POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

REVISÓ:	REVISÓ:	APROBÓ:
Chistian Fajardo Oficial de Seguridad de la información	Guillermo Bolaños Coordinador Tecnologia de la Información	Ricardo Postarini Herrera Gerente General

1. INTRODUCCIÓN

El propósito de este documento es definir los lineamientos, controles y dar a conocer a los colaboradores de COVIANDINA S.A.S, la Política de Seguridad de la Información y ciberseguridad establecida para la protección de la información.

Esta Política de Seguridad de la Información y ciberseguridad aplica para todos los niveles de la organización: Usuarios (que incluye empleados y accionistas), Clientes, Terceros (que incluye proveedores y contratistas), Entes de Control y Entidades Relacionadas; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación.

Por lo tanto, los colaboradores de la Concesionaria Vial Andina COVIANDINA S.A.S, deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, ya que éstos soportan la Política de Seguridad de la Información y ciberseguridad; en el entendido que la alta gerencia tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de seguridad de la información, de acuerdo con las responsabilidades asignadas dentro de la organización en relación con los siguientes temas:

2. GENERALIDADES

2.1. SEGURIDAD DE LA INFORMACIÓN.

- La información de COVIANDINA S.A.S, sin importar su presentación, medio o formato, en el que sea creada o utilizada para el soporte a las actividades de negocio, se califica como información del negocio o activo de información.
- La Seguridad de la información del negocio es el conjunto de medidas de protección que toma COVIANDINA S.A.S, contra la 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 Responsables de la información son los responsables de asegurar que la información del negocio, cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información.
- COVIANDINA S.A.S, debe disponer de los medios necesarios para asegurarse de que cada miembro de la Comunidad preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.
- COVIANDINA S.A.S, debe contar con una estructura organizacional de seguridad de la información que permita gestionar y controlar lo dispuesto en el Modelo de Seguridad de la Información.
- COVIANDINA S.A.S, debe controlar la copia de información por medio de dispositivos USB, para ello COVIANDINA S.A.S tiene disponible el antivirus SYMANTEC ENDPOINT PROTECTION el cual permite el bloqueo y administración de los puertos USB.
- COVIANDINA S.A.S, debe controlar el bloqueo y protección de Discos Duros de cada equipo, para ello COVIANDINA S.A.S tiene disponible en la configuración del sistema operativo el aplicativo de cifrado de unidades BITLOCKER, el cual permite el bloqueo y cifrado de los Discos Duros de cada equipo de la compañía

2.2. PROPIEDAD INTELECTUAL

- La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de COVIANDINA S.A.S.
- Todo el material que es desarrollado mientras se trabaja para COVIANDINA 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 que menoscabe la competitividad de COVIANDINA S.A.S.

2.3. RESPONSABLES DE LA INFORMACIÓN.

- COVIANDINA S.A.S, utiliza información para realizar sus actividades. Esta se crea y se entrega a cada miembro de la Comunidad para que pueda desarrollar y cumplir sus respectivas metas dentro del marco del negocio.
- La información que COVIANDINA S.A.S, utilice para el desarrollo de sus objetivos de negocio debe tener asignado un Responsable, quien la utiliza en su área y es el responsable por su correcto uso. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso.

2.4. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN.

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

2.5. CAPACITACIÓN Y CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN

- COVIANDINA S.A.S, debe contar con un programa permanente que permita asegurar que los usuarios y terceros están informados acerca de sus responsabilidades en Seguridad de la Información y de las continuas amenazas que ponen en riesgo la información que maneja.
- Los colaboradores y terceros deben estar enterados de los procedimientos de seguridad de la información que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo.

2.6. SEGURIDAD EN EL PERSONAL

- Los empleados que ingresen a COVIANDINA S.A.S, deben seguir un proceso de selección, y una vez vinculados, recibirán copia del documento “Política de la Seguridad de la Información y Ciberseguridad” 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 conocimiento y entendimiento de la Política de Seguridad de la Información y ciberseguridad, mediante la certificación de este documento y las demás normas y procedimientos que se expidan al respecto.

