MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - SOCIETE TSALACH

1. INTRODUCCION

Para **SOCIETE TSALACH** el objetivo es "Alcanzar la excelencia operacional y optimizar los procesos y la productividad de la organización y convertirnos en la mejor empresa del sector turismo.

La información es un recurso que, como el resto de los activos, tiene valor para la sociedad y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la Compañía.

Este documento tiene como objeto dar a conocer las políticas de seguridad de la información y para que los principios de la Política de Seguridad de la Información sean efectivos, se implementa la misma, buscando que forme parte de la cultura organizacional de la Compañía, lo que implica que debe contarse con el manifiesto compromiso de todos(as) los(as) colaboradores(as) de una manera u otra vinculados a la gestión para difusión, consolidación y cumplimiento.

2. DEFINICIONES

2.1. La seguridad de la información se entiende como la preservación de las siguientes características:

§ **CONFIDENCIALIDAD:** Se garantiza que la información no esté disponible o se revele a personas no autorizadas.

§ **INTEGRIDAD:** Cuando la información es exacta y completa.

§ **DISPONIBILIDAD:** Cuando la información es accesible y utilizable a los usuarios autorizados. Adicional, se debe considerar los siguientes aspectos que la complementan:

- Ø **Autenticidad:** Cuando se garantiza la identidad de quien solicita acceso a la información.
- Ø **No repudio:** Es la forma de evitar que quien envió o recibió información alegue que no lo realizó ante terceros.
- Ø **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la empresa.
- Ø **Confiabilidad:** La información generada es la adecuada para la toma de decisiones.
- Ø **Información:** se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas, cartográficas, narrativas o audiovisuales y en cualquier medio, ya sea magnético, en papel, en computadoras, audiovisual u otro medio.
- Ø **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procesamientos, tanto automatizados como manuales.

2.2. ACTIVO: Cualquier cosa que tenga valor para **SOCIETE TSALACH.**

2.3. CONTROL: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la empresa que pueden ser de naturaleza administrativa, técnica de gestión o legal. También se usa como sinónimo de salvaguarda o contramedida.

2.4. DIRECTRIZ: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

2.5. SERVICIOS DE PROCESAMIENTO DE INFORMACIÓN: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que lo albergan.

2.6. EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información. Una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

2.7. INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

2.8. POLÍTICA: Toda intención y directriz expresada formalmente por **SOCIETE TSALACH**

2.9. RIESGO: Combinación de la probabilidad de un evento y sus consecuencias.

2.10. AMENAZA: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema o a la empresa.

2.11. VULNERABILIDAD: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

3. MARCO REGULATORIO

Para los propósitos de este documento se considera la legislación vigente en informática y proyectos de ley en Colombia:

- **LEY 603 DEL 2000:** Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde que el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
- **LEY 1266 DEL 2008:** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **LEY 1273 DEL 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- **LEY 1341 DEL 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **LEY 1581 DE 2.012:** Por medio de la cual se expidió el Régimen General de Protección de Datos Personales, el cual tiene por objeto: *"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".*

- **DECRETO 1377 DE 2.013:** Por medio del cual se reglamentó parcialmente Ley Estatutaria 1581 de 2.012 en los aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales.
- **DECRETO 886 DE 2.014:** Por medio del cual se reglamentó la información mínima que debe contener el Registro Nacional de Bases de Datos.

Aspectos claves de la normatividad:

- Cualquier ciudadano tendrá la posibilidad de acceder a su información personal y solicitar la supresión o corrección de la misma frente a toda base de datos en que se encuentre registrado.
- Establece los principios que deben ser obligatoriamente observados por quienes hagan uso o de alguna manera realicen el tratamiento o mantengan una base de datos con información personal, cualquiera que sea su finalidad.
- Aclara la diferencia entre clases de datos personales construyendo las bases para la instauración de los diversos grados de protección que deben presentar si son públicos o privados, así como las finalidades permitidas para su utilización.
- Crea una especial protección a los datos de menores de edad.
- Establece los lineamientos para la cesión de datos entre entidades y los procesos de importación y exportación de información personal que se realicen en adelante.
- Define las obligaciones y responsabilidades que empresas de servicios tercerizados tales como Call y Contact Center, entidades de cobranza y, en general, todos aquellos que manejen datos personales por cuenta de un tercero, deben cumplir en adelante.
- Asigna la vigilancia y control de las bases de datos personales a la ya creada Superintendencia Delegada para la Protección de Datos Personales, de la Superintendencia de Industria y Comercio.
- Crea el Registro Nacional de Bases de Datos.
- Establece una serie de sanciones de carácter personal e institucional dirigidas a entidades y funcionarios responsables del cumplimiento de sus lineamientos.

4. POLITICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

SOCIETE TSALACH, consiente de la importancia que tiene la información para el desarrollo de sus procesos, los cuales son de obligatorio cumplimiento por colaboradores(as), proveedores, y contratistas que están encaminadas a proteger los recursos de información y tecnología utilizadas para su procesamiento, frente amenazas internas o externas implementa los mecanismos necesario para garantizar la confidencialidad, integridad y disponibilidad de la información

Para dar cumplimiento a esta política general, se establecen los siguientes objetivos de control:

- Los propietarios de la información, deben identificar y clasificar los activos de información de la empresa para establecer los mecanismos de protección necesarios.
- La sociedad define e implanta controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.
- Todos los(as) colaboradores(as) y contratistas, deben ser responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Se deben realizar auditorías y controles periódicos sobre la gestión de seguridad de la de la compañía.
- La empresa autoriza el uso de software adquirido legalmente.
- Es responsabilidad de todos(as) los(as) colaboradores(as) y contratistas de la empresa, reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las políticas y controles de seguridad de la información deben ser reportadas, registradas y monitoreadas.
- **SOCIETE TSALACH** debe contar con un plan de continuidad del negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- Adicionalmente la sociedad cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

4.1. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. La empresa, debe tener un modelo para administrar la seguridad de la información, enfocado en las mejores prácticas y al cumplimiento a regulaciones internas y externas.

4.2. CAPACITACIÓN Y CONCIENTIZACIÓN. SOCIETE TSALACH, debe llevar a cabo un programa anual de sensibilización y capacitación a los(as) colaboradores(as) sobre seguridad de la información, con el fin de que ésta sea parte integral de nuestra cultura organizacional.

4.3. ORGANIZACIÓN DE SEGURIDAD. Se creará un comité de seguridad de la información, el cual estará integrado por el área de servicio al cliente y el área de sistemas y tecnología de la empresa para que se diseñe e implementen las mejores prácticas y estándares de seguridad de la información, las cuales se deben socializar a través de procedimientos y campañas, asegurando el cumplimiento de su confidencialidad, integridad, disponibilidad y confiabilidad.

4.4. SEGURIDAD DE LOS RECURSOS HUMANOS. La sociedad, debe establecer compromisos de confidencialidad con todos(as) los(as) colaboradores(as) y usuarios externos que tengan la posibilidad de acceder a nuestra información e infraestructura para su procesamiento, así como las herramientas y mecanismos para garantizar que los usuarios se encuentren capacitados para respaldar la **Política de Seguridad de la Información de SOCIETE TSALACH**, con el fin de reducir los riesgos de error humano, uso inadecuado de las instalaciones y recursos, y manejo no autorizado de la información.

4.5. CLASIFICACIÓN Y CONTROL DE ACTIVOS - GESTIÓN DE ACTIVOS. El área de sistemas y tecnología, como custodio y responsable de la protección de los activos de información de la empresa, debe diseñar y establecer los mecanismos que le permitan proteger su confidencialidad, integridad y disponibilidad, de tal manera que garantice que sus usuarios sean conscientes de su responsabilidad y protección.

4.6. CONTROL DE ACCESOS. Los responsables de la administración de la infraestructura tecnológica (área de sistemas y tecnología) de nuestra empresa, debe asignar los accesos a plataformas, usuarios y segmentos de red, de acuerdo a procesos formales de autorización, los cuales deben ser revisados de manera periódica, con el fin de evitar el acceso de usuarios no autorizados a los sistemas de información.

4.7. CRIPTOGRAFÍA. El área de sistemas y tecnología, debe implementar controles criptográficos que les permitan a los usuarios asegurar y proteger la confidencialidad, la autenticidad y la integridad de la información del negocio.

4.8. SEGURIDAD FÍSICA Y DEL ENTORNO. La empresa debe contar con mecanismos y procedimientos de seguridad operacionales, para controlar el acceso a todas las áreas destinadas al procesamiento y/o almacenamiento de información sensible o crítica, así como aquellas en las que se encuentran los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, con el fin de proteger la información, el software y el hardware de daños intencionales o accidentales y evitar el acceso no autorizado.

4.9. SEGURIDAD DE LAS OPERACIONES. La empresa, debe establecer los mecanismos que aseguren la operación correcta y segura del procesamiento de la información y comunicaciones, y la operación adecuada de su infraestructura tecnológica, a través de políticas, normas, procedimientos e instructivos de trabajo, debidamente actualizados y socializados.

4.10. SEGURIDAD DE LAS COMUNICACIONES. La empresa debe establecer los mecanismos que aseguren la protección y la confidencialidad e integridad de la información en las redes y los servicios relacionados contra acceso no autorizado, a través de procedimientos, documentos políticas y controles.

