

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 1 de 17

Tabla de Contenido

DEFINICIONES	3
1. OBJETIVO GENERAL	4
2. FUNDAMENTO.....	4
2.1. ALCANCE.....	4
2.2. ORGANIZACIÓN ROLES Y RESPONSABILIDADES	4
2.2.1. Comité de Seguridad de la Información	4
2.2.2. Director de Sistemas y Líder de Seguridad de la Información	4
2.2.3. Responsable de la Información	5
2.2.4. Comunidad	5
2.3. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA	5
2.4. ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO.....	5
2.5. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA	5
3. POLÍTICAS INDIVIDUALES	5
3.1. SEGURIDAD DE LA INFORMACIÓN.....	5
3.2. PROPIEDAD INTELECTUAL	6
3.3. RESPONSABLES DE LA INFORMACIÓN	6
3.4. CUMPLIMIENTO DE REGULACIONES.....	6
3.5. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN	6
3.6. CAPACITACIÓN AL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN	7
3.7. SEGURIDAD EN EL PERSONAL.....	7
3.8. TERCEROS QUE ACCEDEN INFORMACIÓN DE CONCESIONARIA PANAMERICANA S.A.S. ..	7
3.9. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL	7
3.10. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN	8
3.11. CLASIFICACIÓN DE LA INFORMACIÓN.....	8
3.12. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE INFORMACIÓN	8
3.13. SEGURIDAD FÍSICA	8
3.14. NO REPUDIO	8
3.15. ADMINISTRACIÓN DE ALERTAS.....	9
3.16. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.....	9
3.17. CONECTIVIDAD	9
3.18. USO DE LOS RECURSOS INFORMÁTICOS DEL NEGOCIO	9
3.19. 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	9
4. NORMAS EN SEGURIDAD DE LA INFORMACIÓN	9

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 2 de 17

4.1. SEGURIDAD DE LA INFORMACIÓN.....	9
4.2. PROPIEDAD INTELECTUAL.....	10
4.3. RESPONSABLES DE INFORMACIÓN.....	10
4.4. CUMPLIMIENTO DE REGULACIONES.....	10
4.5. ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN.....	10
4.6. CAPACITACIÓN AL PERSONAL SEGURIDAD DE LA INFORMACIÓN.....	10
4.7. SEGURIDAD EN EL PERSONAL.....	10
4.8. TERCEROS QUE ACCEDEN A LA INFORMACIÓN LOCAL O REMOTAMENTE.....	11
4.9. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL.....	11
4.10. CONTROL Y ADMINISTRACIÓN DE ACCESO A LA INFORMACIÓN.....	12
4.11. CLASIFICACIÓN DE LA INFORMACIÓN.....	12
4.12. CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE INFORMACIÓN.....	13
4.13. SEGURIDAD FÍSICA.....	13
4.14. NO REPUDIO.....	13
4.15. ADMINISTRACIÓN DE ALERTAS.....	14
4.16. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.....	14
4.17. CONECTIVIDAD.....	14
4.18. USO DE LOS RECURSOS INFORMÁTICOS DEL NEGOCIO.....	15
4.19. SEGURIDAD DE INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACION DE SISTEMAS	16
5. EXCEPCIONES.....	16
6. DOCUMENTOS DE REFERENCIA Y ANEXOS.....	16
7. CAMBIOS POSTERIORES A LA CREACIÓN DEL PROCEDIMIENTO.....	16

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 3 de 17

INTRODUCCIÓN

Concesionaria Panamericana S.A.S. define este documento como referencia para todos los trabajadores con el fin de dar a conocer y aplicar las políticas, normas y organización de la Seguridad de la Información, así mismo establecer las personas encargadas de proteger, salvaguardar y vigilar los activos de información de la compañía.

Por lo anterior desde la Gerencia General se lidera todo lo concerniente a la Seguridad de la Información y se determina que todos los trabajadores deben acatar este documento, las políticas, normas, procedimientos, instructivos, manuales, formatos y responsabilidades que se deriven del mismo.

DEFINICIONES

Actividades asociadas al Rol: Se refiere al conjunto de labores que son inherentes a un Rol por la naturaleza de las mismas de pertenecer a una misma área de experticia.

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.

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.

Compañía: se refiere a Concesionaria Panamericana S.A.S.

