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, La Concesión 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, Concesionaria Panamericana S.A.S. desarrolla el presente documento en el marco de la política corporativa para proteger y garantizar la disponibilidad, confidencialidad, Integridad y privacidad de la información y el establecimiento, implementación, mantenimiento y mejora continua de su sistema de gestión de seguridad de la información y ciberseguridad.

2. OBJETIVO

2.1 Objetivo General

Proteger los activos de información de Concesionaria Panamericana S.A.S., gestionando y cumpliendo los principios generales que preservan la información mediante la definición de políticas, identificación de riesgos y controles, que fijan roles y responsabilidades de los actores clave, que intervienen en el Sistema de Gestión de Seguridad de la información (SGSI).

2.2 Objetivo Específicos

- Establecer los lineamientos para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información y ciberseguridad en Concesionaria Panamericana S.A.S., con el fin de ser protegida de forma homogénea con base en la valoración de los activos de información.
- Garantizar la gestión de riesgos de seguridad de la información y ciberseguridad en Concesionaria Panamericana S.A.S., asimismo establecer e implementar los controles que preserven la confidencialidad, integridad, disponibilidad y privacidad de la información en la Concesión.
- Fijar roles y responsabilidades en materia de los pilares de seguridad de la información y ciberseguridad de Concesionaria Panamericana S.A.S.
- Garantizar la aplicación de los requisitos de seguridad de la información y ciberseguridad en la continuidad del negocio y la recuperación ante desastres en Concesionaria Panamericana S.A.S.
- 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

La presente Política de Seguridad de la Información y Ciberseguridad aplica a la alta dirección, la administración, todos los trabajadores de Concesionaria Panamericana S.A.S. y proveedores o contratistas que en el ejercicio de sus funciones utilicen información y servicios tecnológicos de la Concesión.

4. DEFINICIONES

- **Activo de información:** Todos los datos que hacen parte de un sistema de información y que pueden o no llegar a generar una decisión a la dirección de una compañía.
- **Administración:** Gerente General, Gerente Financiero y Administrativo y directores de área o quienes hagan sus veces.
- **Alta Dirección:** Junta Directiva, Gerente General y Representantes Legales o quienes hagan

sus veces.

- **Amenaza:** Causa potencial de un incidente no deseado, el cual puede causar daños a un sistema o a la organización

- **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 que pudiera convertirse en un ciberataque.

- **Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

- **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 desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad**.**

- **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.

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que reduce el riesgo.

- **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 Concesión 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 de una situación que puede afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

- **Incidentes de seguridad de la información:** 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.

- **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.

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

- **Políticas, Normas y Organización de Seguridad de la Información**: Documento de referencia para el buen uso de los activos de información de Concesionaria Panamericana S.A.S.

- **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 Datos, equipos y el software propietario o licenciado por Concesionaria Panamericana S.A.S.

- **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 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.

- **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:** Dícese de 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 defensa de Grupo Aval.

  Riesgo Inherente: 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 futuros. Una pérdida material es una pérdida o

combinación de pérdidas que puede dañar/deteriorar la condición financiera de una Entidad o Conglomerado, de manera que tenga la potencialidad de generar pérdidas para los depositantes, aseguradores e inversionistas.

- **Riesgo Residual:** 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 entidad.

- **Sistema de gestión de seguridad de la información:** 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 alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **Tecnología disruptiva:** Es aquella que desplaza a una tecnología sostenida, basada en productos innovadores que crean una industria completamente nueva.

- **Trabajador:** Trabajadores incluyendo la administración.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo**.** también denominada la 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.

5. NORMAS EXTERNAS

- **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 o naturaleza.

- **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.

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

disposiciones

- **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.