4.11. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN. La empresa debe contar con procedimientos que contengan los requisitos para los controles de seguridad en la adquisición de nuevos sistemas de información o en las mejoras a los existentes; proteger la confidencialidad, autenticidad o integridad de la información.

4.12. RELACIONES CON PROVEEDORES. La empresa debe, implementar controles a los proveedores que gestionan información para asegurar la protección de los activos de la sociedad. Como también se debe establecer y acordar todos los requisitos, riesgos y niveles acordado de seguridad de la información pertinente, con cada proveedor.

4.13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. La sociedad debe establecer los mecanismos para que los(as) colaboradores(as), contratista y usuarios, tomen conciencia de su responsabilidad de reportar los eventos y debilidades de seguridad de la

información, asociados con los sistemas de información, inmediatamente sucedan, con el fin de tomar las medidas necesarias para responder a tales incidentes y establecer las medidas necesarias para evitarlos en el futuro.

4.14. PLAN DE CONTINUIDAD DEL NEGOCIO. SOCIETE TSALACH, debe implementar un proceso de gestión para la continuidad del negocio, mediante controles preventivos y acciones de recuperación según la evaluación de riesgos, el cual contenga los requisitos de seguridad de la información necesarios, con el fin de atender la recuperación por la pérdida de los activos de información, causados por desastres naturales, accidentes, fallas o acciones deliberadas u otros hechos.

4.15. CUMPLIMIENTO DE POLÍTICAS Y NORMATIVIDAD LEGAL. **SOCIETE TSALACH**, debe implementar procedimientos y establecer controles para asegurar el cumplimiento de las normas y políticas de seguridad internas, requisitos estatutarios, reglamentarios y contractuales pertinentes para cada sistema de información.

4.16. PROTECCION DE DATOS PERSONALES. SOCIETE TSALACH, ha establecido manuales y procedimientos para el uso, protección y transferencia adecuado de los datos personales dando cumplimiento a la Ley 1581 de 2012 de Protección de Datos Personales.

5. POLÍTICAS EMPRESARIALES DE LA SEGURIDAD DE LA INFORMACIÓN

5.1. POLITICA PARA EL MANEJO DE LA INFORMACIÓN.

Esta política tiene como finalidad establecer las directrices para proteger la información contra uso no autorizado, divulgación o publicación, modificación, daño o pérdida y establecer el cumplimiento de reglamentaciones y leyes aplicables a **SOCIETE TSALACH**

- **Acuerdos de Confidencialidad:** Los funcionarios y contratistas de la empresa deben firmar acuerdos de confidencialidad al momento de realizar la legalización de sus respectivos contratos, en los cuales se comprometen a no divulgar, usar o explotar la información empresarial a la cual tengan acceso. L
- Los proveedores, prestadores de servicio u otros, que requieran tener acceso a la información confidencial de la empresa, deben firmar un acuerdo de confidencialidad. En caso de que el proveedor no esté de acuerdo con la firma de éste, no podrá tener acceso a la información requerida.
- **Propietario de la Información:** La información empresarial (artículos, revistas, videos, fotos, entre otros) administrada, manejada o creada por los empleados de **SOCIETE TSALACH,** independiente de su forma de vinculación es de la empresa, al igual que los sistemas de información desarrollados por personal interno o externo. La sociedad es propietaria de los derechos de esta información.
- **Derechos de Autor:** Está prohibido por las leyes de derechos de autor y por **SOCIETE TSALACH** hacer copias de la información institucional en cualquier formato, copias no autorizadas de software ya sea adquirido o desarrollado por la empresa. La sociedad no realizará copias de seguridad de software que no le esté permitido.
- **Publicaciones de Seguridad de la Información:** Todos los usuarios de servicios de tecnologías de información, deben aplicar las directrices dadas a través de publicaciones o

comunicadas en capacitaciones o campañas institucionales respecto a la seguridad de la información.

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de **SOCIETE TSALACH**, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable y sin afectar la productividad.

- Los usuarios no deben propagar cadenas de mensajes de cualquier tipo y la comunicación de tipo comercial, político, religioso y en general cualquier contenido ofensivo para los funcionarios de **SOCIETE TSALACH**
- Los empleados o contratistas de la empresa deben cumplir con fidelidad como producto de las tareas que les fueron asignadas y guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa de la cual tengan conocimiento en el ejercicio de sus funciones.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por **SOCIETE TSALACH** y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Es deber de los funcionarios verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
- **Equipos de procesamiento de datos tipo servidor:** Los administradores de servidores, bases de datos y demás roles que manejen información clasificada como semiprivada y privada, deben garantizar la confidencialidad de la información y el uso de credenciales de administración (usuario y contraseña), sin excepción.
- **Equipos de procesamiento de datos tipo servidor:** La administración de los equipos de procesamiento de datos tipo servidor que soportan servicios empresariales debe ser realizada por el área de sistemas y tecnología.
- Cualquier cambio o modificación en el sistema de información interno de la empresa, debe ser realizado por el área de sistemas y tecnología.