Comunidad: se refiere a todos los trabajadores de Concesionaria Panamericana S.A.S., sin importar el rol que desempeñe.

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.

Disponibilidad de la información: Es un estado de la información que siempre se deberá mantener con el fin de ser consultada por un usuario o aplicación en cualquier momento.

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 de la información: Propiedad que busca mantener los datos sin modificaciones no autorizadas.

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.

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

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.

Rol: Se refiere al papel, área de responsabilidad y actividades que debe desempeñar una persona para contribuir a la organización en la protección de la información.

 CONCESIONARIA PANAMERICANA	TITULO DEL DOCUMENTO POLÍTICAS Y NORMAS EN SEGURIDAD DE LA INFORMACIÓN DE CONCESIONARIA PANAMERICANA S.A.S.	Código: CP-PO-TI-01
		Versión : 2
		Fecha: Ago.16/2017
		Página: 4 de 17

1. OBJETIVO GENERAL

Establecer las directrices, roles, lineamientos y responsabilidades necesarias relacionadas con la Seguridad de la Información al interior de Concesionaria Panamericana S.A.S., protegiendo siempre el buen nombre de la organización.

El siguiente documento es una declaración de las Políticas y Normas de Seguridad de la Información aceptadas para proteger la Información en Concesionaria Panamericana S.A.S., tomando como documento de referencia la norma ISO 27001.

2. FUNDAMENTO

Toda la Información de Concesionaria Panamericana S.A.S. es clasificada como un activo de información, por lo anterior, siempre se deberán mantener los principios básicos de seguridad como son la confidencialidad, la integridad, la disponibilidad de la misma.

La confidencialidad de la Información de Concesionaria Panamericana, así como aquella perteneciente a terceros, debe ser mantenida, independientemente del medio o formato donde se encuentre.

La Información del Negocio debe ser preservada en su integridad y debe estar disponible cuando se requiera, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.

2.1. ALCANCE

Este documento da las directrices requeridas para implantar en Concesionaria Panamericana Modelo de Seguridad de la Información confiable y flexible y a su vez servirá como referencia de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con la misma.

La Seguridad de la Información deberá ser aplicada a todos los niveles jerárquicos incluyendo usuarios, proveedores y entes que requieran hacer uso de ella. El acceso y uso externo de la información solo está permitido a los trabajadores que estén autorizados y que así lo requieran.

2.2. ORGANIZACIÓN ROLES Y RESPONSABILIDADES


La administración de la Seguridad de la Información será responsabilidad de quienes al interior de Concesionaria Panamericana S.A.S., estén o desempeñen algunos de los siguientes roles:

2.2.1. Comité de Seguridad de la Información

- Responsables de asegurar la planeación, implantación y mantenimiento de las Políticas, Normas y Organización de Seguridad de la Información; al igual que de la ejecución de las acciones preventivas y correctivas para mantener niveles de seguridad óptimos.
- El comité está conformado por: Gerente Financiero y Administrativo, Director Jurídico, Director de Operación y Mantenimiento, Director de Sistemas y Líder de Desarrollo Organizacional los cuales sesionarán cada seis meses. Sus atribuciones responsabilidades y funcionamiento se encuentran descritos en el documento Organización de Seguridad de la Información.

2.2.2. Director de Sistemas y Líder de Seguridad de la Información

- Responsable por la implantación, mejoras verificación y cumplimiento de la Política de Seguridad de la Información y los medios requeridos para lograrlo.
- El Oficial de Seguridad de la Información es quien coordina la implementación y vela por el correcto funcionamiento del Modelo de Seguridad de la Información en línea con los requerimientos del área y bajo las directrices del Comité de Seguridad de la Información de la Compañía, soportado en el Asesor de Seguridad de la Información.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 5 de 17

- Representa a la compañía interna y externamente en todo lo que concierne a Seguridad de la Información de la Entidad

2.2.3. Responsable de la Información

- Todos los trabajadores de la compañía que manejen activos de información son responsables por mantener la confidencialidad de la misma. Será responsable por administrarla y clasificarla acorde a la importancia que la misma tiene para u área. Debe velar por el cumplimiento de la Política de Seguridad de la Información al interior de su área de los trabajadores que tienen acceso a ella.