2.7. TERCEROS QUE ACCEDEN INFORMACIÓN DE COVIANDINA S.A.S. LOCAL O REMOTAMENTE

- El uso de la información de COVIANDINA S.A.S S.A.S, por Terceros, ya sea local o remotamente, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política.
- En los contratos se debe incluir la obligación de proteger la información de COVIANDINA S.A.S, los requisitos de seguridad para mitigar los riesgos sobre la información y las consecuencias a que estarían sujetos en caso de incumplirla.
- La transferencia, envió y recepción de información a terceros debe ser realizada a través de mecanismos de comunicación seguros.

2.8. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL

- Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de COVIANDINA S.A.S., Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser establecida y autenticada de una manera única y no podrá ser compartida.
- Los usuarios de COVIANDINA S.A.S., una vez creados y asignadas sus autorizaciones en el Sistema de Información, podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo, COVIANDINA S.A.S., definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

2.9. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN

- Se deben establecer mecanismos de control de acceso físico y lógico para asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el negocio y con los riesgos de pérdida de Confidencialidad, Integridad, Disponibilidad, Privacidad y Auditabilidad de la información.
- Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso a la información de COVIANDINA S.A.S, deberá ser otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de COVIANDINA S.A.S, debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.
- El acceso a plataformas y aplicaciones debe ser asignado de acuerdo a las políticas definidas, y teniendo en cuenta las funciones de los cargos en las diferentes áreas de la organización.
- **VPN:** La conexión remota al área local debe realizarse a través de una conexión VPN segura suministrada por la organización, el cual debe ser aprobada y registrada.

- **Redes inalámbricas:** El área de tecnología debe implementar mecanismos de autenticación que eviten accesos no autorizados. Para el caso de personal externo a la organización, se le otorgará una conexión por WIFI de invitados, que se será gestionado por el área de tecnología con autorización del personal encargado.

2.9.1. Gestión de accesos de usuarios:

- La organización establecerá privilegios para el control de acceso, de cada usuario o grupo de usuarios, a los distintos aplicativos o sistemas de información. De igual forma se velará que los colaboradores y personal tengan acceso a información con base a las funciones o responsabilidades asignadas.
- Todo funcionario que requiera tener acceso a los sistemas de información de la entidad, debe ser autorizado y así mismo acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password).
- Cada funcionario debe hacerse responsable del uso y manejo de credenciales asignadas, evitando publicarlas o compartirlas.
- La creación, modificación y eliminación de usuarios, contraseñas y privilegios de acceso en infraestructura es responsabilidad del área de tecnología.
- En el momento que se termine el contrato laboral, el funcionario de la entidad o tercero, se debe inactivar o retirar inmediatamente los permisos que fueron otorgados en los diferentes sistemas de información.

2.9.2. Revisión de los derechos de acceso:

Los derechos de acceso, de los colaboradores a los diferentes aplicativos o sistemas de información, se deben revisar después de cada cambio, promoción, cambio de cargo o terminación de contrato.

2.9.3. Procedimiento de ingreso seguro

- Para el ingreso seguro a los sistemas de información o aplicativos, la entidad debe llevar un control de registro a través de un log de los ingresos exitosos y fallidos.
- Se debe implementar un mecanismo seguro que permita bloquear los equipos de cómputo en cierto periodo de inactividad.
- En los aplicativos, no se debe visualizar las contraseñas de ingreso de los usuarios.
- Los tiempos de conexión deben ser restringidos para brindar seguridad a los diferentes aplicativos.