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

6. DECLARACIÓN DE COMPROMISO

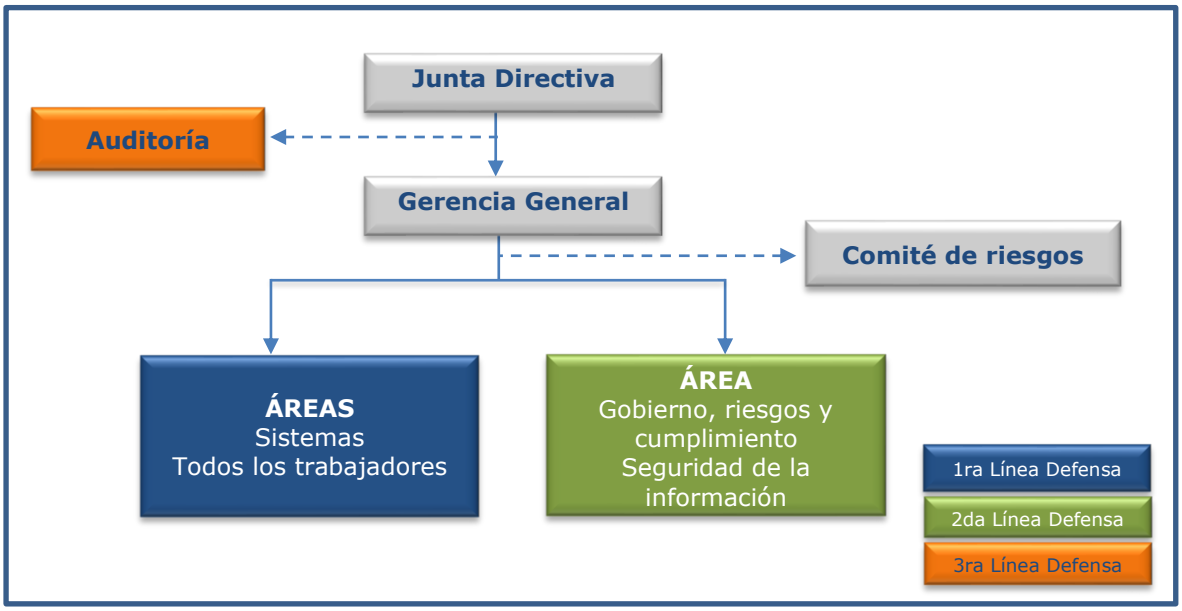
Concesionaria Panamericana S.A.S. está comprometida con la Política de Seguridad de la Información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los principios establecidos por el sistema de gestión de seguridad de la información y ciberseguridad por lo anterior deben:

- 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 al negocio 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.

7. 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 frente a todos los riesgos, de acuerdo con la Política Corporativa para la Gestión Integral de Riesgos; este marco de referencia define el esquema de las tres líneas de defensa, 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.



7.1 Primera línea de defensa

La primera línea de defensa la constituye la Dirección de Sistemas, la Coordinación de Peajes y todos los trabajadores de Concesionaria Panamericana. La Política de Seguridad de la Información y Ciberseguridad reconoce a las áreas de tecnología y demás colaboradores 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. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

