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en Panamericana, con el fin de ser protegida de forma homogénea con base en la valoración de los activos de información.
- Establecer los fundamentos para el desarrollo y la implantación del Modelo de Seguridad de la Información y ciberseguridad en La Compañía.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información que se encuentran en los aplicativos locales como en los implementados en el ciberespacio.
- Garantizar la gestión de riesgos de seguridad de la información y ciberseguridad en Panamericana, asimismo, establecer e implementar los controles que preserven la

confidencialidad, integridad, disponibilidad y privacidad de los activos de información en La Compañía.

- Fijar roles y responsabilidades en materia de los pilares de seguridad de la información y ciberseguridad de Panamericana
- Garantizar la aplicación de los requisitos de seguridad de la información y ciberseguridad en la continuidad del negocio y la recuperación ante desastres en Panamericana.
- Definir el marco general para gestionar el Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a los requerimientos del negocio y que esté acorde a los lineamientos establecidos en esta política corporativa.

3. ALCANCE

Esta Política de Seguridad de la Información y Ciberseguridad aplica para todos los niveles de La Compañía, a la Alta Gerencia, la Administración, accionistas, todos los trabajadores de Panamericana y terceros (que incluye proveedores y contratistas) y entes de control que en ejercicio de sus funciones acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación.

Adicionalmente, la presente Política aplica a toda la información creada, procesada o utilizada en el soporte al negocio, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. DECLARACIÓN DE COMPROMISO

Panamericana está comprometida con la Política de Seguridad de la Información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el Sistema de Gestión de Seguridad de la Información y Ciberseguridad Por lo anterior deben:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.
- Promover continuamente una cultura de seguridad de la información y ciberseguridad.
- Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y ciberseguridad asociados a La Compañía y su relacionamiento con terceros.

La Alta Dirección, así como cada trabajador, proveedor o contratistas, es responsable por aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los valores corporativos y lineamientos establecidos en seguridad de la información y ciberseguridad, de igual forma, es responsable de reportar los incidentes de los que pudiera llegar a tener conocimiento.

5. DEFINICIONES

- **Activo de información:** conocimiento o datos que tienen valor para La Compañía o el individuo.
- **Administración:** Gerente General, Directores y Coordinadores de área o quienes hagan sus veces.

- **Alta Gerencia:** Gerente General y Representantes Legales o quienes hagan sus veces. Son las personas responsables de dirigir, ejecutar y supervisar las operaciones de Panamericana bajo la dirección de la Junta Directiva.

- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daños a un sistema o a La Compañía[1].

- **Apetito riesgo:** Es la exposición al nivel de riesgo que una entidad está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios. Es una ponderación de alto nivel de cuanto riesgo la administración y la junta directiva están dispuestos aceptar en el logro de sus metas.

- **Ciberamenaza o amenaza cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar o que pudiera convertirse en un ciberataque.

- **Ciberespacio:** Entorno o ambiente complejo resultante de la interacción de personas, software y servicios en Internet, soportado a través de dispositivos tecnológicos conectados a dicha red, propiedad de múltiples dueños con diferentes requisitos operativos y regulatorios, el cual no existe en ninguna forma física.

  Nota: Para el presente documento, se entenderá ciberespacio como el entorno donde se establezcan los servicios de La Compañía y los prestados a través de terceros.

- **Ciber riesgo o riesgo cibernético:** Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos**.**

- **Ciberseguridad:** Es el conjunto de políticas, conceptos de seguridad, recursos, controles de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para prevenir el acceso, obstaculización, interceptación, daño, violación de datos, uso de software malicioso, hurto de medios y la transferencia no consentida de activos informáticos, con el fin de proteger los activos de Información de Panamericana en el ciberespacio.

- **Código malicioso:** Software que tiene como objeto ingresar a un sistema de cómputo saltándose los controles de seguridad con el fin de ejecutar programas que generalmente hacen captura de información sin que nos demos cuenta.

- **Confiabilidad:** Indica que la información debe ser la apropiada para la administración de la Entidad y el cumplimiento de obligaciones.

- **Confidencialidad:** Es la propiedad con la que se garantiza que la información solo es accedida por el personal autorizado, Asimismo hace referencia a la protección de información cuya divulgación no está autorizada.

- **Control:** Salvaguardas basadas en dispositivos o mecanismos que se requieren para cumplir con los requisitos de las políticas, los procedimientos, las prácticas y las estructuras

organizativas concebidas para mantener los riesgos de seguridad de la información y ciberseguridad por debajo del nivel de riesgo asumido. El control son las medidas que tome La Compañía y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

- **Estándares y buenas prácticas de seguridad de la información:** Conjunto de medidas implementadas para asegurar que la información de La Compañía y aquella que se encuentre en su poder sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (confidencialidad), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (integridad), que esté disponible cuando sea requerida (disponibilidad) y que sólo sea utilizada para los propósitos con que fue obtenida (privacidad y reserva) y única y exclusivamente para fines del negocio.

- **Evaluación de Riesgos:** Proceso de la entidad para identificar y analizar riesgos relevantes para el logro de sus objetivos, formando las bases para determinar cómo se deben administrar los riesgos.

- **Evento de ciberseguridad:** Ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible violación de la política de seguridad de la información y ciberseguridad o falla en las salvaguardas o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Incidentes de seguridad de la información y Ciberseguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de amenazar la seguridad de la información.

- **Incidente de ciberseguridad:** Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

- **Información:** Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de soporte a las actividades de área y la toma de decisiones.

- **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

- **Internet:** Es la conexión lógica de múltiples redes de comunicaciones, las cuales utilizan como estándar el protocolo TCP/IP para comunicarse y compartir datos entre dichas redes.

- **Log:** Archivo donde se registran las diversas actividades realizadas por los usuarios en el sistema (rastro).

- **Magnitud impacto:** Es la pérdida (monetaria o no monetaria) generada por la materialización de un riesgo, que puede ser medida cualitativa y cuantitativamente.

- **Modelo de Seguridad de la Información y Ciberseguridad:** Se refiere al conjunto de políticas, procedimientos, estándares, normas de seguridad, elementos de seguridad y topologías que garantizan la protección de la información del negocio que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de La Compañía y/o los prestados a través de terceros.

- **Norma:** Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.

- **Pilares de seguridad de la información:** Principios o características de seguridad de la información (Confidencialidad, Integridad, Disponibilidad).

- **Políticas de Seguridad de la Información y ciberseguridad**: Documentos de referencia para el manejo seguro y buen uso de la información de Panamericana que se encuentre alojada en la infraestructura tecnológica y el ciberespacio donde se establezcan los servicios de La Compañía y/o los prestados a través de terceros.

- **Privacidad:** Propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla.

- **Probabilidad de Ocurrencia:** es la posibilidad que un riesgo se materialice. Para determinar esta probabilidad se puede utilizar el análisis cualitativo o cuantitativo.

- **Recursos de información**: dispositivos o elementos que almacenan datos, tales como: registros (formatos), archivos, bases de Ddatos, equipos y el software propietario o licenciado por Panamericana.

- **Responsable de la Información - RES:** es el trabajador para quien la información fue creada con el objetivo de realizar sus funciones en el negocio y tiene la responsabilidad de administrarla, clasificarla, tomar decisiones de control con respecto al uso de su información y evaluar los riesgos que pueden afectarla. También es el primer responsable de implantar la Política de Seguridad de la Información y Ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios que requieran para su uso.

- **Reserva:** hace referencia a que la información sólo pueda ser utilizada para los propósitos con que fue obtenida del titular y única y exclusivamente para fines del negocio. Conlleva la obligación de no utilizar, revelar o distribuir la información adquirida para fines diferentes para los cuales fue obtenida del titular y única y exclusivamente para fines del negocio.

- **Riesgo:** es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño de un activo de información de Panamericana, donde el riesgo suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgos Emergentes:** entiéndase por aquellos riesgos nuevos o no identificados que nunca han sido considerados previamente por la entidad, o riesgos conocidos que están evolucionando de manera inesperada, que puedan afectar no solo a una compañía sino a todo un sector o toda la economía**.**

- **Riesgo Genérico:** son todos aquellos riesgos identificados por la segunda línea de Grupo Aval.

- **Riesgo Inherente (RI):** Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. En otras palabras, Riesgo Inherente es la probabilidad de que una Entidad pueda incurrir una pérdida material como resultado de su exposición a, y de la incertidumbre que surge de, potenciales eventos adversos. El RI es intrínseco a cada actividad significativa y se evalúa sin tener en consideración el tamaño de esta en relación con La Compañía y antes de evaluar la calidad de la administración de los riesgos que ésta realiza. Para identificar y evaluar los RI a los que está expuesta La Compañía es esencial tener un conocimiento profundo tanto de la naturaleza de las actividades que ésta realiza como del entorno en el que opera.

- **Riesgo Residual (RR):** También conocido como riesgo neto, es el resultado de la mitigación de los riesgos inherentes por parte de la gestión operativa y las funciones de supervisión. En otras palabras, es el riesgo que permanece tras haberse ejecutado. los controles y se hayan tomado las medidas preventivas para dar respuesta a los riesgos identificados.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información. También denominada el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para preservar los pilares de la información, que se almacene, reproduzca o procese en los sistemas informáticos de La Compañía.

- **Seguridad Física:** Protección de los equipos de procesamiento de la información de daños físicos, destrucción o hurto; asimismo, se protege al personal de situaciones potencialmente dañinas.

- **Sistema de gestión de seguridad de la información y ciberseguridad:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y ciberseguridad alcanzando dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **Trabajador:** Trabajadores incluyendo la Alta Gerencia y la administración.

- **Usuarios:** Son todos los trabajadores de Panamericana o personas externas contratadas por esta para la prestación del servicio, que tiene acceso a sus sistemas o activos de información a través de un equipo de cómputo.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio. También es la debilidad de una organización que potencialmente permite

que una amenaza afecte a un activo.

6. NORMAS EXTERNAS

- **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.