5.2. POLITICA DE USO DE RECURSOS TECNOLÓGICOS.

- **Instalación, Mantenimiento y Actualización de Hardware:** El personal adscrito al área de sistemas y tecnología es el único autorizado para instalar aplicaciones y realizar mantenimientos preventivos y correctivos en los equipos de cómputo de la sociedad.
- **Uso de los Equipos de Cómputo:** Los equipos de cómputo (computadores, impresoras, portátiles, servidores, tablas y demás elementos similares) de la empresa serán utilizados únicamente por el personal autorizado para el desarrollo de las actividades asignadas.
- Todo funcionario o contratista es responsable del equipo que le sea asignado; el cual será incluido a su inventario personal, de acuerdo con el procedimiento establecido por el área de recursos humanos de la empresa.
- Los dispositivos móviles (portátiles, tablets, celulares) propiedad de la sociedad, no deben ser desatendidos. El usuario deberá tomar las medidas de seguridad pertinentes que permitan garantizar la integridad y confidencialidad del activo de información.
- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad de la empresa, el usuario responsable del mismo deberá informarlo al área de sistemas y tecnología a través de un correo electrónico, para una asistencia especializada y, por ningún motivo, deberá intentar resolver el problema.

- **Artículos de Decoración en Equipos de Cómputo:** Se debe mantener el equipo de cómputo libre de fotos, calcomanías, plantas y/o cualquier otro elemento que lo pueda deteriorar o comprometer su integridad.
- **Software en los Equipos de Cómputo:** Para todos los equipos de cómputo propiedad de la empresa, se instalará únicamente el software que cuente con licencia autorizada para uso en la sociedad. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley antipiratería.

- **Software Antivirus:** Para todos los equipos de cómputo propiedad de la empresa, se instalará únicamente el software antivirus que el área de sistemas y tecnología establezca.
- Los usuarios que hacen uso de los servicios de tecnología de información y comunicación, deban realizar tareas de escaneo de archivos y directorios, no deben cambiar o eliminar la configuración del software de antivirus en los equipos de cómputo propiedad de la empresa.
- Los usuarios no deben descargar archivos adjuntos que provengan de fuentes desconocidas, para evitar contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo o equipos portátiles.
- **Aplicaciones de Ofimática:** La suite de ofimática permitida por la empresa para equipos con sistema operativo Windows y Mac, son las versiones de Microsoft Office licenciadas por la empresa. Se permite el uso de la versión libre de Open Office, en los equipos de cómputo propiedad de la empresa.
- **Sistemas Propietarios Desarrollados por SOCIETE TSALACH** La instalación de productos de software desarrollados por el área de sistemas y tecnología de la empresa, se realizará en los equipos de cómputo propiedad de la sociedad designados para tal fin.
- **Acceso a Código Fuente de Aplicaciones:** Está prohibido manipular el código fuente de una aplicación sin la autorización correspondiente del área de sistemas y tecnología de la empresa, para generar cambios o mejoras a la misma. Si se requiere tener acceso al código fuente de una aplicación desarrollada en la empresa, se debe solicitar permiso al área de sistemas y tecnología. Si se trata de una aplicación desarrolla por un proveedor externo, se deben revisar las condiciones del contrato.
- **Monitoreo de Equipos: SOCIETE TSALACH** se reserva el derecho de monitorear los equipos de cómputo, conectados a la red de datos de la empresa, de los cuales se sospeche que están comprometiendo la confidencialidad, integridad y disponibilidad de la información.
- Los usuarios no pueden portar información de la empresa clasificada como privada sin la previa autorización del propietario del activo de información independiente del medio que utilice.
- La instalación de un nuevo componente en la red de datos debe estar autorizada por el área de sistemas y tecnología.
- La adopción y uso de tecnologías de la información y la comunicación orientadas a la gestión de servicios institucionales, serán aprobados por el área de sistemas y tecnología.

5.3. POLITICA DE ACCESO REMOTO.

La presente política contempla las comunicaciones electrónicas y conexiones remotas de usuarios autorizados para acceder a los servicios de la red de datos institucional.

- El Servicio de acceso remoto permite el acceso a la red de datos empresarial a aquellos usuarios externos e internos expresamente autorizados por el área de sistemas y tecnología con visto bueno de la gerencia general, para que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección.
- Solo Los equipos de procesamiento de datos tipo servidor y de comunicación tendrán habilitado el servicio de conexión de acceso remoto. Los clientes para acceder a estos recursos serán previamente identificados y autorizados.