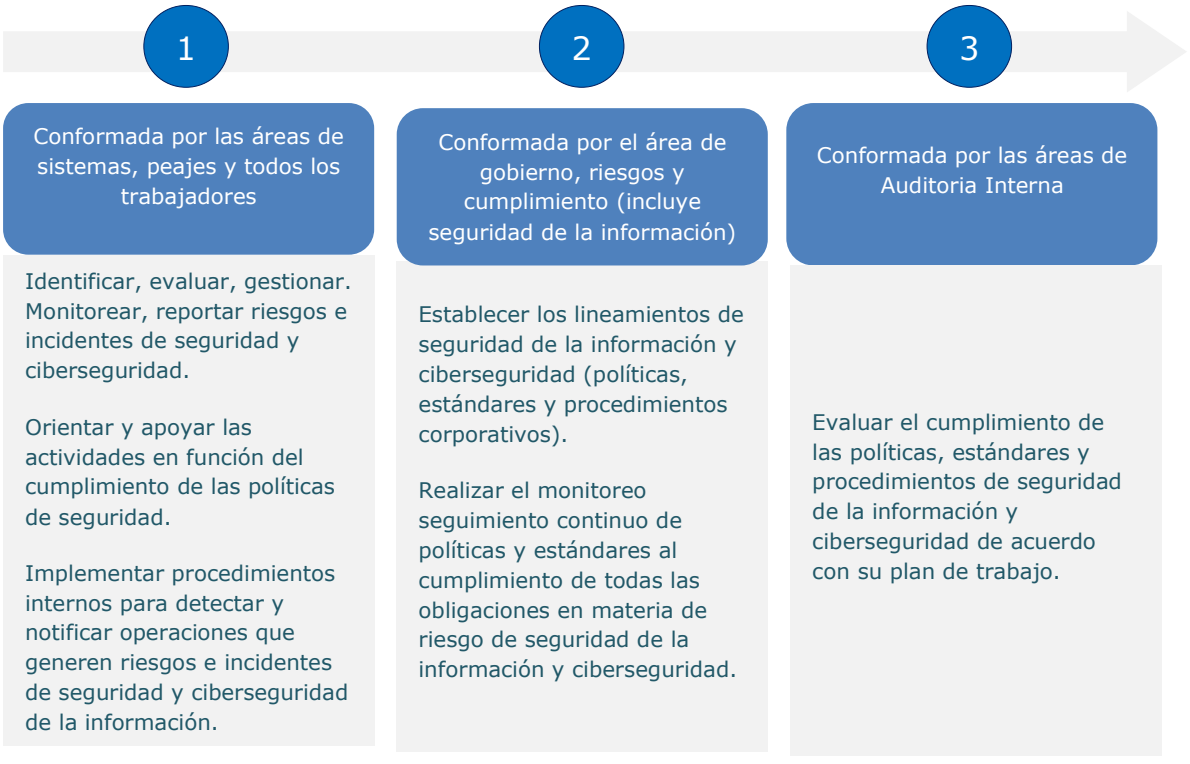
7.2 Segunda línea de defensa

Esta línea de defensa 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 Dirección. 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. 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.

7.3 Tercera Línea de Defensa

La tercera línea de defensa 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 Dirección. 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.



8. ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos 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 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 Concesionaria Panamericana	Aprobar la Política de Seguridad de la Información y Ciberseguridad de Panamericana. 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.	Supervisar la seguridad de la información y ciberseguridad, comprendiendo los riesgos y asegurando que estos sean gestionados.
Administración	Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de gestión de seguridad de la información.	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.	
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.	
Comité Ejecutivo de Seguridad de la Información de Grupo Aval	Informar de los acuerdos y decisiones corporativos de Seguridad de la Información y Ciberseguridad.	Monitorear el cumplimiento a nivel internos de las políticas del Sistema de gestión de seguridad de la información y ciberseguridad en cada entidad.
	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.	
	Informar principios, directrices y lineamientos Corporativos de Seguridad de la información y Ciberseguridad. Verificar el desarrollo de proyectos Corporativos de Seguridad de la información y Ciberseguridad y tomar las acciones preventivas y correctivas pertinentes para las empresas de Grupo Aval participantes en el servicio.	
	Identificar, evaluar e incluir los requerimientos de Seguridad de la información y Ciberseguridad en las iniciativas corporativas realizadas para las empresas del servicio.	
	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 actuará como comité de seguridad de la información	De acuerdo con los lineamientos corporativos, adapta, adopta e implementa las directrices, para el mejoramiento de la Gestión de Seguridad de la Información.	Conocer el resultado de la Gestión de Seguridad de la Información y ciberseguridad realizada por parte del Líder de Seguridad de la Información.
	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. 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.	Conocer los Incidentes de Seguridad de la Información presentados y que hayan tenido impacto significativo, reportados por las áreas y los planes de acción llevados a cabo para la mitigación de estos.
Área GRC (Segunda Línea)	Preparar reportes de Seguridad de la Información y ciberseguridad para los Comités.	Mantener actualizados los lineamientos de Seguridad de la Información y ciberseguridad aprobados por Junta Directiva.
	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.	
Líder Seguridad de la Información corresponde al Coordinador GRC	Presentar el informe de Gestión.	Conocer los Incidentes de Seguridad de la información y las medidas que se han implementado para mitigarlos.
	Participar en el Comité de Riesgos.	Monitorear el resultado de evaluación de Riesgos.
	Adoptar y socializar las mejores prácticas sugeridas en el Comité.	Definir y monitorear indicadores clave de desempeño sobre la gestión de Seguridad de Información y Ciberseguridad para dar alcance a