- **Ley 1273 de 2009:** Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones

- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

7. OTROS MARCOS DE REFERENCIA

Como mejores prácticas del mercado, son utilizados los siguientes marcos de referencia. De igual forma, se aclara que las prácticas no pretenden ser un listado taxativo:

- **Framework de Ciberseguridad NIST:** Marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo deciberseguridad.

- **NTC-ISO-IEC 27001:2013:** Esta norma específica los requisitos para establecer, implementar**,** mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. La presente norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño onaturaleza.

- **ISO/IEC 27000:** es un grupo de estándares internacionales titulados: Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de la Seguridad de la Información - Visión de conjunto y vocabulario. Tiene como fin ayudar a organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).

- **ISO/IEC 27701:** Estándar que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de privacidad de la información.

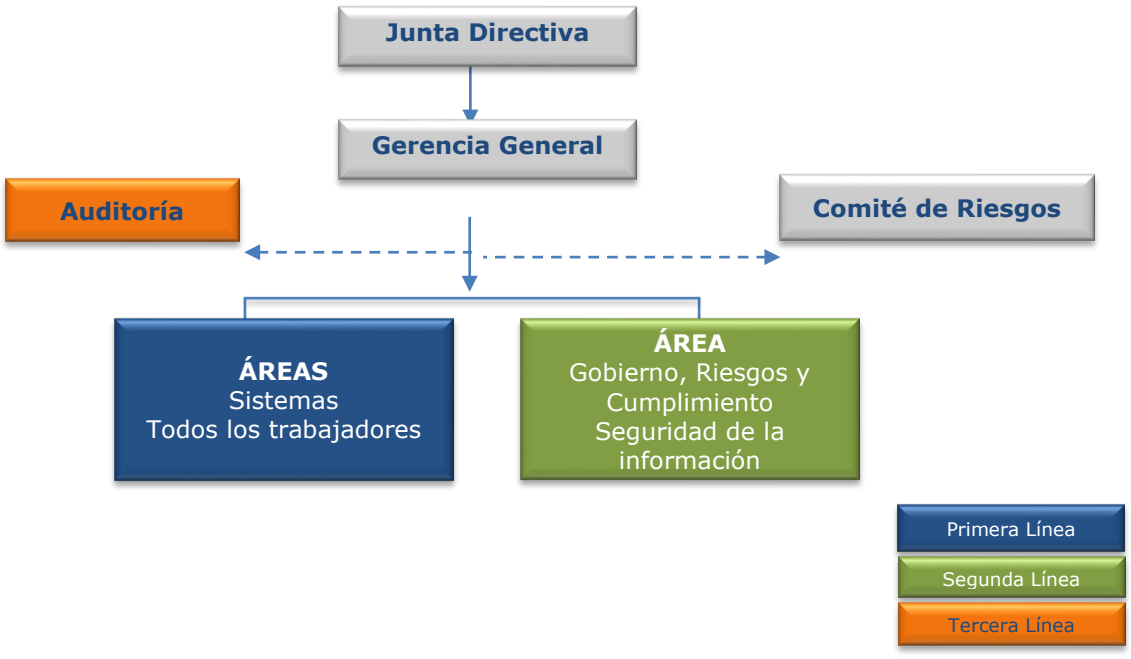
8. PRINCIPIOS

Panamericana ha establecido los siguientes principios que soportan la Política de Seguridad de la Información y Ciberseguridad:

- **a.** La Información es uno de los activos más importantes de La Compañía y por lo tanto debe ser utilizada acorde con los requerimientos del negocio y conservando criterios de calidad (Efectividad, Eficiencia y Confiabilidad).
- **b.** La confidencialidad de la Información del negocio, así como aquella perteneciente a terceros, debe ser mantenida, independientemente del medio o formato donde se encuentre.
- **c.** La Información de La Compañía debe ser preservada en su integridad, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
- **d.** La Información de La Compañía debe estar disponible cuando sea requerida y por quienes tengan autorización de utilizarla; asimismo, presentarse de forma oportuna cuando por requisitos legales y reglamentarios así se requiera.
- **e.** La privacidad y confidencialidad de la información de Panamericana. debe ser preservada.
- **f.** Los eventos que ocurren al tener acceso a la información de Panamericana deben dejar rastro y permitir la reconstrucción, revisión y análisis de la secuencia de estos.

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

Concesionaria Panamericana debe estructurar las funciones y responsabilidades frente al Riesgo de Seguridad de la Información y Ciberseguridad y frente a la gestión de todos los riesgos identificados, de acuerdo con la Política Corporativa para la Gestión Integral de Riesgos; este marco de referencia define el esquema de las tres líneas, considerando (i) la gestión por línea de negocio, (ii) una función de gestión de riesgo de Seguridad de la Información independiente, y (iii) una revisión independiente.



9.1 Primera línea

La primera línea la constituyen principalmente las áreas que gestionan el negocio, tal como aquellas que tienen contacto directo con terceros. La Política de Seguridad de la Información y Ciberseguridad reconoce a todas las áreas como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de seguridad de la información y ciberseguridad inherentes a las actividades, procesos y sistemas de seguridad, según el procedimiento para la Administración y Gestión de Incidentes de Seguridad de la información y Ciberseguridad. Quienes conforman esta línea deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas. Asimismo, debe cumplir con las políticas y procedimientos definidos por La Compañía, contribuyendo a una sólida cultura de seguridad de información y ciberseguridad.

9.2 Segunda línea

Esta línea está conformada por el área GRC, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de riesgo en seguridad de la información y ciberseguridad.

El Líder de Seguridad de la Información es responsable de presentar los resultados de gestión directamente a la Alta Gerencia. Asimismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Seguridad de la Información y Ciberseguridad. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la Información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

9.3 Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y ciberseguridad, así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas a la Alta Gerencia. Las personas encargadas de auditorías que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control.

Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

10. ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos y administración de la Política de Seguridad de la Información y Ciberseguridad, se han definido los siguientes actores clave en la Gestión de Seguridad de la Información:

Actor	Actividades	
	De Ejecución	De Supervisión
Junta Directiva del Grupo Aval	Aprobar la política corporativa de Seguridad de la Información y Ciberseguridad.	Supervisar la seguridad de la información y ciberseguridad, comprendiendo los riesgos y asegurando que estos sean gestionados.
	Estudiar y aprobar el apetito de riesgo de las entidades.	
	Exigir el cumplimiento de las normas y regulaciones gubernamentales de seguridad de la información y ciberseguridad.	
	Participar en programas de concientización y capacitación en temas de Seguridad de la Información y Ciberseguridad.	
Junta Directiva de Panamericana	Aprobar la Política de Seguridad de la Información y Ciberseguridad de Panamericana.	Supervisar la seguridad de la información y ciberseguridad, comprendiendo los riesgos y asegurando que estos sean gestionados.
	Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la seguridad de la información y ciberseguridad.	
	Exigir el cumplimiento de las normas y regulaciones gubernamentales de seguridad de la información y ciberseguridad.	
	Participar en programas de concientización y capacitación en temas de Seguridad de la Información y Ciberseguridad.	
	Fortalecer la cultura de Seguridad de la Información y Ciberseguridad de los trabajadores, proveedores, contratistas y terceras partes que administren activos de información.	
Administración	Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de gestión de seguridad de la información y Ciberseguridad.	Supervisar la seguridad de la información y ciberseguridad, comprendiendo los riesgos y asegurando que estos sean gestionados.
	Evaluar los informes que le presente el Líder de Seguridad de la Información y Ciberseguridad sobre los resultados de la evaluación de efectividad del programa de seguridad de la información y ciberseguridad, propuestas de mejora en materias de Ciberseguridad y resumen de los incidentes que afectaron a la entidad.	

Actor	Actividades	
	De Ejecución	**De Supervisión**
	Promover la aplicación y apropiación de buenas prácticas de seguridad de la información y ciberseguridad.	
	Garantizar la evaluación de seguridad de la información y ciberseguridad de todos sus activos de información sin excepción.	
	Fortalecer la cultura de seguridad de la información de los trabajadores de Panamericana, que administren activos de información, así como evaluar la necesidad de sensibilizar en seguridad de la información a sus proveedores críticos que acceden a los activos de información.	
Comité Corporativo de Seguridad de la Información del Grupo Aval	Proveer principios, directrices y lineamientos Corporativos de Seguridad de la información y Ciberseguridad, tomar las acciones preventivas y correctivas pertinentes para las Entidades del Grupo Aval.	Monitorear el cumplimiento a nivel corporativo de las políticas del Sistema de gestión de seguridad de la información y ciberseguridad en cada entidad.
	Identificar, evaluar e incluir los requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las entidades.	
	Tomar decisiones relacionadas con la Seguridad de la información y Ciberseguridad de las entidades.	
	Socializar actividades y proyectos que sean de interés común y/o impacten a las entidades.	
	Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI realizados y contribuir a la mejora continua de la postura de Seguridad de la Información y Ciberseguridad.	
	Definir principios, directrices y lineamientos Corporativos de Seguridad de la Información y Ciberseguridad.	
	Definir requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las entidades.	
	Socializar actividades y proyectos que sean de interés común y/o impacten a las Empresas del servicio.	