2.2.4. Comunidad

- Son todos los trabajadores de Concesionaria Panamericana, (usuarios de la información) responsables de poner en práctica los programas y planes liderados por el Comité de Seguridad de la Información 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.

2.3. 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 los 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 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.

2.4. 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 Seguridad de la Información. 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 Seguridad de la Información y a su vez podrán ser comunidades al líder de Seguridad de la Información para ejercer este rol en Concesionaria se designó Director de Sistemas

2.5. IMPLANTACIÓN Y PROGRAMACIÓN DE LA POLÍTICA

El Comité de Seguridad de la Información 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.

3. POLÍTICAS INDIVIDUALES

3.1. SEGURIDAD DE LA INFORMACIÓN

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 6 de 17

LA INFORMACIÓN DEL NEGOCIO ES UN ACTIVO VITAL DE CONCESIONARIA PANAMERICANA S.A.S. Y POR LO TANTO DEBEN 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 empresa.

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.

**3.2. 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.

**3.3. 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.

**3.4. 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.

**3.5. 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 Seguridad de la Información, 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.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 7 de 17

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

3.6. 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.

3.7. 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, mediante la certificación de este documento y las demás normas y procedimientos que se expidan al respecto.


Concesionaria Panamericana S.A.S. desarrollará un programa de manejo de sugerencias en seguridad de la información, por medio del cual los empleados reportarán vulnerabilidades y riesgos que detecten.

3.8. 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

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 encargada. 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 y disponibilidad y las consecuencias a que estarían sujetos en caso de incumplirla.

3.9. 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

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 8 de 17

individual mediante un usuario y clave de autenticación, la cual no será develada ni podrá ser compartida

**3.10. 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.

**3.11. CLASIFICACIÓN DE LA INFORMACIÓN
LOS RESPONSABLES DE LA INFORMACIÓN DEBEN CLASIFICAR LA INFORMACIÓN BASADOS EN SU VALOR, SENSITIVIDAD, 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.

**3.12. 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.


**3.13. 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 O SENSITIVA AL 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 idóneo de Concesionaria Panamericana S.A.S.

**3.14. 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.

 CONCESIONARIA PANAMERICANA	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 9 de 17

3.15. 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

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

3.16. 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 (ERP-Nomina) poseen registros de seguridad que permiten a Concesionaria Panamericana S.A.S. auditarlos en caso de ser necesario.

La fecha y hora de todos los relojes de donde se encuentren recursos de información deben estar sincronizadas (aplica inicialmente para la sede administrativa) con el fin de tener una fecha y hora precisa de un evento.

3.17. 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.

3.18. 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.


3.19. 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

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

4. NORMAS EN SEGURIDAD DE LA INFORMACIÓN

4.1. 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.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 10 de 17

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

4.2. 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.

4.3. RESPONSABLES DE INFORMACIÓN

Se establece a los Gerentes, Directores, Coordinadores 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.

4.4. 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 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.

4.5. ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Concesionaria Panamericana realizara periódicamente análisis de riesgos 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 con custodiadas.

4.6. CAPACITACIÓN AL PERSONAL SEGURIDAD DE LA INFORMACIÓN

Los nuevos trabajadores de Concesionaria Panamericana S.A.S. después de seguir un proceso de selección y una vez vinculados, recibirán capacitación de este documento para su conocimiento, haciendo énfasis en la importancia y cumplimiento del mismo.


El documento podrá ser consultado en la Intranet corporativa, este será el único sitio donde se encuentran los documentos actualizados y en las últimas versiones del Sistema de Gestión de Calidad.

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

Se realizaran pruebas aleatorias que permitan medir bajo encuestas o preguntas el conocimiento de las políticas y normas en seguridad de la información.

4.7. 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.

 CONCESIONARIA PANAMERICANA	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 11 de 17

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 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 Seguridad de la Información deben estar actualizados en avances tecnológicos que mitiguen el riesgo en el que se pueda ver afectada la compañía.

4.8. 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:

- Acompañamiento por parte de un trabajador de Concesionaria Panamericana.
- 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.