Actor	Actividades	
	De Ejecución	**De Supervisión**
		las actividades de supervisión al Área de sistemas
	Actualizar el Inventario de riesgos de seguridad de la información y ciberseguridad.	
	Adoptar los lineamientos establecidos por Grupo Aval y Corficolombiana.	
	Apoyar a la primera línea de defensa 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 Organización, con el fin de fortalecer la cultura de prevención de riesgos de Seguridad de la información y Ciberseguridad	
Área de Sistemas	Participar en el Comité Ejecutivo de Seguridad de la Información de su Entidad.	Velar porque se adopten medidas para responder a los incidentes presentados y para prevenir futuros incidentes.
	Adoptar y socializar las mejores prácticas sugeridas en el Comité.	Adoptar las mejores prácticas vigentes en el mercado con respecto a respuestas a incidentes.
	Informar al líder de Seguridad de Información sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad.	Apoyar en la definición y monitorear indicadores clave de desempeño sobre la gestión de seguridad informática y Ciberseguridad.
	Adoptar los lineamientos establecidos.	
	Apoyar a la segunda línea de defensa 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	Conocer los riesgos de Seguridad de Información que le son aplicables.	Vigilar y velar que su equipo de trabajo dé cumplimiento a la política de seguridad y ciberseguridad.
	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).	

Actor	Actividades	
	De Ejecución	**De Supervisión**
	Reportar a las áreas de seguridad informática y de seguridad de información, 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 y vigilar el cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.
Demás trabajadores	Son todos los trabajadores de Concesionaria 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.

9. POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La Alta Dirección de Concesionaria Panamericana S.A.S. reconoce la importancia de proteger adecuadamente la información de amenazas que vulneren 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 Concesión debe velar por:

1. El cumplimiento de los requisitos y principios de Seguridad de la Información y Ciberseguridad.
2. Proteger los activos de información y los activos tecnológicos de la organización.
3. Administrar, gestionar y mitigar los riesgos asociados a seguridad de la información y ciberseguridad en los procesos críticos de la Concesión.
4. 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.
5. Fortalecer la cultura de seguridad de la información de los colaboradores de Grupo Aval y sus Entidades Subordinadas, funcionarios temporales, contratistas y terceras partes, que administren activos de información.
6. 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, Concesionaria Panamericana S.A.S. 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:

9.1 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.

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

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

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

9.3 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 Gestión de Riesgos de Seguridad de la información y Ciberseguridad emitidas por Grupo Aval y Corficolombiana.

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

La Alta Dirección y la segunda línea de defensa de Panamericana deberán alinearse con la definición y alcance del modelo corporativo para la gestión de riesgos de Seguridad de la Información y Ciberseguridad, 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.

9.5 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.

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

La Alta Dirección y la segunda línea de defensa 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.

9.7 Gestionar el cambio

La Alta Dirección y la segunda línea de defensa 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.

9.8 Realizar Seguimiento y Presentar Informes

La segunda línea de defensa debe implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad de la Información 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 Concesionaria Panamericana, Indicadores Corporativos, Evolución de Riesgos y Evolución de Controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de Ciberseguridad.

9.9 Controlar y mitigar

La primera y segunda Línea de defensa 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 de defensa debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

9.1.1 Supervisión de controles de accesos físicos.
9.1.2 Supervisión de controles de accesos lógicos.
9.1.3 Supervisión y protección de contraseñas.
9.1.4 Supervisión protección de los puertos de configuración y acceso remoto.
9.1.5 Restricción de la instalación de aplicaciones por parte del usuario final.
9.1.6 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
9.1.7 Asegurar que las aplicaciones de software se actualicen regularmente, cuando aplique.
9.1.8 Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de una computadora).

9.10 Garantizar el sistema de Seguridad de Información y Ciberseguridad en situaciones de contingencia

La segunda Línea de defensa debe velar porque en los planes de continuidad del Negocio se incluyan y garanticen los pilares de la Seguridad de la información y ciberseguridad.