Actor	Actividades	
	De Ejecución	**De Supervisión**
Comité de Riesgos quien actúa como Comité de Seguridad de la Información y Ciberseguridad	De acuerdo con los lineamientos corporativos, adapta, adopta e implementa las directrices para el mejoramiento de la Gestión de Seguridad de la Información y Ciberseguridad.	Conocer el resultado de la Gestión de Seguridad de la Información y ciberseguridad realizada por parte del Líder de Seguridad de la Información y Ciberseguridad. Conocer los Incidentes de Seguridad de la Información y Ciberseguridad presentados y que hayan tenido impacto significativo, reportados por las áreas y los planes de acción llevados a cabo para la mitigación de estos.
	Monitorear la Gestión realizada por medio de los reportes consolidados que se le presentan periódicamente. Como resultado de esta revisión puede proponer la generación o modificación de lineamientos corporativos que pueden afectar a una o a todas las entidades del Conglomerado, según se requiera.	
	Revisar, evaluar, aprobar o rechazar cambios o proyectos que se apliquen en la infraestructura tecnológica de La Compañía.	
	Validar los riesgos, afectaciones, funcionalidades y desarrollo dentro de los ítems de seguridad de la información.	
	Responsable por asegurar la planeación, implantación y mantenimiento de La Política de Seguridad de la información y Ciberseguridad; al igual que, la ejecución de las acciones requeridas para mantener los niveles de seguridad establecidos en la infraestructura tecnológica local y en el ciberespacio.	
	Informar de acuerdo con el modelo de comunicaciones de Grupo Aval, los acuerdos y decisiones corporativos de seguridad de la información y ciberseguridad.	
	Generar retroalimentación de las jornadas de sensibilización y diagnostico al SGSI para contribuir con la mejora continua.	
	Tomar acciones preventivas y correctivas pertinentes de proyectos corporativos comunicados por casa matriz, CFC o Grupo AVAL.	
Comité Ejecutivo de Seguridad de la Información (CESI), aplica	Informar los acuerdos y decisiones de seguridad de la información y ciberseguridad.	Monitorear el cumplimiento a nivel interno de las Políticas del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en Grupo Aval.
	Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI	

Actor	Actividades	
	De Ejecución	De Supervisión
para Grupo Aval.	realizados y contribuir a la mejora continua de la postura de seguridad de la información.	
	Informar principios, directrices y lineamientos de seguridad de la información y ciberseguridad, verificar el desarrollo de proyectos de seguridad de la información y ciberseguridad, velar el nivel de seguridad de la información por medio del análisis de los indicadores y tomar las acciones preventivas y correctivas pertinentes para Grupo Aval.	
	Identificar, evaluar e incluir los requerimientos de seguridad de la información y ciberseguridad en las iniciativas corporativas.	
	Socializar actividades y proyectos que sean de interés común.	
	Aprobar los cambios y homologaciones de la arquitectura de seguridad de la información	
	Aprobar los planes de acción para mitigar los riesgos identificados por los RES.	
	Aprobar el cronograma anual de pruebas de penetración con base en la propuesta elaborada por el área de seguridad TI.	
Área GRC (Segunda Línea)	Preparar reportes de Seguridad de la Información y ciberseguridad para el Comité de Riesgos o cualquier otro comité corporativo de seguridad de la información y de ciberseguridad que lo requiera.	Mantener actualizados los lineamientos de Seguridad de la Información y ciberseguridad aprobados por Junta Directiva. Apoyar y sugerir los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.
	Reportar el estado actual del Sistema de Gestión de Seguridad de la Información y ciberseguridad.	
	Definir los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y ciberseguridad.	
	Cumplir con las demás responsabilidades que sean definidas para la Administración.	
Líder Seguridad de la Información y	Presentar el informe de Gestión.	Conocer los Incidentes de Seguridad de la información y Ciberseguridad y las medidas que
	Participar en el Comité de Riesgos.	

Actor	Actividades	
	De Ejecución	De Supervisión
Ciberseguridad corresponde al Coordinador GRC	Adoptar y socializar las mejores prácticas sugeridas en el Comité.	se han implementado para mitigarlos. Monitorear el resultado de evaluación de Riesgos. Definir y monitorear indicadores clave de desempeño sobre la gestión de Seguridad de Información y Ciberseguridad para dar alcance a las actividades de supervisión al Área de sistemas
	Propiciar la actualización del inventario de riesgos de Seguridad de la Información y Ciberseguridad.	
	Actualizar el Inventario de riesgos de seguridad de la información y ciberseguridad.	
	Adoptar los lineamientos establecidos por Grupo Aval y Corficolombiana.	
	Velar por su correcto desarrollo del Modelo de Seguridad de la Información y ciberseguridad.	
	Apoyar a la primera línea en el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción establecidos en la gestión de incidentes de seguridad de la información y ciberseguridad.	
	Capacitar periódicamente a los colaboradores de La Compañía, con el fin de fortalecer la cultura de prevención de riesgos de seguridad de la información y ciberseguridad.	
	Hacer seguimiento a los indicadores de seguridad de la información y ciberseguridad de La Compañía.	
	Hacer seguimiento a los proyectos de implementación de nuevos controles de seguridad de la información y ciberseguridad en La Compañía.	
	Cumplir con las demás responsabilidades que sean definidas por la Alta Gerencia.	
Área de Sistemas	Apoyar al Líder de Seguridad de Información en la preparación del informe de Gestión establecido por Grupo Aval.	Analizar los Incidentes de alto impactos de Seguridad de la Información y Ciberseguridad reportados por las áreas y apoyar los planes de remediación. Velar porque se adopten medidas para responder a los incidentes
	Participar en el Comité de riesgos de La Compañía.	
	Adoptar y socializar las mejores prácticas sugeridas en el Comité.	

Actor	Actividades	
	De Ejecución	**De Supervisión**
	Informar al Líder de Seguridad de Información y Ciberseguridad sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad.	presentados y para prevenir futuros incidentes. Adoptar las mejores prácticas vigentes en el mercado con respecto a respuestas a incidentes. Apoyar en la definición y monitoreo indicadores clave de desempeño sobre la gestión de seguridad de la información y Ciberseguridad.
	Velar por su correcto desarrollo del Modelo de Seguridad de la Información y ciberseguridad.	
	Adoptar los lineamientos establecidos.	
	Apoyar a la segunda línea en el proceso de identificación de riesgos y controles, así como en su evaluación.	
	Implementar y operar los controles de seguridad informática y ciberseguridad.	
Responsables de la información	Identificar, clasificar y proteger la información bajo su responsabilidad, conociendo los riesgos a los que podría estar expuesta y velar porque se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables, considerando costo-beneficio para su proceso y La Compañía.	Vigilar y velar que su equipo de trabajo dé cumplimiento a la política de seguridad y ciberseguridad.
	Conocer los riesgos de Seguridad de Información que le son aplicables.	
	Con el apoyo de la segunda línea, identificar los controles clave para mitigar los riesgos identificados.	
	Llevar a cabo la ejecución de los controles para mitigar los riesgos (Autocontrol).	
	Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información y ciberseguridad a su cargo.	
	Reportar a las áreas de Sistemas y GRC, cualquier incidente de seguridad de información y de manera particular cualquier evento material de ciberseguridad.	
Auditoría	Adelantar las pruebas de auditoría que considere apropiadas de acuerdo con el plan de trabajo anual probado por el Comité de Auditoría en cada Entidad.	Evaluar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.

Actor	Actividades	
	De Ejecución	De Supervisión
Demás trabajadores	Son todos los trabajadores de Panamericana (usuarios de la información) son responsables de poner en práctica los programas y planes liderados por el Comité de Riesgos que garanticen la protección de la información del área.	Deben de estar alerta para identificar y reportar alguna falta a las normas y políticas establecidas en este documento. Realizar el reporte oportuno de incidentes de seguridad de la información y ciberseguridad.

11. POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Alta Gerencia de Panamericana reconoce la importancia de proteger adecuadamente la información de amenazas que vulneren o puedan afectar la continuidad del negocio, por lo anterior, establece el desarrollo de actividades para la protección de los activos de información, gestión y administración de riesgos de seguridad de la información y ciberseguridad, protección de datos personales, cultura de seguridad y las conductas que deben adoptar todos los Trabajadores de Panamericana y proveedores o contratistas que en el ejercicio de sus funciones utilicen información y servicios tecnológicos, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información; por lo anterior, La Compañía debe velar por:

a) El cumplimiento de los requisitos y principios de Seguridad de la Información y Ciberseguridad.
b) Proteger los activos de información y los activos tecnológicos de la organización.
c) Administrar, gestionar y mitigar los riesgos asociados a seguridad de la información y ciberseguridad en los procesos críticos de La Compañía.
d) Establecer y divulgar las directrices, normas, Políticas, Estándares, Procedimientos e Instructivos de Seguridad de la Información y Ciberseguridad, generando compromiso en todas las áreas de la organización.
e) Fortalecer la cultura de seguridad de la información y ciberseguridad de los colaboradores de Grupo Aval y sus Entidades Subordinadas, funcionarios temporales, contratistas y terceras partes, que administren activos de información.
f) Garantizar los requisitos de seguridad de la información y ciberseguridad en el plan de continuidad del negocio frente a incidentes de Seguridad de la Información y Ciberseguridad.

Acorde con lo anterior, Panamericana acoge las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Seguridad de la Información (SGSI). Tales Políticas son expresiones de la gerencia para una presentación y valoración justa y transparente de riesgos de Seguridad de la Información y ciberseguridad. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados:

11.1 Garantizar la protección de la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información

Todos los trabajadores de Panamericana deben garantizar y asegurar, la confidencialidad, Integridad, disponibilidad y privacidad de la información, de tal manera que la información:

- Solo sea accedida por personal autorizado.
- Sea concisa, precisa, incidiéndose en la exactitud.
- Esté disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó.

11.2 Adoptar y mantener una sólida cultura de Seguridad de la Información y Ciberseguridad

Las tres líneas deben tomar la iniciativa en el establecimiento de una sólida cultura de Seguridad de la Información y Ciberseguridad donde:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en seguridad de la información y ciberseguridad, en el cumplimiento de políticas y procedimientos organizacionales definidos.

- La segunda línea debe definir y ejecutar las actividades de concienciación y cultura, que abarquen a todos los trabajadores, sobre las políticas y procedimientos organizacionales de seguridad de la información y ciberseguridad.

- La tercera línea debe monitorear la ejecución y el cumplimiento de cultura y concienciación de seguridad de la información y ciberseguridad.

11.3 Implementar y mantener un sistema de gestión integral de riesgos de Seguridad de la Información y Ciberseguridad

Todos los trabajadores de Panamericana deberán utilizar un marco de control interno generalmente aceptado donde defina los elementos que se espera que estén presentes y funcionando en un sistema de control interno efectivo. Para el efecto, se deberá alinear con la Metodología Corporativa de Administración de Riesgo Operativo – SARO (evaluación riesgo inherente, riesgo residual y mapa de calor) y de Gestión de Riesgos de Seguridad de la información y Ciberseguridad emitidas por Grupo Aval y Corficolombiana.