2.9.4. Sistema de gestión de contraseñas

- La contraseña de los usuarios de los diferentes aplicativos o sistemas de información, deben cumplir con los parámetros mínimos de seguridad como número mínimo de caracteres, uso de mayúsculas y minúsculas, uso de caracteres especiales, entre otros) para tener una contraseña fuerte y segura.
- Para el uso y administración de contraseñas, se debe tener en cuenta los siguientes aspectos:

- ✓ Que sean fáciles de recordar
- ✓ No estar basadas en algo que otra persona pueda adivinar fácilmente como por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- ✓ Estar libres de caracteres numéricos o alfabéticos idénticos consecutivos.

- Los sistemas de información o aplicativos deben exigir el cambio periódico de contraseñas a los usuarios.

2.9.5. Manejo de medios

- La información almacenada en cualquier medio removible, debe ser eliminada en el momento de ser entregada algún ente externo, con el fin de que no se pueda recuperar.
- El funcionario autorizado para el acceso y manejo de medios removibles, debe proteger la información que contiene los medios removibles.
- Los medios removibles que estén a punto de perder su funcionalidad, se debe realizar una copia de seguridad para evitar la pérdida de información.
- Los equipos de cómputo, no deben contar con el acceso o el permiso para el ingreso de memorias USB o cualquier dispositivo de almacenamiento externo.
- El oficial de seguridad de la información realiza un monitoreo al estado de los puertos y cifrado de discos duros.

2.10. CONTINUIDAD DEL NEGOCIO

La información debe estar disponible para su uso autorizado cuando COVIANDINA S.A.S., la requiera en la ejecución de sus tareas regulares. Por lo que se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de COVIANDINA S.A.S S.A.S, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que utilice COVIANDINA S.A.S., como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso de tiempo.

La entidad tiene definido a través de sus procedimientos documentados las actividades a desarrollar para la activación del plan de continuidad del negocio, las cuales deben ser desarrollado como mínimo una (1) vez al año.

La organización cuenta con una estructura adecuada sobre un centro alterno de operaciones, el cual tiene como funcionalidad preparar, mitigar y responder ante un evento que requiera la activación del plan de continuidad del negocio.

2.11. SEGURIDAD FÍSICA

- Las áreas físicas construidas para soportar toda la operación del negocio, deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.
- Los recursos informáticos de COVIANDINA S.A.S, deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.

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

2.11.1. Protección de Equipos

- Los colaboradores y/o proveedores que tenga acceso a las instalaciones de COVIANDINA S.A.S no puede fumar y consumir algún tipo de alimento cerca de los equipos de cómputo.
- Los equipos de la entidad, como servidores, equipos de comunicaciones, centros de cableado, UPS, aire acondicionado, planta telefónica, estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contenga o brinde información sensible deben estar protegidos y ubicados de forma adecuada.
- No se debe realizar uso de un PC diferente al asignado al funcionario, el cual se puede realizar en casos importantes que requiera la operación de la organización.

2.11.2. Retiro y seguridad de equipos, medios de información

- Todos los colaboradores de COVIANDINA S.A.S son responsables de velar por la seguridad de los equipos que se encuentran fuera de las instalaciones.
- Los equipos portátiles deben tener especial cuidado, y no exponerlos a cualquier riesgo que pueda afectar la confidencialidad de la información y la integridad física del funcionario.
- En caso de pérdida o robo de un equipo de COVIANDINA S.A.S, se debe reporta de forma inmediata al jefe del área, para realizar los respectivos trámites internos, como poner la denuncia ante las autoridades competentes.
- El retiro de equipos de cómputo, dispositivos de almacenamiento, software y medios magnéticos con información sensible de COVIANDINA S.A.S, deben seguir con los procedimientos establecidos por el área de tecnología.

2.11.3. Equipo de usuario sin atención

- El usuario en su equipo de cómputo asignado, debe bloquear la sesión en el momento que deje de realizar funciones sobre el o realice cualquier cese de actividades.
- Es responsabilidad de todos los colaboradores cerras las sesiones y dejas los equipos apagados cuando termine sus labores.