5.4. POLITICA DE ESCRITORIO Y PANTALLA LIMPIOS.

Esta política se aplica a la protección de cualquier tipo de información, cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que se utiliza para apoyar la realización de las actividades laborales. El objetivo es reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo.

- Todas las estaciones de trabajo deben usar el papel tapiz empresarial o imagen corporativa y contar con bloqueo de sesión automática después de 2 minutos de inactividad, el cual, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña al ser reanudado.
- La información confidencial o sensible, cuando se imprime se debe retirar inmediatamente de las impresoras.
- Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo para proteger el acceso a las aplicaciones y servicios de la empresa de personal no autorizado.
- Los datos sensibles almacenados en los equipos o sistemas de información, deberán encontrarse ubicados en rutas que no sean de fácil acceso.
- Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, así mismo debe cerrar la sesión o salir de todas las aplicaciones correctamente y dejar los equipos apagados (no sólo el monitor).

5.5. POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO.

- Todas las personas que ingresen a la empresa, deben hacer uso del sistema de control de acceso implementado por el edificio donde se encuentran ubicadas nuestras oficinas.
- El área de sistemas y tecnología, debe elaborar un listado del personal que por el rol de sus funciones está autorizado para ingresar a sus oficinas.
- No se permiten las visitas al área de sistemas y tecnología a no ser que sea para llevar a cabo labores de mantenimiento o auditorias.
- Las puertas de acceso al área de sistemas y tecnología así como donde se encuentren los servidores y los centros de cableado deben permanecer siempre cerradas y aseguradas. De igual manera, todos los gabinetes y puertas de los equipos que se encuentran en estos lugares deben permanecer cerrados.

- Los funcionarios deben portar el carné que los identifica como empleados de la empresa, mientras permanezcan dentro de las oficinas.

5.6. POLITICA DE INSTALACION DE CABLEADO.

- **Instalación de Cableado Estructurado:** Planeación, diseño, construcción, instalación, administración y mantenimiento del cableado estructurado de telecomunicaciones de la empresa es responsabilidad del área de recursos humanos y sistemas y tecnología, por tanto deben cumplir con las normas técnicas o estándares adoptados por los mismos, con el fin de garantizar la integridad, conservar la estética y la seguridad de las redes.

5.7. POLITICA DE COPIAS DE RESPALDO.

- El área de sistemas y tecnología debe respaldar con copias de seguridad la información empresarial.
- El área de sistemas y tecnología debe garantizar copia de la información de configuración contenida en la plataforma tecnológica de la empresa como equipos tipo servidores, equipos activos de red y dispositivos de red inalámbricos.
- El área de sistemas y tecnología debe garantizar copia de los productos de software que administra
- Los medios magnéticos que tienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra ubicada. El sitio externo donde se resguardan dichas copias, solo tendrá acceso el área de sistemas y tecnología.
- Es responsabilidad exclusiva de los usuarios, la creación de copias de seguridad de archivos usados, custodiados o producidos por estos.

5.8. POLITICA DE INTERCAMBIO DE INFORMACIÓN.

- El intercambio de información manual, solo debe utilizar los servicios de correos autorizados en la empresa. De ser entregada por mano, debe ser entregada personalmente al destinatario y su entrega debe quedar registrada.
- Toda información enviada a través del correo institucional, debe incluir en su pie de página, una advertencia en cuanto a su uso y autorizaciones al respecto, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información.
- Todo intercambio de información a través de acceso remoto, debe cumplir con la Política de Acceso Remoto establecida en este manual **(5.3.)**
- El intercambio de información privada a o semiprivada por vía telefónica no está permitido.

5.9. POLITICA DE MANEJO DE INCIDENTES Y PETICIONES.

- Todos los incidentes y peticiones solicitados por los usuarios de la empresa deben ser canalizados a través del área de sistemas y tecnología.
- Toda la información relativa a los incidentes reportados, debe ser manejada con total confidencialidad.
- El área de sistemas y tecnología reportará ante la gerencia general los incidentes de seguridad que estén considerados como un delito informático para que sean conocidos por las autoridades que correspondan.

5.10. POLITICA DE GESTION DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

- La revisión del plan de continuidad de la seguridad de la información debe hacerse anualmente, dependiendo de los cambios y nuevos requerimientos en los procesos.
- El Data Center se debe proveer con unidades suplementarias de energía eléctrica (UPS) y se debe garantizar el óptimo funcionamiento de dichas unidades.
- Las copias de seguridad de los sistemas de computación que incluye sistema operativo, base de datos, aplicación, servicios, entre otros; deben ser almacenados en un lugar diferente de donde reside la información original, dentro de las instalaciones de la empresa.
- Debe realizarse mantenimiento preventivo y periódico a los equipos servidores, de comunicaciones y demás equipos en los cuales haya configurados servicios, de tal forma que el riesgo a fallas físicas se mantenga en una probabilidad de ocurrencia baja.