11.4 Determinar el apetito de riesgo, el nivel de tolerancia y la capacidad de riesgo

La Alta Gerencia y la segunda línea de Panamericana deberán alinearse con la definición y alcance del modelo corporativo para la gestión de riesgos de Seguridad de la Información y Ciberseguridad (apetito de riesgo, nivel de tolerancia y capacidad máxima al riesgo), considerando el efecto de la naturaleza de sus operaciones y líneas de negocio, así como los tipos y niveles de riesgo de Seguridad de la Información y Ciberseguridad que La Compañía está dispuesta a asumir en cada uno de estos niveles. La Junta Directiva de Panamericana debe aprobar el apetito de riesgo, el nivel de tolerancia y la capacidad máxima al riesgo.

11.5 Evaluación de riesgos de Seguridad de la Información y Ciberseguridad

Concesionaria Panamericana debe contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de Seguridad de la Información y Ciberseguridad. Este proceso se hace por lo menos una vez al año o cuando circunstancias especiales ocurran, identificando riesgos y evaluando su probabilidad e impacto, el cual debe estar alineado con las Metodologías Corporativas de Gestión de Riesgos de Seguridad de la información y Ciberseguridad.

11.6 Supervisar la Administración del Sistema de Gestión de Seguridad de la información y Ciberseguridad

La Alta Gerencia y la segunda línea deben establecer, aprobar y revisar periódicamente el "Sistema de Gestión de Seguridad de la Información y ciberseguridad", Así mismo, debe supervisar la Administración para asegurarse que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

11.7 Gestionar el cambio

La Alta Gerencia y la segunda línea deben asegurar que haya un proceso de aprobación que evalúe plenamente los riesgos de seguridad de la información y ciberseguridad en todos los nuevos procesos, actividades y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realicen cambios sobre alguna aplicación que impacte el negocio, se lleva al comité de riesgos donde se evalúan los posibles riesgos que traería la implementación de dicho cambio.

11.8 Realizar Seguimiento y Presentar Informes

La segunda línea debe implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad de la Información y Ciberseguridad y las exposiciones a pérdidas importantes. Adicionalmente, debe realizar un diagnóstico de Seguridad de la Información basados en normas, estándares y marcos de referencia que respalden la gestión de seguridad de la información y ciberseguridad como por ejemplo ISO 27000 y Framework de Ciberseguridad NIST con el fin de calcular el nivel de seguridad y madurez en el que ese encuentra Panamericana, indicadores corporativos, evolución de riesgos y evolución de controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de Ciberseguridad.

11.9 Controlar y mitigar

La primera y segunda Línea deben tener un fuerte "ambiente de control", estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de riesgos.

Con lo anterior, la primera línea debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

- Supervisión de controles de accesos físicos.

- Supervisión de controles de accesos lógicos.
- Supervisión y protección de contraseñas.
- Supervisión protección de los puertos de configuración y acceso remoto.
- Restricción de la instalación de aplicaciones por parte del usuario final.
- Los sistemas operativos deben actualizarse periódicamente para aquellos que así lo permitan y de acuerdo con la criticidad de los riesgos que se deriven de esta actividad
- Asegurar que las aplicaciones de software se actualicen regularmente, cuando aplique.
- Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).

11.10 Asegurar que el sistema de Seguridad de Información y Ciberseguridad opera en situaciones de contingencia

La segunda Línea debe velar porque en los planes de continuidad del negocio se incluyan y se implementen los controles necesarios, garantizando los pilares de la seguridad de la información y ciberseguridad.

11.11 Garantizar el cumplimiento de la Ley vigente aplicable

Es obligación de las tres líneas dar cumplimiento a todas las normas de los reguladores vigentes que le aplique aPanamericana relacionadas con seguridad de la información y ciberseguridad.

12. POLÍTICAS INDIVIDUALES

12.1 Seguridad de la información y ciberseguridad.

La información del negocio es un activo vital de Panamericana, por lo tanto, debe ser protegido.

La información de La Compañía sin importar su presentación, medio o formato en el que sea creada o utilizada para el soporte de las actividades, se califica como activo de información y deberá mantenerse dentro de un nivel de protección adecuado, el cual es ejecutado exclusivamente por personal de Panamericana, y no por personal ajeno a La Compañía.

La Seguridad de la información y ciberseguridad del negocio es el conjunto de medidas de protección que toma Panamericana contra una divulgación, modificación, hurto, destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.

Los Dueños de la información son los responsables de asegurar sus procesos de riesgos de seguridad de la información y ciberseguridad, así mismo que cuenten con la protección apropiada para así preservar la confidencialidad, integridad, disponibilidad, privacidad y auditabilidad de la misma.

Panamericana debe disponer de los medios necesarios para preservar y proteger los activos de información de una manera consistente y confiable.

Cualquier persona que intente de alguna manera sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.

12.2 Propiedad Intelectual

La propiedad de la información se debe mantener.

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de Panamericana. Asimismo, se da cumplimiento a las normas para instalación de software dando cumplimiento a derechos de autor y propiedad intelectual adoptadas por La Compañía.

Todo el material que es desarrollado mientras se trabaja para Panamericana se considera que es de su propiedad intelectual y de uso exclusivo de la misma, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso indebido que afecte negativamente a La Compañía.

12.3 Responsables de la información

Cada activo de información de Panamericana debe tener un responsable que vele por su seguridad con base en los riesgos a los que está expuesta.

La información que Panamericana utilice para el desarrollo de los objetivos de procesos debe tener asignado un responsable, quien la utiliza en sus áreas y debe velar por su correcto uso. Así, él toma las decisiones que son requeridas para la protección y determina quiénes son los usuarios y sus privilegios de uso. Actuarán como responsables de la información, los Gerentes, directores, coordinadores y demás titulares de las áreas que reporten directamente del Gerente General o a quienes éste delegue.

12.4 Cumplimiento de regulaciones

Panamericana debe cumplir con las regulaciones locales e internacionales de privacidad y seguridad de la información y ciberseguridad.

La Política de Seguridad de la Información y Ciberseguridad de Panamericana está acorde y apoya el cumplimiento de las leyes y regulaciones locales e internacionales relativas a la privacidad, la seguridad de la información y ciberseguridad. Por lo tanto, tales requerimientos deben ser incluidos en el desarrollo del Modelo de Seguridad de la Información y Ciberseguridad y se deben establecer acciones específicas para mantener alineada permanentemente a Panamericana con tales disposiciones.

12.5 Administración del riesgo en seguridad de la información y ciberseguridad.

Los riesgos a que está expuesta la información de Panamericana deben ser identificados, evaluados y mitigados acorde con su valor, probabilidad de ocurrencia e impacto en el negocio.

La información de La Compañía se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través del Comité de riesgos, se debe realizar periódicamente un

análisis del estado del negocio frente a la seguridad de la información y Ciberseguridad, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable.

Establecidos el nivel de riesgo y el valor de la información, cada responsable debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por Panamericana.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información y ciberseguridad de Panamericana y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información y la ciberseguridad.

12.6 Capacitación al personal y creación de cultura en seguridad de la información y ciberseguridad.

Panamericana debe establecer un programa permanente de creación de cultura en seguridad de la información y ciberseguridad para los usuarios y terceros.

Todos los trabajadores de La Compañía recibirán charlas o capacitaciones en Seguridad de la Información, con el objetivo de crear cultura en el uso de las prácticas adecuadas así como que los usuarios de la información y terceros estén informados acerca de sus responsabilidades en Seguridad de la Información y Ciberseguridad y de las continuas amenazas que ponen en riesgo la información que maneja; a su vez Panamericana estará en la obligación de informar cualquier modificación o cambio de este documento a los trabajadores, proveedores o terceros que accedan a la información. Como parte de su programa de capacitación, el nuevo personal debe asistir durante el periodo de inducción a una charla sobre los requerimientos de seguridad de la información y ciberseguridad de Panamericana.

12.7 Seguridad en el personal

Panamericana debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en seguridad de la información y ciberseguridad desde su ingreso hasta su retiro.

Los trabajadores que ingresen a Panamericana deben seguir un proceso de selección y una vez vinculados deberán recibir capacitación sobre esta política, para su conocimiento y certificación.

Los contratos de los trabajadores deben incluir cláusulas que indiquen las responsabilidades correspondientes para con la seguridad de la Información y Ciberseguridad y el cumplimiento del Código de Ética Conducta, haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.

Se debe mantener un registro por empleado de su conocimiento y entendimiento de la Política de Seguridad de la Información y Ciberseguridad, mediante la certificación de este documento y las demás normas y procedimientos que se expidan al respecto.

Panamericana incentivará a través de las capacitaciones y campañas el reporte de vulnerabilidades y riesgos que detecten los trabajadores.

12.8 Terceros que acceden información de Panamericana local o remotamente en los aplicativos locales o en el ciberespacio.

Los terceros que utilizan local o remotamente información de Panamericana deben cumplir con la Política de Seguridad de la Información y Ciberseguridad.

Todo acceso a la información de Panamericana por parte de un tercero local ó remotamente deberá contar con la previa autorización de la Gerencia, Dirección o Coordinación encargada, o quien estos deleguen comunicando al área de Sistemas para su registro y conocimiento. En los contratos que así lo requieran deben existir acuerdos y/o cláusulas que hagan obligatorio el cumplimiento del presente documento realizando énfasis en la obligación de proteger la información y cumplir las directrices, controles y políticas para mantener siempre los principios de confidencialidad, integridad, disponibilidad y privacidad y las consecuencias a que estarían sujetos en caso de incumplirla. Asimismo, los terceros que en la prestación de sus servicios involucren acceso, custodia, almacenamiento, gestión, administración, procesamiento, e intercambio de información que puedan afectar la confidencialidad, integridad y disponibilidad de la información, deberán incluir la cláusula de ciberseguridad en sus contratos, otrosíes u otro documento utilizado para formalización de la relación.