2.11.4. Escritorio y pantalla limpia

- Todos los equipos de cómputo, deben usar papel tapiz y protector de pantalla corporativo, con un tiempo de cinco (5) minutos para que se active automáticamente, después del periodo de inactividad.
- Los colaboradores deben ser responsables de la información bajo su custodia, manteniéndola segura bajo llave, en el momento de abandonar su puesto de trabajo o se deje desatendido.

2.11.5. Dispositivos móviles

- Los colaboradores que manejen información de la entidad a través de dispositivos móviles deberán protegerla física y lógicamente con el fin de evitar el hurto, acceso o divulgación de información no autorizada.
- La utilización de los dispositivos móviles para el manejo de información de la entidad, deben estar autorizados por el líder o jefe de área.

2.12. CONECTIVIDAD

- Las conexiones a la red privada de COVIANDINA S.A.S, deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida a otras empresas deben realizarse sobre redes aprobadas por COVIANDINA S.A.S.
- Los miembros de la Comunidad que se conecten a la red privada, deben cumplir con la presente Política antes de que se realice la misma. Esto aplica igualmente a cualquier conexión actual o futura en la red de COVIANDINA S.A.S, que utilice medios públicos para integrar lugares que estén geográficamente dispersos.
- Se requiere la aprobación del Responsable de la Información para poder acceder remotamente a la información de COVIANDINA S.A.S, y dichos accesos deben cumplir con la Identificación y Autenticación requerida.

2.13. USO DE LOS RECURSOS INFORMÁTICOS DE LA COMPAÑÍA

- Los recursos informáticos de COVIANDINA S.A.S, son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Miembros de la Comunidad que intenten acceder a información para la que no tienen un requerimiento autorizado de negocio, están violando la presente Política.
- COVIANDINA S.A.S, se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por COVIANDINA S.A.S, podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Responsable de Seguridad de la Información.
- El uso del correo electrónico debe ser realizado de forma adecuada por los colaboradores, y con fines netamente laborales.

2.14. USO ADECUADO DEL INTERNET:

- Los colaboradores deben realizar buen uso del internet, no accediendo a paginas desconocidas o con contenido pornográfico y así mismo cumpliendo con los protocolos de seguridad recomendados.
- No acceda a sitios web a través de enlaces incluidos en mensajes de correo electrónico o en sitios Web de terceros; usualmente la suplantación de identidades (Pishing) se vale de este medio para recolectar los datos de los usuarios y cometer fraude. La forma más segura de ingresar es digitando la dirección del sitio que se desea (es decir escribiendo www.sitio_que_quiero_visitar.com

- El uso de Youtube, grooveshak, realplayer, emisoras por internet, servicios de reloj por Internet, estado del tiempo, horóscopos, calendarios, protectores de pantalla o cualquier servicio que se actualice por Internet, consumen grandes cantidades de recursos de red (ancho de banda), ocupan la memoria y sobrecargan el procesador. Como consecuencia, el desempeño del computador y de la red corporativa serán lentos para todos los usuarios dificultando la tarea de quienes requieren los recursos de la red disponibles para el envío de mensajes importantes en el desempeño de sus labores y perjudicando en general a toda la compañía.
- Se tiene configurado y establecido un firewall para no permitir el acceso a páginas web o sitios no autorizados para tener una navegación segura.

2.15. SEGURIDAD DE INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACIÓN DE SISTEMAS

- Actividades, normas y responsabilidades en seguridad de la información deben ser incluidas dentro de cada uno los procesos de administración de sistemas de COVIANDINA S.A.S, para lograr el cumplimiento de la Política y las Normas de Seguridad de la Información.
- La Dirección de TIC debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura. Los requerimientos de seguridad de la información deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información.
- Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información que han sido previamente establecidos. El nivel de Seguridad de la Información de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.
- La implantación de un sistema nuevo o cambio significativo a los existentes, debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.
- La realización de un cambio tecnológico que no considere los requerimientos de seguridad de la Información hace que COVIANDINA S.A.S, este expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad y ciberseguridad de la Información y sus respectivas normas, y en caso de exponer a COVIANDINA S.A.S, a un riesgo en seguridad de la información, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo Responsable de la Información.
- En la gestión de Incidentes de seguridad de la información, se registra, asigna, hace seguimiento y resuelve situaciones (problemas) que comprometen la disponibilidad de los servicios que provee tecnología al negocio.