9.11 Garantizar el cumplimiento de la Ley vigente aplicable

Es obligación de las tres líneas de defensa dar cumplimiento a todas las normas de los reguladores vigentes que le aplique a Panamericana.

10. POLÍTICAS INDIVIDUALES

10.1 Seguridad de la información

La información del negocio es un activo vital de concesionaria panamericana S.A.S., 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 Concesionaria Panamericana S.A.S., y no por personal ajeno a la compañía.

La Seguridad de la información del negocio es el conjunto de medidas de protección que toma Concesionaria Panamericana S.A.S. contra una divulgación, modificación, hurto o 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 sus procesos, así mismo que cuenten con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de la misma.

Concesionaria Panamericana S.A.S., dispondrá 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.

10.2 Propiedad Intelectual

La propiedad de la información se debe mantener

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención ó información que es propiedad de Concesionaria Panamericana S.A.S.

Todo el material que es desarrollado mientras se trabaja para Concesionaria Panamericana S.A.S. 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.

10.3 Responsables de la información

Cada activo de información de concesionaria panamericana S.A.S. Debe tener un responsable que debe velar por su seguridad

La información que Concesionaria Panamericana S.A.S. 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 dependencias que reporten directamente del Gerente General o a quienes éste delegue.

10.4 Cumplimiento de regulaciones

Concesionaria Panamericana S.A.S. debe cumplir con las regulaciones locales de privacidad y seguridad de la información

Concesionaria Panamericana S.A.S. está acorde al cumplimiento de las leyes y regulaciones vigentes que así se requieran o apliquen.

10.5 Administración del riesgo en seguridad de la información

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

La información del área 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 un análisis del estado del área frente a la seguridad de la información, 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 Concesionaria Panamericana S.A.S.

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 de Concesionaria Panamericana S.A.S. y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información

10.6 Capacitación al personal en seguridad de la información

Concesionaria Panamericana S.A.S. debe establecer un programa permanente de creación de cultura en seguridad de la información 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; a su vez Concesionaria Panamericana S.A.S. estará en la obligación de informar cualquier modificación o cambio de este documento a los trabajadores, proveedores o terceros que accedan a la información.

10.7 Seguridad en el personal

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

Todo aspirante que pase un proceso de selección y que sea contratado directa o indirectamente como trabajador de la compañía será capacitado en este documento para su conocimiento y certificación.

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

Se debe mantener un registro por empleado de su entendimiento y seguimiento 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.

Concesionaria Panamericana S.A.S. incentivará a través de las capacitaciones el reporte de vulnerabilidades y riesgos que puedan identificar los trabajadores.

10.8 Terceros que acceden información de concesionaria panamericana S.A.S.

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

Todo acceso a la información de Concesionaria Panamericana S.A.S. 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. 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 manteniendo siempre los principios de confidencialidad, integridad, disponibilidad y privacidad y las consecuencias a que estarían sujetos en caso de incumplirla.

10.9 Identificación y autenticación individual

Todos los usuarios que acceden la información de Concesionaria Panamericana S.A.S. 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 de información de Concesionaria Panamericana S.A.S., 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.

10.10 Control y administración del acceso a la información

El uso de la información de Concesionaria Panamericana S.A.S. 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 Concesionaria Panamericana S.A.S. 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 basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad.

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.

10.11 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

Para la clasificación de la información Concesionaria Panamericana S.A.S., cuenta con las tablas de retención documental donde se establecen las siguientes categorías: Restringida, Confidencial y Pública. Esta clasificación es exclusiva del dueño de área y será el responsable de comunicarla a Gestión Documental para que sea incorporada en las tablas de retención documental.

Así mismo la información sensible que se maneje a través de archivos de Excel deberán contar con protección a través de claves que minimicen los riesgos de accesos no autorizados, cambios involuntarios de formulación errónea.

10.12 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

Concesionaria Panamericana cuenta con un procedimiento 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. Por lo anterior este procedimiento deberá estar documentado y divulgado a cada uno de los trabajadores cuando se requiera hacer uso del mismo.