12.9 Identificación y autenticación individual

Todos los usuarios que acceden la información de Panamericana deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal.

Cada trabajador es responsable por sus acciones mientras usa cualquier recurso o activos de información de Panamericana ya sea local o en el ciberespacio, por lo tanto, deberá tener acceso a la información de forma individual mediante un usuario y clave de autenticación, la cual no será develada ni podrá ser compartida, siguiendo lo establecido en los procedimientos publicados para tal fin.

Una vez creados usuarios y asignadas las autorizaciones en cualquier Sistema de Información, se podrá acceder a la información mediante su usuario y clave de autenticación. Dependiendo de la clasificación, valor del activo de información y del nivel de riesgo, La Compañía definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información sensible/restringida que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

12.10 Control y administración del acceso a la información

El uso de los recursos y activos de información de Panamericana debe ser controlado para prevenir accesos no autorizados. los privilegios sobre la información deben ser mantenidos en concordancia con las necesidades del negocio, limitando el acceso solamente a lo que es requerido.

Los accesos a la información de Panamericana por parte de los usuarios deben ser definidos y autorizados por el Dueño (responsable) de la Información (Gerentes/Directores/Lideres/Coordinadores) del área a la que pertenece el activo de información, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad sin comprometer la segregación de tareas y responsabilidades.

El acceso a carpetas compartidas solo se permite a los trabajadores autorizadas con los permisos de lectura o escritura según sea el caso, cuando la conexión se realiza a través de VPN, estos permisos se conservan.

12.11 Clasificación de la información

Los responsables de la información deben clasificar la información basados en su valor, riesgo de pérdida o compromiso, y/o requerimientos legales de retención.

No toda la información tiene el mismo uso o valor, y por consiguiente requiere diferentes niveles de protección. Todos los activos de información de Panamericana serán clasificados por el responsable de la Información con base en un análisis de alto nivel del impacto al negocio en seguridad de la información y ciberseguridad, que determine su valor relativo y nivel de riesgo a que está expuesta.

Para la clasificación de la información Panamericana, cuenta con una clasificación de activos de información definida en la Matriz de Identificación y Clasificación de Activos de Información (ICAI) donde se establecen las siguientes categorías: Sensible/Restringida, Uso Interno y Pública. Esta clasificación es exclusiva del dueño de proceso y será el responsable de comunicarla a Gestión Documental y el área de GRC. Por lo tanto, no se debe asumir que otros protegen la información, ya que es deber de trabajadores de Panamericana, tomar las medidas necesarias para proteger la información.

Según los riesgos que se detecten, el responsable de la información y el Líder de Seguridad de la Información, determinarán los controles que sean necesarios para proveer un nivel de protección apropiado y consistente en toda La Compañía sin importar el medio, formato o lugar donde se encuentre la información. Estos controles deben ser aplicados y mantenidos durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción.

De igual forma, los activos de información clasificados en sensible/Restringida que se manejen a través de archivos de Excel y que el dueño de proceso solicite control de edición o modificación deberán contar con protección a través de claves que minimicen los riesgos de accesos no autorizados, cambios involuntarios de formulación errónea.

12.12 Continuidad del negocio y recuperación de información

Todos los recursos de información y los procesos asociados deben contar con un plan de continuidad del negocio y estar preparados para ataques de seguridad de la información y ciberseguridad, manteniéndolo en situaciones de contingencia.

Concesionaria Panamericana cuenta con un Plan de Continuidad del Negocio que involucra cada una de las áreas y sus actividades a realizar en caso de presentarse alguna falla en los sistemas de información de La Compañía o que por algún evento externo no permita la correcta operación del negocio.

Adicionalmente, Panamericana cuenta con un procedimiento de restauración de la información en caso de presentarse falla o ausencia de alguno de sus sistemas.

Panamericana establecerá medidas de reacción inmediata que permitan detectar y mitigar los efectos de ataques en seguridad de la información y ciberseguridad como son los de negación de servicios y el ingreso de código no autorizado. Estas medidas estarán fundamentadas en procedimientos y elementos que permitan mantener informada a La Compañía de la existencia de estas amenazas, detectar los ataques de manera inmediata y ejecutar las acciones consiguientes.

12.13 Seguridad física

Todas las áreas físicas del negocio deben tener un nivel de seguridad acorde con el valor de la información que se procesa y administra en ellas.

La información sensible/restringida de La Compañía debe mantenerse en lugares con acceso restringido cuando no es utilizada. Todos los trabajadores deben cumplir las directrices de protección física de la información sensible/restringida que usen.

Las áreas físicas designadas para soportar toda la infraestructura deberán estar provistas de controles adecuados (puertas, cerraduras, lectores de tarjetas, lector biométrico, entre otros) según el valor de la información que contienen.

Los recursos informáticos de Panamericana deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de La Compañía.

Por tal motivo, el acceso a los sitios restringidos centros de cómputo, archivo y oficinas de peajes por parte de terceros está totalmente prohibido, para ello se deberá contar con el acompañamiento de personal autorizado de Panamericana o del dueño del proveedor o tercero.

La información clasificada como Sensible / Restringida no se dejará desatendida o sin control, por lo que, Panamericana desarrollará un programa que permita prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.

Lo anterior, en cumplimiento del Procedimiento para la Gestión de Seguridad Física.

12.14 No repudio

La autenticidad de un negocio o transacción electrónica que realice Panamericana debe ser asegurada ya sea localmente o en el ciberespacio.

Panamericana se apoya en los medios electrónicos para realizar transacciones. Por lo tanto, para cualquier negocio o transacción que se haga por estos medios, La Compañía debe asegurar la autenticidad de cada parte que interviene y evitar que alguna de ellas niegue su participación (no repudio). Asimismo, cada ingreso a un portal bancario u aplicación de La Compañía deberá ser exclusivamente por los usuarios autorizados y cada uno de ellos deberá contar con un perfil de acceso, el cual estará identificado en la matriz de usuarios y perfiles. El acceso a los portales bancarios se deberá hacer mediante un token, el cual deberá estar en custodia de cada usuario.

12.15 Administración de alertas

Panamericana debe ser alertada en el mismo instante en que existan violaciones a la Política de Seguridad de la Información y Ciberseguridad.

Las situaciones o acciones que incumplan la presente política deben ser detectadas, registradas e informadas al Líder de Seguridad de la Información y Ciberseguridad o al Comité de Riesgos de manera inmediata (alertas) de conformidad con el Procedimiento para la Administración y Gestión de Incidentes de Seguridad de la Información y Ciberseguridad. Estas alertas quedarán registradas con el fin de mitigarlas, llevarlas a comité y tomar acciones sobre ellas. Se debe mantener un registro de eventos e incidentes que dé prioridad a dichas alertas y las resuelva conforme a la criticidad de la información para La Compañía de conformidad con el procedimiento para la administración y gestión de incidentes de seguridad de la información y ciberseguridad.

12.16 Auditabilidad de los eventos de seguridad de la información y ciberseguridad

Los registros de seguridad de la información y ciberseguridad de Panamericana deben ser revisados permanentemente para asegurar el cumplimiento del modelo de seguridad de la información y ciberseguridad.

Las aplicaciones Core del negocio o de misión crítica poseen registros de seguridad que permiten auditarlos en caso de ser necesario.

La fecha y hora de todos los relojes de donde se encuentren recursos de información deben estar sincronizadas con el fin de tener una fecha y hora precisa de un evento.

El Director de Sistemas y el Líder de Seguridad de la Información deben definir los eventos considerados como críticos y los respectivos registros de seguridad de la información y ciberseguridad que deben ser generados, los cuales deben ser activados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera oportuna al Comité de Riesgos. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las pruebas cuando se requieran.

12.17 Conectividad

Todas las conexiones a redes públicas deben ser autenticadas para prevenir que la información sea develada o alterada.

Las conexiones a la red privada de Panamericana deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida al ciberespacio y a otras empresas deben realizarse sobre redes aprobadas por Panamericana, para ello se cuenta con un firewall que permite la segmentación de redes y separación del tráfico de los servidores.

Cualquier usuario que se conecte a la red privada debe cumplir con la presente política. Esto aplica igualmente a cualquier conexión actual o futura en la red de Panamericana que utilice redes públicas, de requerirse una conexión segura VPN, esta deberá ser aprobada por el dueño de proceso justificando el porqué de su uso.

Todas las conexiones hacia las aplicaciones de La Compañía se realizan mediante el uso de la red LAN corporativa. En caso de que el acceso a la aplicación se realice desde una red externa de La Compañía, se empleará el servicio de internet con el uso de VPN, para acceder a la misma.

El servicio de VPN se realiza mediante el firewall check point estableciendo un túnel seguro IPSEC entre la estación de trabajo y las aplicaciones de La Compañía.

Las reglas de conexión VPN en el firewall solo permite las aplicaciones y servicios necesarios para acceder a los mismos.

12.18 Uso de los recursos informáticos de La Compañía local y en el ciberespacio de dispositivos móviles

Los recursos informáticos provistos a los usuarios localmente y en el ciberespacio son para uso exclusivo del negocio

Los recursos informáticos y de comunicaciones de Panamericana tanto locales como en el ciberespacio son exclusivamente para propósitos de La Compañía y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. está prohibido el uso de estos recursos en actividades distintas a las del proceso. Los trabajadores que intenten acceder a información para la que no tienen un requerimiento autorizado, están violando la presente Política.

Panamericana se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Director de Sistemas.

Para acceder a la información de Panamericana tanto local como en el ciberespacio a través de medios tales como los dispositivos o trabajo móviles, se deben implementar los controles necesarios para reducir los riesgos introducidos por estas prácticas.

12.19 Seguridad de información y ciberseguridad en los procesos de administración de sistemas

Cada proceso de administración de sistemas de Panamericana debe cumplir con la presente Política de Seguridad de la Información y Ciberseguridad.

Actividades, normas y responsabilidades en seguridad de la información y ciberseguridad se incluyen en cada uno los procesos de administración de sistemas, de esta manera se logra el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.