4.9. 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.
- Para los trabajadores de la vía se manejara autenticación individual en cada estación de trabajo y no bajo la modalidad de autenticación en un servidor de dominio, a su vez estos usuarios están en la obligación de hacer el cambio de contraseña de forma periódica.
- Toda solicitud de creación, modificación y eliminación de usuario debe ser aprobada por los Gerentes o Directores 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, acceso a la red, Uno Enterprise Siesa.
- 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, (aplica para usuarios de la sede administrativa), 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 usuarios deben usar siempre su código para acceder a los Recursos de Información de Concesionaria Panamericana S.A.S. incluso si deben hacerlo desde una estación diferente a la asignada.

 CONCESIONARIA PANAMERICANA	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 12 de 17

4.10. CONTROL Y ADMINISTRACIÓN DE ACCESO A LA INFORMACIÓN

Las aplicaciones que así lo permitan manejen perfiles de acceso que permitan las actividades del trabajador.

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 (Jefes/Gerentes/Directores 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.

El Dueño (Responsable) de la Información debe realizar una comparación periódica entre los requerimientos de acceso de los usuarios a los aplicativos y el nivel de acceso con que realmente cuentan y verificar que los usuarios que efectivamente acceden la información corresponden a los autorizados previamente por él.

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 quien este delegue.
- 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 con el fin de utilizarlos en los casos que el usuario principal presente problemas.

4.11. 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.

Toda información clasificada como restringida y almacenada en cualquier medio (físico, magnético, portable o impreso), debe ser rotulada. En el caso que la información contenga piezas de distinto tipo, ésta debe rotularse con la clasificación más alta de cualquier elemento de información contenida.

- 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 es enviado a un tercero y a su vez tiene información restringida esta deberá ser eliminada, desechada o destruida.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 13 de 17

4.12. 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 debe estar aprobada por el Gerente de área.

Se deben definir usuarios de contingencia y un programa de administración de los mismos, para ser utilizados en el momento en que se presente la contingencia

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 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.

4.13. 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, Auxiliar de Gestión Documental, Analista de Peajes y Director de Sistemas según el área que corresponda.

Concesionaria 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.

Concesionaria Panamericana cuenta con circuitos alternos de suministro de energía UPS para soportar la carga de los equipos que almacenan activos de información del negocio.


Las llaves físicas o tarjetas que permiten el acceso a sitios restringidos solo debe ser usada 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.

Concesionaria cuenta con un cronograma de mantenimiento de los recursos que alojan activos de información.

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

4.14. NO REPUDIO

 CONCESIONARIA PANAMERICANA	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 14 de 17

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 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 nieguen su participación.

4.15. 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 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.

4.16. 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.

La información de auditoría de Concesionaria Panamericana S.A.S. debe estar disponible para su uso por las personas autorizadas para tal fin.

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.

4.17. 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 legítima 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.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 15 de 17

Todo acceso externo debe ser autenticado, para ésta 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 firewall que bloquean categorías de navegación para toda la organización impidiendo el acceso a sitios no autorizados para el desarrollo de sus actividades.

4.18. 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 correspondiente gerencia.

Solamente los recursos de seguridad designados para este fin deben de estar instalados en los equipos, End Point 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 continua 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.

	TITULO DEL DOCUMENTO	Código: CP-PO-TI-01
	POLÍTICAS Y NORMAS EN SEGURIDAD DE LA	Versión : 2
	INFORMACIÓN DE CONCESIONARIA PANAMERICANA	Fecha: Ago.16/2017
	S.A.S.	Página: 16 de 17

Está prohibido el envío 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.

4.19. SEGURIDAD DE INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACION 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 aplicativos de Concesionaria Panamericana S.A.S. debe 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.

5. EXCEPCIONES

No hay excepciones.

6. DOCUMENTOS DE REFERENCIA Y ANEXOS

Documentos de Referencia:


- Organización de Seguridad de la Información de Concesionaria Panamericana S.A.S.
- Política para el adecuado uso de elementos de información en los puestos de trabajo

Anexos:

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

7. 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

	<p>TITULO DEL DOCUMENTO</p> <p>POLÍTICAS Y NORMAS EN SEGURIDAD DE LA INFORMACIÓN DE CONCESIONARIA PANAMERICANA S.A.S.</p>	Código: CP-PO-TI-01
		Versión : 2
		Fecha: Ago.16/2017
		Página: 17 de 17

		seguridad de la información y delegación del nuevo líder de seguridad de la información.
--	--	------------------------------------------------------------------------------------------