- Debe realizarse mantenimiento preventivo a intervalos programados a equipos de cómputo de los usuarios finales, propiedad de la empresa, para reducir el riesgo de falla.
- Los planes de continuidad deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la gerencia general.
- **SOCIETE TSALACH** gestiona y ejecuta los planes de capacitación para garantizar la formación y actualización de los funcionarios de la empresa.

5.11. POLITICA DE CUMPLIMIENTO.

- La gerencia general tiene la responsabilidad de identificar la legislación vigente que debe cumplir la empresa en función de la protección de la información y divulgar estos requerimientos. Además, debe servir de apoyo en la interpretación, asistencia y manejo de dicha legislación.
- Todos los funcionarios de la empresa deben cumplir con la normatividad vigente adoptada por la empresa, leyes de derechos de autor, acuerdos de licenciamiento de software y acuerdos de confidencialidad.

5.12. POLITICA DE CONTROL DE ACCESO.

- El control de acceso a todos los sistemas de información de la entidad y en general cualquier servicios de tecnologías de Información, debe realizarse por medio de credenciales de acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.
- El área de sistemas y tecnología con el visto bueno del área de recursos humanos será el responsable de la asignación y/o eliminación de credenciales de acceso de usuarios.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de la empresa debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y de la sociedad, que se definan por las diferentes áreas de la compañía, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por el área de sistemas y tecnología.

- La asignación de la contraseña para acceso a sistemas, se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.

- Los usuarios son responsables de todas las actividades llevadas a cabo con su identificación de usuario y contraseña.
- La contraseña inicialmente emitida por el administrador de sistema es válida solamente para la primera conexión del usuario, quien debe cambiarla antes de realizar cualquier actividad en el sistema.
- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

- Los usuarios deben tener en cuenta el siguiente lineamiento para la construcción de sus contraseñas: Debe estar compuesta de al menos ocho (8) caracteres. Estos caracteres deben ser caracteres alfabéticos, numéricos y símbolos o caracteres especiales.
- La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarla inmediatamente.
- El área de sistemas y tecnología debe implementar en las bases de datos un límite de intentos consecutivos infructuosos para ingresar la contraseña, el cual, corresponde a tres (3). Superado el tope se suspende el acceso del usuario hasta que el administrador de la base de datos active el usuario nuevamente.
- Cuando un usuario bloquee su cuenta debido a la superación del número máximo de intentos, debe reportarlo de forma inmediata al área de sistemas y tecnología, indicando a que sistema de información, para que se le active la cuenta y restaure su contraseña.
- La activación de la cuenta y obtención de acceso a la contraseña debe hacerse de forma segura.
- Las contraseñas no se deben incorporar dentro de los productos de software, esto para garantizar que las contraseñas se puedan cambiar en el momento que sea necesario.
- Se debe hacer el cambio de las contraseñas proporcionadas por el fabricante (contraseñas por defecto) antes de poner en producción cualquier activo de información en la empresa.

5.13. POLITICA DE USO DE CONTROLES CRIPTOGRAFICOS.

- La empresa establece la presente política de uso de controles criptográficos, a fin de determinar su correcto uso.
- Se utilizarán controles criptográficos en los siguientes casos: Para el resguardo de información, que sea clasificada como confidencial y la que surja de la evaluación de riesgos realizada por el propietario de la Información y el Comité de Seguridad de la Información **(4.3.)**.
- Para el almacenamiento de las contraseñas de los sistemas operativos, gestión de identidad y bases de datos.
- Se definirá el uso de un software para realizar la encripción de la información en los equipos de cómputo.

5.14. POLITICA DE GESTION DE LLAVES.

- Las llaves criptográficas utilizadas para el cifrado de los datos deben estar clasificadas como confidencial y ser protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.
- Para reducir la probabilidad de compromiso, las llaves tendrán fechas de inicio y caducidad de vigencia.

5.15. POLITICA DE DISPOSITIVOS MÓVILES.

- Las características en las capacidades de los equipos serán definidos en función de la importancia de la información procesada o almacenada en cada tipo de usuario que utiliza un dispositivo móvil de la empresa.

- Todos los usuarios de dispositivos móviles que contengan información confidencial o de Uso Interno deben usar la última o la más segura versión de los productos de software. Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Los usuarios de dispositivos móviles deben mantener actualizado el software antivirus del dispositivo.

5.16. POLITICA DE GESTION DE MEDIOS REMOVIBLES.

Esta política define las reglas para la protección de datos en diferentes medios de almacenamiento removible (USB, discos, etc); considerando su administración, protección y traslado. Todos los medios removibles que contengan información sensible o confidencial serán almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante y los niveles de clasificación de la información.