La Dirección de Sistemas debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura que se contrate a través de terceros. Los requerimientos de seguridad de la información y ciberseguridad deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información y ciberseguridad. Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información y ciberseguridad que han sido previamente establecidos. El nivel de Seguridad de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.

La implantación de un sistema nuevo o cambio significativo a los existentes debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.

La realización de un cambio tecnológico a nivel local o en el ciberespacio que no considere los requerimientos de seguridad de la Información y ciberseguridad hace que Panamericana este expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y ciberseguridad y sus respectivas normas, y en caso de exponer a La Compañía a un riesgo en seguridad de la información y/o ciberseguridad, éste debe ser identificado, evaluado, documentado, asumido y controlado por el Director de Sistemas y el Líder de Seguridad de la Información.

12.20 Regulación

Panamericana debe cumplir con las regulaciones de Seguridad de la Información y Ciberseguridad vigentes en el país que se le obliguen a adoptar. Como ejemplo se encuentran:

- **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.

- **Ley 1273 de 2009:** Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

13. NORMAS EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

A continuación, se relacionan cada una de las normas que soportan los principios de Seguridad de la Información y Ciberseguridad enunciados en el numeral anterior de Políticas Individuales:

13.1 Seguridad de la información y Ciberseguridad

La información de Panamericana debe tener un nivel de protección definido de acuerdo con su clasificación y ésta debe mantenerse dentro del nivel de protección sin importar el medio o formato en que ésta se encuentre.

La administración de Seguridad de la Información es exclusiva de Panamericana y no debe ser ejecutada por personal externo a ella.

13.2 Propiedad intelectual

Los descubrimientos, invenciones o las mejoras en los procedimientos, lo mismo que todos los trabajos y consiguientes como resultados de la actividad de los trabajadores de La Compañía o cuando por la naturaleza de sus funciones haya tenido acceso a secretos o investigaciones confidenciales, quedarán de propiedad exclusiva de Panamericana, además, tendrá esta última derecho a hacer patentar a su nombre o a nombre de terceros esos inventos o mejoras, para lo cual, el trabajador accederá a facilitar el conocimiento oportuno, dar su firma o extender los poderes y documentos necesarios para tal fin, según y cuando se lo solicite La Compañía sin que ésta quede obligada al pago de compensación alguna.

13.3 Responsables de información

Se establece a los gerentes, directores, coordinadores y demás titulares de las dependencias que reporten directamente del Gerente General o a quienes éste delegue como responsables de la información que se maneje en cada uno de sus procesos. La propiedad de la información debe ser divulgada a los usuarios.

13.4 Cumplimiento de regulaciones

Panamericana cumple reglamentaciones de derecho de autor, está prohibida la instalación de aplicaciones o software en los recursos tecnológicos de La Compañía sin previa autorización del Director de Sistemas.

Panamericana cuenta con un lugar seguro y específico para almacenar y enviar a custodia las cintas de los backups de los servidores, en este sitio se maneja los originales de las licencias, manuales de los recursos informáticos adquiridos.

13.5 Administración del riesgo de seguridad de la información y ciberseguridad

Panamericana realizará semestralmente la matriz de riesgos de seguridad de la información y ciberseguridad que permita identificar los recursos de información de mayor criticidad y orientar los esfuerzos para proteger dichos recursos.

Los recursos de hardware que almacenen información son asegurados y las cintas de backups son custodiadas.

13.6 Capacitación y entrenamiento al personal sobre seguridad de la información y ciberseguridad

Dentro del proceso de inducción de un trabajador nuevo y al menos anualmente para la totalidad de los trabajadores debe realizarse una capacitación y/o actualización sobre Seguridad de la Información y Ciberseguridad. La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial a los trabajadores, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad de Sistema de Gestión de Seguridad de la Información y Ciberseguridad. La compañía deberá evaluar la necesidad de sensibilizar en seguridad de la información los proveedores críticos que acceden a los activos de información.

Adicionalmente, esta política será publicada en la Intranet de Panamericana para su consulta, dado que es el único sitio donde se encuentran los documentos actualizados y en las últimas versiones.

Cada modificación o cambio en las políticas y normas de Seguridad de la Información y Ciberseguridad serán divulgados a todos los trabajadores.

13.7 Seguridad en el personal

Es obligación de todos los niveles jerárquicos, sin excepción alguna, conocer, respetar, cumplir y hacer cumplir el Modelo de Seguridad de la Información de Panamericana

Todos los trabajadores, sin importar el tipo de contrato de trabajo, ya sea a término fijo o indefinido, deben acatar lo concerniente al manejo confidencial de la información de Panamericana. Lo anterior, según lo establecido tanto en el contrato laboral y en el Código de Ética y Conducta, lo cual será de obligatorio cumplimiento y el no aplicarlo tendrá implicaciones disciplinarias. Dependiendo de la gravedad, Panamericana emprenderá las acciones legales que estime convenientes.

Debe existir una descripción de las actividades para cada rol dentro de la Organización de seguridad de la información y ciberseguridad de Panamericana y ésta debe ser comunicada a los trabajadores que las desarrollen.

La Dirección de Sistemas y el personal del comité de Riesgos de la Información deben estar actualizados en avances tecnológicos que mitiguen el riesgo en el que se pueda ver afectada La Compañía.

13.8 Terceros que acceden a la información local o remotamente

Se deben establecer Acuerdos de Niveles de Servicios con respecto a la seguridad de la información que rijan los compromisos de compartir información entre Panamericana y entes externos, deben ser canalizados a través de un punto focal en cada contraparte.

El acceso por parte de un tercero a la información de Panamericana debe cumplir con los siguientes ítems:

- El ingreso a una aplicación debe ser por parte del trabajador de La Compañía, nunca se deben dar las claves ni los usuarios de acceso a los terceros.

- Deben existir cláusulas de confidencialidad en los contratos para el manejo e intercambio de la información entre terceros y La Compañía.

13.9 Identificación y autenticación individual

- Cada trabajador es responsable por sus acciones mientras usa cualquier recurso de información de Panamericana, por lo tanto, deberá tener acceso a la información de forma individual mediante un usuario y clave de autenticación.
- El director de Sistemas entregará de forma personal esta información a cada uno de los trabajadores que requieran acceso a las aplicaciones para la correcta ejecución de sus funciones. Esta clave es personal e intransferible y aplica para cada uno de los trabajadores de La Compañía.
- Toda solicitud de creación, modificación y eliminación de usuario debe ser aprobada por los dueños de proceso de cada área, ningún usuario diferente está facultado para hacer estos requerimientos.
- Si el trabajador se ausenta de su estación de trabajo y requiere dejarlo encendido, debe bloquear la sesión, para ello es necesario ejecutar la combinación de teclas (Windows + L).
- Si la aplicación lo permite se deberá hacer cambio de contraseña una vez el usuario inicie sesión por primera vez, este cambio esta soportado sobre las siguientes aplicaciones: SIC y acceso a la red.
- Las contraseñas deben cumplir con 3 de los cuatro siguientes requisitos de complejidad: longitud mínima de 8 caracteres, mayúscula, minúscula, números, caracteres especiales.
- Panamericana, cuenta con 5 intentos fallidos de acceso a la red, si existe un sexto intento fallido la contraseña se bloqueará automáticamente por un lapso de 30 minutos.
- Está prohibida la suplantación, el enmascaramiento o la firma por otros usuarios de correos electrónicos o de acceso a cualquier recurso informático de La Compañía.
- Los trabajadores deben usar siempre su código de usuario para acceder a los recursos de información de Panamericana incluso si deben hacerlo desde una estación diferente a la asignada.

13.10 Control y administración de acceso a la información

Las aplicaciones que así lo permitan manejarán perfiles de acceso a las actividades/transacciones que requiera cada rol o perfil.

Los accesos a la información de Panamericana por parte de los usuarios deben ser definidos y autorizados por el Dueño (responsable) de la Información (Gerentes/Directores/Coordinadores del área a la que pertenece el usuario) y deben estar basados en requerimientos específicos del negocio.

Se deben crear perfiles de acceso asociados a roles que tengan responsabilidades y cumplan con actividades comunes; estos perfiles deben permitir el acceso mínimo y suficiente para el adecuado desempeño de las actividades de los usuarios.

Se debe establecer un programa de administración de usuarios de emergencia para ser utilizado en caso de ausencia de los titulares de los roles. Se deben establecer medidas de protección y respaldo para las claves de usuarios de emergencia con el fin de garantizar la confidencialidad y disponibilidad en caso de requerirse. Los usuarios de emergencia deben estar limitados a usuarios

privilegiados, las claves deben ser cambiadas cada vez que se usen y se debe documentar la situación que requirió el uso de estos usuarios y las acciones que realizaron.

- Ningún usuario debe tener herramientas instaladas en sus equipos que permitan la administración de forma directa de una base de datos o que pueda modificar los parámetros de configuración de un sistema, los únicos trabajadores que están facultados para hacer esta labor son los de la Dirección de Sistemas o a quienes estos deleguen.
- Cuando exista una novedad de usuario se debe deshabilitar el acceso a todas las aplicaciones de este trabajador.
- Los privilegios de usuarios deben ser manejados de forma centralizada en sistemas de información que sean administrados por la Dirección de Sistemas.
- Solo las aplicaciones (cliente –servidor-acceso web) son los únicos medios para el ingreso a los datos de producción, cualquier otro acceso deberá ser justificado.
- Los usuarios administradores del sistema están en custodia de la Dirección de Sistemas, de ser necesario usuarios administradores en los aplicativos serán los que el dueño de proceso disponga para tal fin.
- Cada aplicación debe manejar dos usuarios administradores, uno principal y otro de emergencia, lo anterior con el fin de utilizarlos en los casos que el usuario principal presente problemas.

13.11 Clasificación de la información

Toda la información, independientemente del medio en el que se encuentre, debe estar clasificada en una de las siguientes tres categorías: Sensible/Restringida, Uso Interno y Pública, de acuerdo con el estándar de clasificación de información establecido por Panamericana.