2.16. SEGURIDAD DE LAS OPERACIONES

Garantizar las operaciones de la entidad, cumplan con las condiciones de seguridad requeridas para mantener su confidencialidad, disponibilidad e integridad.

2.16.1. Protección contra software malicioso

- La entidad cuenta con herramientas de seguridad como antivirus, AntiSpam, y otras aplicaciones las cuales brindan protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño permanente de la información.

- Proporcionar los mecanismos para generar cultura de seguridad entre los colaboradores de la entidad y terceros frente a los ataques de software malicioso.
- Asegurar que el software de antivirus, AntiSpam, y otras aplicaciones cuenten con licencias de uso requerido.
- Se tiene configurado y establecido un mecanismo a través del firewall que no permite descargar programas no autorizados.

2.16.2. Copias de respaldo

- La entidad debe asegurar que la información de los aplicativos y de las diferentes áreas de la compañía, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su confidencialidad, integridad y disponibilidad.
- La entidad establece un plan de restauración de copias de seguridad que serán probadas a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo.
- Los medios magnéticos que contienen la información sensible deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo debe contener los mecanismos de seguridad adecuados.

2.16.3. Control del software operacional

El oficial de seguridad de la información realiza seguimiento y control al software operacional instalado en los diferentes equipos de la entidad.

2.17. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

- El responsable de seguridad de la información, define los eventos considerados como críticos (intentos de acceso fallido al sistema de información y borrado o alteración de la información) y los respectivos registros de seguridad de la información que deben ser registrados.
- Los incidentes de seguridad de la información se registran y monitorean en el formato de FT-TEC-007 Bitácora de eventos e incidentes de seguridad de la información.
- Los usuarios deben reportar al líder de seguridad de la información cualquier tipo de anomalía o incidente de seguridad que se presente.

2.18. ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

- Los usuarios deben almacenar o guardar la información en las carpetas direccionadas para obtener una seguridad y respaldo de la información a través de un dispositivo de almacenamiento conectado a la red.
- El envío y recepción de información que no pueda ser tramitada por correo electrónico corporativo, debe ser emitida o compartida a través del OneDrive, tanto para personal interno y personal externo.
- No se puede realizar envió o compartir archivos utilitarios a través de la nube OneDrive.

2.19. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

- El cumplimiento de La Política de Seguridad de la Información y Ciberseguridad, con sus respectivas normas es obligatorio para la Comunidad. Cada miembro de la misma debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información de COVIANDINA S.A.S.
- Cualquier incumplimiento de esta Política que comprometa la Confidencialidad, Integridad, Disponibilidad, Privacidad y/o Auditabilidad de la información, puede resultar en una acción disciplinaria que puede llegar hasta la terminación del contrato de trabajo y a un posible establecimiento de un proceso judicial bajo las leyes nacionales o internacionales que apliquen.

3. DOCUMENTOS DE REFERENCIA Y ANEXOS

FT-TEC-007 Bitácora de eventos e incidentes de seguridad de la información

4. CONTROL DE CAMBIOS

FECHA	VERSIÓN	ORIGEN
25/05/2017	1	Creación del Documento
20/02/2020	2	Revisión general del documento
08/07/2020	3	Revisión y actualización del documento, relacionado con los puntos: 2.7; 2.9; 2.10; 2.11; 2.13; 2.14; 2.16; 2.17; 2.18