- Los medios removibles NO son alternativa de respaldo de información permanente, siendo responsabilidad de los usuarios mantener la información en los servidores, servicios en la nube o equipos destinados para ello.
- Los medios removibles deben ser escaneados cada vez que sea conectado a un equipo de la red de la empresa, especialmente en lo concerniente a posible código malicioso.
- El funcionario debe dar buen uso a los medios removibles asignados, informando oportunamente cualquier deterioro.
- No se debe almacenar información confidencial en los teléfonos móviles.
- Una vez asignado el medio removible al usuario, es de su exclusiva responsabilidad tomar las medidas adecuadas para el almacenamiento y custodia necesarios de la información, para protegerla de accesos no autorizados, daño o pérdida.

5.17. POLITICA DE DESARROLLO SEGURO.

- Para apoyar los procesos operativos, comerciales y estratégicos la empresa debe hacer uso intensivo de las tecnologías de la información y las comunicaciones. Los productos de

software pueden ser adquiridos a través de terceras partes o desarrollado por personal propio.

- El área de sistemas y tecnología debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.

5.18. PROHIBICIONES.

- Queda prohibida la ejecución de cualquier herramienta o mecanismo de monitoreo de la red de manera no autorizada, así como evadir los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación servidor o cuenta de usuario, están restringidos.
- Está prohibido utilizar la infraestructura de tecnología de información y redes de la empresa, para conseguir o transmitir material con ánimo de lucro.
- Está prohibida la utilización de la infraestructura de tecnología de información y redes de la compañía para hacer algún tipo de acoso, difamación calumnia o cualquier forma de actividad hostil en contra de cualquier persona o institución.

- Queda prohibida la instalación de puntos de acceso inalámbricos no autorizados en la empresa.
- La tecnología de información que provee la empresa es para el desarrollo de los procesos propios. Por lo tanto, no está permitido el uso con fines personales de estos recursos.
- No se exime a los usuarios de la responsabilidad disciplinaria y legal correspondiente de toda aquella acción que no esté aquí documentada y pueda afectar la seguridad de la información de **SOCIETE TSALACH**

6. ALCANCE DE LAS POLÍTICAS ENUNCIADAS

Las presentes Políticas de Seguridad de la Información se dictan en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la **SOCIETE TSALACH**

La Política de Confidencialidad de la Información de la Compañía, establece los diferentes tipos de información que se maneja, el uso aceptable que debe hacerse de esta información, los principios de retención y divulgación de los datos confidenciales, los deberes de la empresa y los derechos de los(as) colaboradores(as) y contratistas y las medidas de seguridad adoptadas para garantizar la protección de esta información.

7. CUMPLIMIENTO

El cumplimiento de todas las leyes, regulaciones, estándares profesionales, políticas aplicables, la presente política y todos los contratos, es responsabilidad de los(as) colaboradores(as) de la Compañía, de los contratistas y de los Terceros.

8. EXCEPCIONES

En caso de existir situaciones en algún área de **SOCIETE TSALACH** que impidan cumplir con la política de forma parcial o total, debe el responsable del cumplimiento, exponerlo ante el Comité de Seguridad Informática, argumentando las razones; dicho Comité tiene la facultad de aprobar o no la solicitud y debe dejar la evidencia y documentarla para posterior revisión.

9. APLICABILIDAD

La Política de Seguridad de la Información de la empresa, aplica a todo el personal vinculado laboralmente, contratistas y terceros que tengan acceso a los recursos de su información. Estas políticas deben ser compartidas, entendidas y acatadas por los anteriormente mencionados, siendo deber de éstos, expresar sus dudas oportunamente y de buena fe a los funcionarios administradores de la información. Cabe anotar que su aplicación y cumplimiento es de carácter obligatorio para todo el personal de la compañía, cualquiera que sea la situación que revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

10. RESPONSABILIDAD

10.1. DIRECTIVOS DE LA COMPAÑÍA.

- Implementar la Política de Seguridad de la Información dentro de sus áreas y velar por su cumplimiento por parte de su equipo de trabajo.

10.2. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

- El Comité representa el compromiso de la Gerencia General con la Seguridad de la Información y es el canal entre ésta y los(as) colaboradores(as).
- Revisar y proponer a la máxima autoridad de la Compañía para su aprobación, la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Garantizar que la seguridad de la información sea parte del proceso de planificación de la empresa.
- Promover la difusión y apoyo a la seguridad de la información dentro de la empresa.
- Coordinar el proceso de administración de la continuidad de las actividades de la sociedad.