- Cuando la información Sensible/restringida de La Compañía por razones de área deba ser desechada, se debe destruir de manera segura de acuerdo con su criticidad y los controles establecidos, independiente del medio en que ésta se encuentre.
- Cuando un recurso informático va a ser dado a cambio, enviado a servicio o desechado, la información almacenada en él debe ser destruida de acuerdo con los controles establecidos.
- Si un equipo es suministrado a un tercero y a su vez tiene información Sensible/Restringida esta deberá ser eliminada, desechada o destruida.

13.12 Continuidad del negocio y recuperación de información

Toda la información de Panamericana que está alojada en servidores deberá mantener la propiedad de disponibilidad en cualquier momento, para ello se realiza de forma diaria, semanal y mensual backups de esta información.

Las cintas de backups son custodiadas por una empresa externa, si se presenta un evento de recuperación de información es necesario solicitar las cintas a la misma y esperar el tiempo según los procedimientos establecidos por ellos.

La recuperación de la información y la solicitud de cintas está a cargo de la Dirección de Sistemas.

Se deben realizar pruebas periódicas de los medios que contienen copias de respaldo de información crítica que incluyan la restauración y verificación de la información.

Panamericana cuenta con herramienta de detección de virus, ejecución de los mismos, aun así, la información puede ser vulnerada en cualquier momento. Si un usuario sospecha que un recurso informático está bajo los efectos de un código malicioso, debe suspender el uso del mismo inmediatamente y comunicarse directamente con la Dirección de Sistemas.

13.13 Seguridad física

Las áreas físicas de Panamericana deben ser clasificadas considerando entre los principios necesarios la criticidad de la información que resguarden. Adicionalmente, se debe desarrollar un plan de seguridad física por cada área clasificada como crítica. La criticidad de la información que resguardan debe ser uno de los criterios primordiales para clasificar las áreas físicas de Panamericana

En virtud de sus actividades y responsabilidades los únicos que tendrán acceso de forma permanente a estos lugares son: el Coordinador de Peajes, Analista de Gestión Documental, Analista de Peajes, Director de Sistemas y Analista de Sistemas según el área que corresponda.

Panamericana cuenta con:

- Equipos de seguridad ambiental por ejemplo extintores para su uso en cualquier momento que se presente una eventualidad donde se alojan los activos de información.

- Circuitos alternos de suministro de energía UPS para soportar la carga de los equipos que almacenan activos de información del negocio.

- Cronograma de mantenimiento de los recursos que alojan activos de información.

Las llaves físicas o tarjetas que permiten el acceso a sitios restringidos solo deben ser usadas por personal del área que maneja el proceso, adicional se debe tener una copia de respaldo en la Dirección Administrativa con el fin de conceder acceso en caso de pérdida o daño de esta.

Está prohibido el ingreso a terceros a sitios restringidos, para ello se debe contar con el acompañamiento de un trabajador idóneo, y a su vez registrar el acceso en la planilla correspondiente.

Está prohibido el consumo de bebidas y/o alimentos en sitios restringido que alojen activos de información.

13.14 No repudio

Con el fin de garantizar la aceptación en la realización de transacciones efectuadas entre Panamericana, los clientes y entes externos, se deben establecer mecanismos de certificación para las transacciones que así se consideren.

Panamericana tiene el derecho de solicitar log de transacciones a alguna entidad financiera si así lo requiere en caso de presentarse y resolver conflictos cuando alguna de las partes niegue su participación. Estos se deben generar, guardar y ser accedidos acorde con las Políticas y las Normas que regulen estos aspectos en Panamericana.

13.15 Administración de alertas

Se debe establecer información estándar en la generación y registro de alertas que permita documentar en forma completa el evento y provea el nivel de detalle suficiente que facilite su detección, entendimiento, priorización, seguimiento y resolución.

La información específica sobre las vulnerabilidades o condiciones anormales de seguridad de la información tiene carácter de restringida y solo debe darse a conocer a personas autorizadas y que tengan una necesidad demostrada de saberlo.

Panamericana debe establecer y mantener un procedimiento formal de reporte de incidentes de seguridad que le permita a los usuarios, terceros y entidades, informar acerca de éstos cuando se presenten o se tenga sospecha de su ocurrencia.

Todo incidente o alerta de seguridad debe ser tratado de principio a fin mediante un procedimiento de tratamiento de incidentes que garanticen el análisis, investigación, documentación, solución completa y seguimiento a cualquier incidente de seguridad.

13.16 Auditabilidad de los eventos de seguridad de la información y ciberseguridad

Los Recursos de Información deben incluir registros de auditoría que involucren cualquier evento susceptible de verificación posterior e incluyan el código de usuario que lo generó.

Se deben retener los registros que contienen eventos relevantes de Seguridad de la Información y Ciberseguridad por un periodo mínimo de tiempo. Durante este periodo, deben afianzarse los registros en archivos históricos tal que no puedan modificarse y sólo puedan ser leídos por personas autorizadas. Estos registros podrán efectuarse en los formatos destinados para tal fin del Grupo AVAL.

Los usuarios con privilegios administrativos deben ser periódicamente revisados y verificados con el fin de no tener configuraciones no permitidas en La Compañía.

Cada servidor maneja log dependiendo el rol que desempeñe, esto se revisan de forma periódica con el fin de detectar alguna falla o incidente de seguridad.

La fecha y hora de cada servidor es sincronizada mediante protocolos NTP que permiten manejar la misma hora en todos los recursos que alojan información, no se tiene en cuenta la hora de dispositivos móviles.

13.17 Conectividad

Se establece el firewall como único punto de acceso autorizado para redes externas a cualquier recurso informático, este a su vez permitirá el tráfico y flujo de información por los protocolos y puertos necesarios entre las diferentes redes de La Compañía.

Los diagramas de red, así como la información de direccionamiento y configuraciones de la misma, debe estar restringida al personal autorizado o a quien tenga legitima necesidad de conocerla, los cambios a configuraciones deben contar con la aprobación del Director de Sistemas y con el acompañamiento de un trabajador idóneo en el tema.

Todo acceso externo debe ser autenticado, para esta función se utiliza el firewall, permitiendo conexiones seguras mediante clientes VPN. Los trabajadores que requieran de esta conexión deberán ser solicitados y aprobados por los Gerentes.

El acceso a internet debe ser restringido, se aplican políticas en los firewalls que bloquean categorías de navegación para toda La Compañía impidiendo el acceso a sitios no autorizados para el desarrollo de sus actividades.

13.18 Uso de los recursos informáticos de La Compañía

Los Recursos de Información de Panamericana deben ser utilizados únicamente para fines de negocio aprobados. Está prohibido el uso de los Recursos de Información de Panamericana en actividades distintas a las del negocio.

Está prohibido el almacenamiento de archivos multimedia en los servidores o en los equipos de cómputo asignados que no hagan parte del desarrollo propio de sus actividades, estos archivos son: MP3, WMV, AVI, WMA. FLV, JPG, BMP, GIF, FLV, de ser encontrados se procederá a realizar informe al jefe inmediato o con copia al Gerente General.

Solamente los recursos de seguridad designados para este fin deben de estar instalados en los equipos, Symantec EndPoint Protection es el único antivirus aprobado e instalado en las máquinas.

Panamericana se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa solicitud del dueño de proceso y autorización formal el Director de Sistemas.

El usuario se compromete a seguir las recomendaciones del Director de Sistemas en lo referente a la seguridad de la información y ciberseguridad como del buen uso de los equipos asignados.

Para cualquier notificación al usuario final, se usará la dirección de correo electrónico asociada al mismo y de ser necesario con copia a su jefe inmediato.

El usuario final está obligado a comunicar al director de Sistemas o al director Administrativo cualquier cambio en la titularidad del recurso informático que tenga asignado y mientras esta notificación no se produzca continúa siendo el único responsable.

Todo usuario debe ser consciente y cumplir las políticas y las normas de Seguridad de la Información y Ciberseguridad de Panamericana cuando hace uso de los servicios de Internet e Intranet. Los usuarios autorizados explícitamente por Panamericana para acceder a servicios de Internet e Intranet son absolutamente responsables de la utilización que hagan de dichos servicios y por las consecuencias que se deriven de su utilización.

El ancho de banda de la red y la capacidad de almacenamiento tienen límites; por lo tanto, los usuarios no deben realizar deliberadamente actos que desperdicien los Recursos de Información ni monopolicen los recursos injustamente en detrimento de los demás usuarios. Estos actos incluyen, entre otros: enviar correos masivos o cartas de cadena, pasar períodos prolongados en Internet desarrollando actividades personales, jugar, participar en charlas en línea, cargar o descargar archivos de gran tamaño, acceder a archivos de audio o vídeo de remisión continua o crear de cualquier otra forma cargas innecesarias en el tráfico de la red asociadas con el uso de Internet que no se relacione con las actividades de negocio del grupo corporativo.

Panamericana tiene derecho a supervisar y registrar cualquier y todos los aspectos de su sistema informático incluyendo, entre otros, la supervisión de sitios de Internet visitados por usuarios, la supervisión de charlas y foros de noticias, la supervisión de descargas de archivos y todas las comunicaciones enviadas y recibidas por los mismos utilizando los Recursos de Información de Panamericana.

Está prohibido replicar mensajes de divulgación general o advertencias públicas hacia otros sin la autorización explícita del director de Sistemas.

Está prohibido el envió de mensajes de cadena bromas y advertencias de virus, así como inscribir la cuenta de correo electrónico corporativa en sitios como redes sociales o publicitarios con fines personales.

13.19 Seguridad de información y ciberseguridad en los procesos de administración de sistemas

Todos los recursos informáticos nuevos deberán contar con un mínimo de parámetros de seguridad, estos parámetros hacen referencia a las contraseñas, vigencias, bloqueos, permisos usuarios y perfiles.

La realización de un cambio tecnológico que no considere los requerimientos y las políticas, normas y organización en Seguridad de la Información y Ciberseguridad hace que Panamericana esté expuesta a riesgos; por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de este documento y en caso de exponer a La Compañía a un riesgo en seguridad de la información y ciberseguridad, debe ser identificado por el respectivo Dueño (responsable) de la Información.