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

10.13 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 confidencial del negocio debe mantenerse en lugares con acceso restringido cuando no es utilizada

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

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 Concesionaria Panamericana S.A.S.

10.14 No repudio

la autenticidad de un negocio o transacción electrónica que realice Concesionaria Panamericana S.A.S. debe ser asegurada

Concesionaria Panamericana se apoya en los medios electrónicos para realizar transacciones. Por lo anterior cada ingreso a un portal bancario 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 para portales bancarios. Este acceso se deberá hacer mediante un token los cuales deberán estar en custodia de cada usuario.

10.15 Administración de alertas

Concesionaria Panamericana S.A.S. 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 violen el presente documento deberán ser informadas al Líder de Seguridad de la Información o Comité de Riesgos de manera inmediata (alertas). Estas alertas quedaran registradas con el fin de mitigarlas, llevarlas a comité y tomar acciones sobre ellas.

10.16 Auditabilidad de los eventos de seguridad de la información

Los registros de seguridad de la información de Concesionaria Panamericana S.A.S. deben ser revisados permanentemente para asegurar el cumplimiento del modelo de seguridad de la información

Las aplicaciones Core del negocio o de misión crítica poseen registros de seguridad que permiten auditarlos en caso de ser necesario. Se precisa que la administración y soporte de estas aplicaciones está en cabeza de Proindesa.

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.

10.17 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 Concesionaria Panamericana S.A.S. deben realizarse de una manera segura, para ello se cuenta con un firewall que permite la segmentación de redes y separación del tráfico de los servidores.

Cualquier integrante de la comunidad que acceda a la red debe cumplir con la presente política, de requerirse una conexión segura VPN, esta deberá ser aprobada por la gerencia encargada 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 que el acceso a la aplicación se realice desde una red externa de la Concesión, 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.

10.18 Uso de los recursos informáticos del negocio

Los recursos informáticos son provistos a la comunidad para uso exclusivo del negocio

Los recursos informáticos y de comunicaciones de Concesionaria Panamericana S.A.S. son exclusivamente para propósitos del proceso y de la compañía, está prohibido el uso de estos recursos en actividades distintas a las del proceso.

10.19 Seguridad de información en los procesos de administración de sistemas

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

Actividades, normas y responsabilidades en seguridad de la información 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.

11. NORMAS EN SEGURIDAD DE LA INFORMACIÓN

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:

11.1 Seguridad de la información

La información del negocio de Concesionaria Panamericana S.A.S., 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 Concesionaria Panamericana y no debe ser ejecutada por personal externo a ella.

11.2 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 Concesionaria Panamericana S.A.S., 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.

11.3 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 toda La Comunidad.

11.4 Cumplimiento de regulaciones

Concesionaria 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 de la Dirección de Sistemas.

Concesionaria Panamericana S.A.S. 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.

11.5 Administración del riesgo de seguridad de la información

Concesionaria 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.

11.6 Capacitación y entrenamiento al personal sobre seguridad de la información

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. La compañía deberá evaluar la necesidad de capacitar proveedores críticos.

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 serán divulgados a todos los trabajadores.

11.7 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 Concesionaria Panamericana S.A.S.

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 Concesionaria Panamericana S.A.S. Lo anterior, según lo establecido tanto en el contrato laboral como en el Código de Ética y Conducta, lo cual será de obligatorio cumplimiento y el no aplicarlo tendrá implicaciones disciplinarias. Dependiendo de la gravedad, Concesionaria Panamericana S.A.S. 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 de Concesionaria Panamericana S.A.S. 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.

11.8 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 Concesionaria Panamericana S.A.S. 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 Concesionaria Panamericana S.A.S. debe cumplir con los siguientes ítems:

- El ingreso a una aplicación debe ser por parte del trabajador de Concesionaria, nunca se deben dar las claves ni los usuarios de acceso a los terceros.
- Debe de existir cláusulas de confidencialidad en los contratos para el manejo e intercambio de la información entre terceros y la compañía.