10.3. COORDINADOR DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

(RESPONSABLE DEL ÁREA DEL SERVICIO AL CLIENTE)

- Coordinar las acciones del Comité de Seguridad de la Información.
- Impulsar la implementación y cumplimiento de la presente Política.
- Mantener la Política de Seguridad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Coordinar la logística correspondiente a las sesiones del comité de seguridad de la información.
- Recepcionar, revisar, preparar y presentar ante el comité de seguridad de la información las propuestas que requieran ser aprobadas.

10.4. RESPONSABLE DE SEGURIDAD INFORMÁTICA.

(RESPONSABLE DEL ÁREA DE SISTEMAS Y TECNOLOGÍA)

- Cumplir funciones relativas a la seguridad de los sistemas de información de la empresa, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

10.5. PROPIETARIOS DE LA INFORMACIÓN.

(GERENCIA GENERAL - RESPONSABLE DEL ÁREA DEL SERVICIO AL CLIENTE – RESPONSABLE DE RECURSOS HUMANOS – RESPONSABLE DE CONTABILIDAD – RESPONSABLE DEL ÁREA DE SISTEMAS Y TECNOLOGÍA - DIRECTOR COMERCIAL - RESPONSABLE DE TESORERÍA)

- Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.
- Documentar y mantener actualizada la clasificación efectuada.
- Definir los criterios de acceso a la información de acuerdo a sus funciones y competencia para sus colaboradores(as).
- Asegurar que los controles de alto nivel para proteger la información sean implementados.
- Tomar las acciones definidas en las políticas, código de ética y cualquier otro reglamento o control, frente a violaciones de la seguridad.

10.6. RESPONSABLE DEL ÁREA DE TALENTO HUMANO.

- Notificar al personal que ingresa a la empresa, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Socializar a toda la compañía los cambios que se realicen en la política de seguridad de la información, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación permanente en materia de seguridad.
- Incluir las funciones relativas a la seguridad de la información en la descripción de puestos de los(as) colaboradores(as).

10.7. RESPONSABLE DEL ÁREA DE SISTEMAS Y TECNOLOGÍA.

- Cumplir la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la empresa
- Efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

10.8. USUARIOS DE LA INFORMACIÓN Y LOS SISTEMAS UTILIZADOS PARA SU PROCESAMIENTO.

- Los usuarios incluyen a todo el personal vinculado laboralmente con **SOCIETE TSALACH**, contratistas y terceros cuyas labores diarias comprenden el procesamiento, resguardo o transmisión de la información privada, confidencial, interna o pública de la empresa.
- Conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.
- Aceptar, comprender y aplicar las políticas, estándares y controles técnicos de seguridad de la información de la empresa.
- Usar la información y recursos de forma ética y responsable, para los propósitos autorizados únicamente.

10.9. UNIDAD DE AUDITORÍA INTERNA.

- Quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

10.10. CUSTODIOS DE LA INFORMACIÓN.

(ÁREA DE SISTEMAS Y TECNOLOGÍA)

- Implementar (a nivel técnico) los controles requeridos para proteger los activos de información, con base en el nivel de clasificación asignado por el administrador correspondiente.
- Proporcionar asistencia en la selección de soluciones técnicas apropiadas.
- Proveer operativamente el aseguramiento de la información.

10.11. ASESOR DE SEGURIDAD DE LA INFORMACIÓN.

(RESPONSABLE ÁREA DE SISTEMAS Y TECNOLOGÍA)

- Asesorar a la empresa en Seguridad de la información: o Dar los lineamientos relacionados a la seguridad de la información sujetos a las mejores prácticas.

- Diseñar y adaptar políticas enfocadas en las mejores prácticas de la seguridad de la información.
- Asesorar en el diseño y preparación de los planes de trabajo como respuesta a las recomendaciones planteadas por las auditorías a la Compañía.

- Realizar periódicamente monitoreos que permitan diagnosticar el estado de seguridad de la información.

LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO TIENE UN NIVEL DE CONFIDENCIALIDAD INTERNA DE SOCIETE TSALACH, LA UTILIZACIÓN O DIFUSIÓN NO AUTORIZADA DE ESTA INFORMACIÓN ESTÁ PROHIBIDA POR LA LEY.

En el presente documento aparecen los(as) colaboradores(as) que participaron en la revisión y aprobación del documento, los cuales hacen constar que recibieron documentación e información previa para tal efecto y que el documento está adecuado a las actividades y prácticas de **SOCIETE TSALACH**

GERENTE GENERAL

RESPONSABLE DEL ÁREA DE SERVICIO AL CLIENTES

RESPONSABLE DEL ÁREA DE RECURSOS HUMANOS

RESPONSABLE DE CONTABILIDAD

RESPONSABLE DEL ÁREA DE SISTEMAS Y TECNOLOGÍA

DIRECTOR COMERCIAL

RESPONSABLE DE TESORERÍA

Última actualización del documento: Diciembre de 2019.