En los contratos que así lo requieran se debe incluir mantenimiento y renovación de aplicaciones, estos mantenimientos o actualizaciones son programados con tiempo con el fin de asignar los recursos humanos y tecnológicos necesarios.

Toda adquisición, desarrollo o modificación de software debe incluir el suministro o actualización de

la documentación correspondiente del producto. Es obligación de quien adquiere o solicita un desarrollo o modificación del software de Panamericana, requerir la documentación del producto o la actualización de los manuales para en caso de cambio.

Los sistemas o aplicativos de Panamericana deben haber pasado por un proceso completo de pruebas y certificación por parte del Dueño (responsable) de la Información, antes de ser liberados a producción en un ambiente dedicado para tal fin.

Las aplicaciones por sí solas deben asegurar que la información que se procesa mantenga su integridad. En el diseño de aplicaciones se debe considerar la existencia de validaciones para el ingreso correcto de la información, mecanismos de verificación que aseguren su correcto procesamiento, especialmente cuando se realizan cálculos y alertas que comuniquen desviaciones críticas o de alto impacto.

14. SEGURIDAD EN NUEVAS TECNOLOGÍAS Y RIESGOS EMERGENTES

Es importante implementar un plan de seguridad de la información y ciberseguridad, con relación a las nuevas tecnologías. Para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se debe:

1. Establecer políticas de seguridad sobre las tecnologías que se implementen.
2. Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de seguridad de la información y ciberseguridad.
3. Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos.
4. Incluir en el plan de continuidad del negocio los requisitos de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.
5. Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de La Compañía en materia de seguridad.

15. MODELO DE EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para la identificación de riesgos y la aplicación de controles de seguridad de la información y ciberseguridad, Panamericana adopta y da a conocer el modelo de evaluación de seguridad de la información y ciberseguridad. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de seguridad de la información y Ciberseguridad e identificar las oportunidades de mejora que permitan fortalecerlo, basados en los dominios y controles propuestos en la norma NTC-ISO 27001:2013 y en el Framework de Ciberseguridad NIST.

16. COMUNICACIÓN LÍDERES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para propender por la estandarización de la aplicación del cumplimiento de la presente política en La Compañía, se establecerá como mecanismo de información oficial los siguientes:

Instrucciones Generales, donde incluirá actividades, por lo general metodológicas, previa evaluación y análisis. El Equipo de Seguridad de la Información Corporativo emite las Instrucciones Generales a los presidentes, Líderes de Seguridad de la Información y Ciberseguridad y cuando aplique Dueños de Proceso de los cuatro Bancos, Corficolombiana y Porvenir. Estos a su vez, divulgan la Instrucción General a sus pares de las filiales respectivas y algunas veces a otras áreas de interés según se indique en la Instrucción, para el caso de Panamericana las instrucciones son notificadas directamente de Proindesa S.A.S. Lo anterior, en cumplimiento del Protocolo de Comunicación definido por la Vicepresidencia Senior Corporativa de Riesgos y Cumplimiento de Grupo Aval.

Conceptos, son aclaraciones o ampliación de información, útiles para dar cumplimiento a las Instrucciones Generales, generalmente comunicaciones por medio de correo electrónico institucional. El Equipo Seguridad de la Información Corporativo emite Conceptos a los Líderes de Seguridad de la Información y Ciberseguridad de los cuatro Bancos, Corficolombiana y Porvenir, así como filiales adicionales en casos especiales, y éstos a su vez divulgan los Conceptos a los Líderes de Seguridad de la Información y Ciberseguridad de las filiales respectivas siguiendo el protocolo de comunicación.

Dentro del proceso de comunicación corporativo Grupo Aval y sus Entidades Subordinadas ha establecido el protocolo de comunicación con el fin de que la información emitida llegue a los niveles requeridos de manera clara y oportuna, así:

17. REPORTES

Con el fin de facilitar el monitoreo de cumplimiento, serán solicitados diferentes reportes de gestión que constituyan un efectivo apoyo para la administración; éstos deberán ser veraces, comprensibles, completos y oportunos.

Así mismo, Panamericana deberá informar a Proindesa y siguiendo el protocolo de comunicaciones establecido por Grupo Aval aquellos Incidentes Seguridad de la Información y Ciberseguridad que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de La Compañía en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos. Adicionalmente, La Compañía deberá tener una base de datos consolidada de incidentes de seguridad de la información y ciberseguridad clasificada en tipo de incidente, impacto y plan de remediación, así como, que este reporte se encuentre protegido dada la sensibilidad de esta información.

18. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

Todo trabajador de Panamericana deberá seguir las Políticas y normas para el buen uso de la información independiente del medio en que se utilice o acceda a ella, (software, hardware, redes y físicas) manteniendo siempre las características de confidencialidad, integridad, disponibilidad y privacidad y/o auditabilidad de la información de la misma. El cumplimiento es de carácter obligatorio para todos trabajadores, el no cumplimiento puede resultar en una acción disciplinaria que puede llegar hasta la terminación del contrato de trabajo y a un posible establecimiento de un proceso judicial bajo las leyes nacionales o internacional que apliquen. El desconocimiento de este documento no exime su aplicación.
La Política de Seguridad de la Información y Ciberseguridad está basada en las mejores prácticas en seguridad de la información y está acorde con la legislación nacional e internacional y por ende tomará los pasos necesarios, incluyendo las medidas legales aplicables, para proteger sus activos y el uso de ellos.

19. INVESTIGACIONES Y SANCIONES

Panamericana reconoce que en el evento de incumplimiento de esta política y demás actividades que se deriven de ella, las personas responsables por su aplicación y cumplimiento podrán ser objeto de acciones disciplinarias por parte de La Compañía que deberán tratarse con base en lo establecido en el Reglamento Interno de Trabajo y el Código de Ética y Conducta. Lo anterior, sin prejuicio de la eventual responsabilidad que pudiera derivarse por el incumplimiento de la normatividad aplicable a Seguridad de la Información y Ciberseguridad.

20. ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO

Las políticas y normas de Seguridad de la Información y Ciberseguridad deben mantenerse en el tiempo. Por lo anterior, es necesario efectuar una revisión anual o ante cambios estructurales y

normativos que afecten a Panamericana, para asegurar que ésta cumple con el cambio de las necesidades del negocio a este documento con el fin de validar cuáles serán los cambios para realizar teniendo como base las reuniones efectuadas por el Comité de Riesgos. Realizados los cambios se deberá publicar los mismos a todo el personal que hace uso de la información capacitando y haciendo énfasis en los cambios realizados.

Cualquier trabajador de La Compañía podrá enviar sugerencias o solicitudes que serán evaluadas en el Comité de Riesgos.

21. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

La Política de Seguridad de la Información y Ciberseguridad involucra el desarrollo e implantación de un programa de seguridad de la información y ciberseguridad, integrado en el día a día de la operación de Panamericana. Un programa efectivo de Seguridad de la Información y Ciberseguridad es un proceso continuo, no un evento. Para lograr los objetivos establecidos en este documento, la presente Política anticipa y autoriza el desarrollo de normas, estándares, procedimientos operativos detallados y otras medidas administrativas, los cuales serán publicados para conocimiento de los funcionarios; así como el desarrollo o la adquisición de herramientas de software que ayuden a detectar o prevenir ataques contra los sistemas donde reside la información de La Compañía ya sea que se encuentre en los aplicativos locales o en el ciberespacio.

El Comité de Riesgos debe impulsar la implantación y divulgación del programa de Seguridad de la Información y Ciberseguridad para lograr los objetivos establecidos en este documento con el fin de crear una cultura en la mejora de la aplicación de las políticas, normas estándares, procedimientos operativos detallados y otras medidas administrativas, los cuales serán publicados para conocimiento de los trabajadores.

22. EXCEPCIONES

No hay excepciones.

23. DOCUMENTOS DE REFERENCIA Y ANEXOS

- Política Corporativa de Seguridad de la Información y Ciberseguridad del Grupo Aval Versión 3.
- Políticas de Seguridad de la Información y Ciberseguridad Corporación Financiera Colombiana (Corficolombiana) versión 10.
- Instructivo modelo corporativo de gestión de riesgo – seguridad de la información y ciberseguridad de Grupo Aval.

24. CAMBIOS POSTERIORES A LA CREACIÓN DE LA POLÍTICA.

Fecha	Versión	Naturaleza del cambio
Nov.25/2013	1	Creación del Documento.

Fecha	Versión	Naturaleza del cambio
Agos.16/2017	2	Actualización del documento por cambios en denominación de cargos, periodicidad del comité de seguridad de la información y delegación del nuevo Líder de Seguridad de la Información.
Dic.31/2019	3	Actualización del documento.
Feb.28/2020	4	Actualización del documento.
Mar.17/2020	5	Actualización del documento.
Sept.28/2020	6	Actualización del documento, alineación a la política corporativa y al modelo de gestión de riesgos de seguridad de la información y ciberseguridad. Aprobado por la Junta Directiva mediante acta No. 292 del 28 de septiembre del 2020.
Nov. 29/2021	7	Actualización del documento, alineación a la política corporativa de Seguridad de la Información y ciberseguridad. Aprobado por la Junta Directiva mediante acta No. 308 del 29 de noviembre de 2021.
Dic.12/2022	8	Actualización del documento, alineación a la Política corporativa de Seguridad de la Información y Ciberseguridad de Corficolombiana. Aprobado por la Junta Directiva mediante acta No. 323 del 12 de diciembre de 2022.
Sep.19/2023	9	Actualización del documento, alineación a la Política corporativa de Seguridad de la Información y Ciberseguridad del Grupo Aval versión 3 según Instrucción Seguridad de la Información y Ciberseguridad No. 29 - Actualización Política Corporativa. Aprobado por la Junta Directiva mediante acta No. 334 del 19 de septiembre de 2023. Actualizado a la imagen corporativa el 22 de mayo de 2024.