11.9 Identificación y autenticación individual

- Cada trabajador es responsable por sus acciones mientras usa cualquier recurso de información de Concesionaria Panamericana S.A.S., 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.
- Concesionaria Panamericana S.A.S., 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 Concesionaria Panamericana S.A.S. incluso si deben hacerlo desde una estación diferente a la asignada.

11.10 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 Concesionaria Panamericana S.A.S. 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.

11.11 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: Restringida, Uso Interno y Pública, de acuerdo con el estándar de clasificación de información establecido por Concesionaria Panamericana S.A.S.

- Cuando la información restringida o confidencial de la Compañía por razones de área, deba ser desechada se debe destruir de manera segura, 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.
- Si un equipo en enviado a un tercero y a su vez tiene información restringida esta deberá ser eliminada, desechada o destruida.

11.12 Continuidad del negocio y recuperación de información

Toda la información de Concesionaria Panamericana S.A.S. que está alojada en servidores y 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.

Concesionaria Panamericana S.A.S. 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.

11.13 Seguridad física

Las áreas físicas de Concesionaria Panamericana S.A.S. 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 Concesionaria Panamericana S.A.S.

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.

Concesionaria Panamericana S.A.S. 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 Coordinación Administrativa con el fin de conceder acceso en caso de pérdida o daño de la misma.

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.

11.14 No repudio

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

Concesionaria Panamericana S.A.S. 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.

11.15 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.

Concesionaria Panamericana S.A.S. 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.

11.16 Auditabilidad de los eventos de seguridad de la información

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 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.

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.

11.17 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 organización impidiendo el acceso a sitios no autorizados para el desarrollo de sus actividades.

11.18 Uso de los recursos informáticos del negocio

Los Recursos de Información de Concesionaria Panamericana S.A.S. deben ser utilizados únicamente para fines de negocio aprobados por Concesionaria. Está prohibido el uso de los Recursos de Información de Concesionaria 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 a la Gerencia General.

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

Concesionaria Panamericana S.A.S. 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 de las Gerencias y 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 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 Coordinador 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 de Concesionaria Panamericana S.A.S. cuando hace uso de los servicios de Internet e Intranet. Los usuarios autorizados explícitamente por Concesionaria 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.

Concesionaria Panamericana S.A.S. 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 Concesionaria Panamericana S.A.S.

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

Está prohibido él 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.

11.19 Seguridad de información 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 hace que Concesionaria Panamericana S.A.S. 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, 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 Concesionaria Panamericana S.A.S., requerir la documentación del producto o la actualización de los manuales para en caso de cambio.

Los sistemas o aplicativos de Concesionaria Panamericana S.A.S. 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.

12. SEGURIDAD EN TECNOLOGÍAS DISRUPTIVAS Y RIESGOS EMERGENTES

Es importante implementar un plan de seguridad de la información y ciberseguridad, con relación a los servicios de integración de datos, digitalización, automatización de procesos, seguridad en la nube, entre otros, alineando esfuerzos para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se debe:

1. Establecer políticas de las tecnologías disruptivas que se implementen en la compañía.
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 tecnologías disruptivas para determinar y aplicar los controles de seguridad de la información y ciberseguridad.
3. Documentar los procedimientos de muestreo hasta la presentación de reportes, flujos de los procesos de automatización, codificación y pruebas de los sistemas disruptivos utilizadas por la compañía.
    - Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las tecnologías disruptivas como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos. Incluir en el plan de continuidad del negocio los requisitos de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.
    - 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 organización.

13. 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 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.

14. COMUNICACIÓN LÍDERES DE SEGURIDAD DE LA INFORMACIÓN

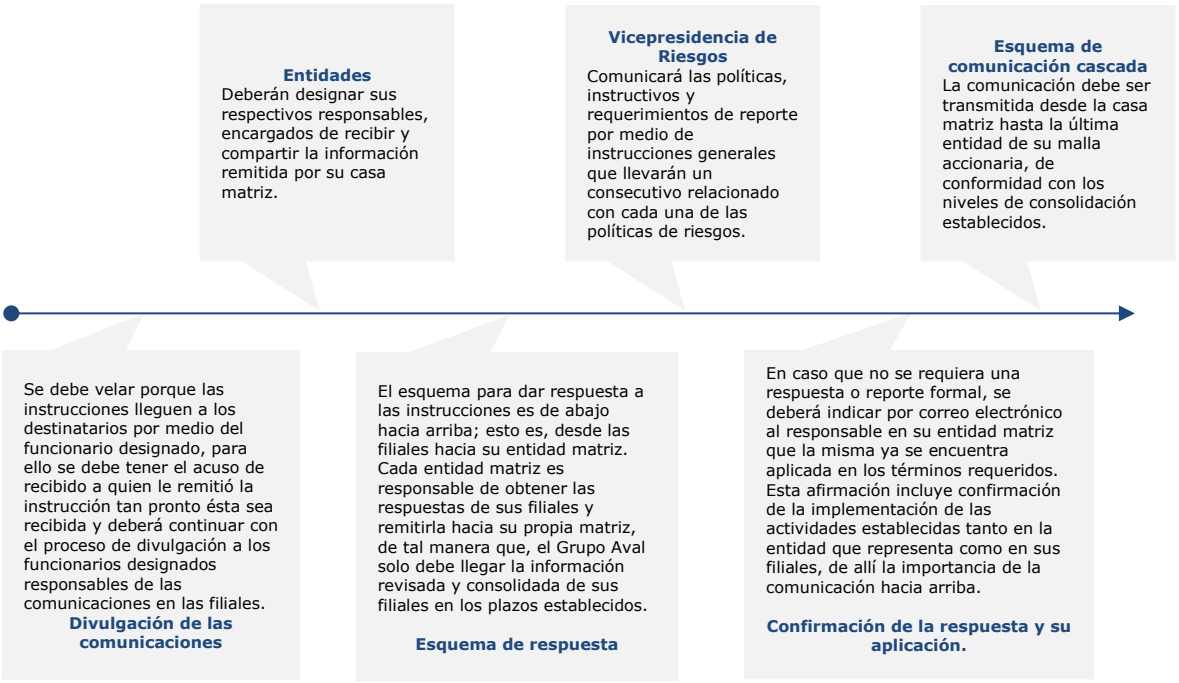
Para propender por la estandarización de la aplicación del cumplimiento de la presente política en la compañía, se establecerá como mecanismo de información oficial los siguientes:

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 cuando aplique Dueños de

Proceso de los cuatro Bancos y Corficolombiana. 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 Concesionaria Panamericana las instrucciones son notificadas directamente de Proindesa S.A.S. Lo anterior, en cumplimiento del Protocolo de Comunicación definido por la Vicepresidencia de Riesgos 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 de los cuatro Bancos y Corficolombiana, así como filiales adicionales en casos especiales, y éstos a su vez divulgan los Conceptos a los Líderes de Seguridad de la Información 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:



15. 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.

Asimismo, 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.

16. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

Todo trabajador de Concesionaria Panamericana S.A.S. 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 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 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.

17. INVESTIGACIÓNES Y SANCIONES

Concesionaria Panamericana S.A.S 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 deberán tratarse con base en lo establecido en el Código de Ética y Conducta, en el capítulo acciones por incumplimiento.

18. ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO

Las políticas y normas de Seguridad de la Información deben mantenerse en el tiempo. Por lo anterior, es necesario efectuar una revisión anual a este documento con el fin de validar cuáles serán los cambios a 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 integrante de la comunidad podrá enviar sugerencias o solicitudes que serán evaluadas en el Comité de Riesgos.

19. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

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

20. EXCEPCIONES

No hay excepciones.

21. DOCUMENTOS DE REFERENCIA Y ANEXOS

- Política corporativa de seguridad de la información y ciberseguridad
- Instructivo modelo corporativo de gestión de riesgo – seguridad de la información y ciberseguridad de Grupo Aval

22. ANEXOS:

Anexo 1: Matriz de Roles de la Organización de Seguridad Vs. Cargos de la Compañía

23. CAMBIOS POSTERIORES A LA CREACIÓN DEL PROCEDIMIENTO.

FECHA	VERSIÓN	NATURALEZA DEL CAMBIO
Nov.25/2013	1	Creación del Documento
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.