Tabla de contenido

PRESENTACIÓN DEL MANUAL

La dirección de World Travel Assist, entendiendo la importancia de una adecuada gestión de su información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, buscando adoptar un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes, normativa internacional ISO NTC IEC 27001: 2013 y en concordancia con la misión y visión de la entidad.

Para World Travel Assist, la protección de la información busca la disminución de los riesgos generados sobresus activos, identificándose de manera sistemática, con objeto de mantener un nivel de exposición que permita conservar la integridad, confidencialidad y la disponibilidad de la misma, acorde a las necesidades delos diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que, los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSIestarán determinadas por las siguientes premisas:

- Minimizar el riesgo en todas las funciones de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Protegerlos activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices,practicantes y clientes de World Travel Assist.
- Garantizar la continuidad del negocio frente a incidentes.

World Travel Assist ha decidido definir, implementar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros, en concordancia con las necesidades del negocio y los requerimientos regulatorios.
A continuación, se establecen 12 principios de seguridad que soportan el SGSI de World Travel Assist:

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas yaceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• World Travel Assist protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• World Travel Assist protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• World Travel Assist protegerá su información de las amenazas originadas por parte del personal.

• World Travel Assist protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• World Travel Assist controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• World Travel Assist implementará control de acceso a la información, sistemas y recursos de red.

• World Travel Assist garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas deinformación.

• World Travel Assist garantizará a través de una adecuada gestión de los eventos de seguridad y lasdebilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• World Travel Assist garantizará la disponibilidad de sus procesos de negocio y la continuidad de suoperación basada en el impacto que pueden generar los eventos.

• World Travel Assist garantizará el cumplimiento de las obligaciones legales, regulatorias y contractualesestablecidas.

NOTA: Estas políticas se revisarán y actualizarán si es necesario de manera semestral o antes en caso detener una eventualidad que lo amerite.

1. OBJETIVO

El propósito del presente manual es definir un marco de referencia para el desarrollo del sistema de gestiónde seguridad de la información, con el fin de proteger esta y sus activos contra su uso no autorizado, divulgación o revelación, modificación, daño o pérdida y para asegurar el cumplimiento de regulaciones y leyes aplicables a WORLD TRAVEL ASSIST LATAM S.A.S.

2. ALCANCE DE LA POLÍTICA DE SEGURIDAD EN LA INFORMACIÓN

La presente política es aplicable en los procesos descritos en el mapa de procesos de World Travel Assist Latam SAS, los cuales deberán cumplir este requisito sin perjuicio de tener políticas adicionales o más restrictivas, en pro de mejorar la seguridad de la información. El alcance de la presente política también abarca proveedores, clientes, terceros y en sí todas las partes interesadas.

Cada uno de los procesos de la organización desarrollará esta política en sus actividades y deberán reportar su adecuación al proceso de mejora para la monitorización del sistema de gestión de seguridad de la información.

La política deberá estar disponible en la página web corporativa de WTA https://wtabyhas.com/, así como en un repositorio común de la compañía y divulgada en las instalaciones de la organización.

3. DEFINICIONES

Activo: Según [ISO IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria pararealizar los procesos misionales y operativos del DAPRE. Se pueden clasificar de la siguiente manera:

Acuerdo de Confidencialidad: es un documento en los que los funcionarios de WORLD TRAVEL ASSIST LATAM S.A.S o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tenga acceso en virtud de la labor que desarrollan

dentro de la misma.

Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SIGEPRE.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de unsujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el DAPRE. Ejemplo: archivo de Word “listado de personal.docx”.

Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Pagaduría.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Personal: Es todo el personal del DAPRE, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del DAPRE. Ejemplo: Pedro Pérez.

Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Plan de continuidad del negocio (Business Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Seguridad de la información: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad ydisponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO IEC 27001: 2013]: Sistema global degestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones. MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Proceso asociado Código Versión Tecnologías de Información y Comunicaciones M-TI-01 10 6 Ejemplo: equipo de cómputo, teléfonos, impresoras.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos y a quienes se les otorga un nombre de usuario y una clave de acceso.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmentepermite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

"World Travel Assist proporciona los recursos necesarios para establecer y operar un sistema de gestión de seguridad en la información que establece los lineamientos para asegurar la confidencialidad, integridad y disponibilidad de la información corporativa y de todas las partes interesadas, ubicada en los sistemas de información y software que almacenan, procesan y transmiten información de todos nuestros procesos, cumpliendo con los requisitos y expectativas de nuestros clientes. El sistema tiene como propósito la protección de la información a través de la implementación y evaluación de eficacia de planes de tratamiento, acciones y mantenimiento de controles físicos, organizacionales, de personas y tecnológicos y establece para ello los siguientes objetivos:

- *Disminuir los riesgos a los cuales están expuestos los activos de información*
- *Establecer una cultura de seguridad de la información en la compañía*
- *Garantizar el cumplimiento de los requisitos, legales, contractuales y del negocio vigentes*
- *Adoptar los lineamientos de seguridad en la información estipulados en el presente documento*
- *Establecer acciones disciplinarias y o legales, frente al incumplimiento de dichas políticas"*

5. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

WORLD TRAVEL ASSIST LATAM S.A.S ha definido las siguientes las condiciones para el manejo de los dispositivos móviles (teléfonos inteligentes, tabletas, entre otros) de índole institucional y personal:

La compañía suministra los dispositivos móviles con fines exclusivamente empresariales para cada proceso de la compañía, dotados de los recursos necesarios como plan de datos y minutos para el cumplimiento de las respectivas funciones.

La compañía velará porque los funcionarios hagan un uso responsable de los equipos proporcionados,conforme a lo establecido en la DC-MPR-018 POLÍTICA DE LINEAS Y EQUIPOS CELULARES CORPORATIVOS**.** Estas revisiones de buen uso están a cargo del oficial de seguridad de la información de acuerdo a la programación de revisiones dejando evidencia de los hallazgos en el formato FO-MPR-020 REGISTROS DE LLAMADO DE ATENCIÓN
La gerencia establece el siguiente listado de personal con autorización de uso de equipos móviles personales al interior de la organización:

Proceso	Nombre de director autorizado
Gerencia general	Sabrina Morales
Mejora de procesos	Carolina Jaramillo
Contabilidad	Carolina León
Fidelización de clientes	Mariana Vega
Recursos humanos	Paula Cocomá
Claims	Erika Rengifo
Calidad	Luisa Mejía
TPA y reportes de seguros	Felipe Navarrete
Tecnología	Andrés Ramírez
Proveedores	Andrés Mejía
Seguridad y salud en el trabajo	Vanessa Restrepo
Reembolsos	Catalina Moribe
Operaciones	Julio Carvajal
Departamento médico	David Ñañez

Capacitación y entrenamiento	Steven Castaño
Desarrollos digitales	Arturo Álvarez

6. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Dirección de Tecnología de WORLD TRAVEL ASSIST LATAM S.A.S, como responsable de las redes de datos ylos recursos de red de la compañía, ha empleado diversos mecanismos de control de acceso lógico, con el fin de que las mismas se encuentren protegidas contra cualquier acceso no autorizado.

Las redes inalámbricas de la compañía cuentan con métodos de autenticación que evitan accesos no autorizados, entre ellos el uso del firewall y del documento HOST con dominios enlistados a los cuales se encuentra restringido el acceso. Adicionalmente, el uso de la plataforma KASPERSKY y los bloqueos que la misma maneja, la descripción detallada del procedimiento de administración de redes se encuentra en el documento DC-ITS-003 ADMINISTRACIÓN DE REDES Y PLATAFORMAS TECNOLOGICAS

Los equipos de cómputo que deseen conectarse a las redes de datos de la empresa, deberán cumplir con todos los requisitos y/o controles para autenticarse en ellas (Credenciales de usuario), relacionados en el procedimiento PR-ITS-009 CONFIGURACIÓN DE EQUIPOS PARA USO EMPRESARIAL y únicamente podrán realizar las funciones para las que fueron autorizados.

La conexión de terceros o visitantes a las redes de la compañía se realizará acorde a lo establecido en el procedimiento PR-ITS-012 PROCEDIMIENTO PARA INGRESO A LA RED DE WTA POR PARTE DE TERCEROS.

Los sitios web de ocio que no corresponden a las actividades laborales de la compañía se encuentran restringidos, sin embargo, se cuenta con una red con conexión a portal cautivo (red GUEST), separada de la IP pública empresarial, que permite el acceso a estos sitios con fines lúdicos y únicamente en el tiempo que no se esté laborando (Horas de almuerzo y respectivos tiempos de descanso).

7. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

WORLD TRAVEL ASSIST LATAM S.A.S ha determinado privilegios para el control de acceso lógico de cada usuario o grupo de usuarios sobre los recursos tecnológicos y los sistemas de información de la empresa. Garantizando que los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores.

La Dirección de Tecnología ha establecido el procedimiento PR-ITS-016 CREACIÓN, MODIFICACIÓN Y DESACTIVACIÓN DE CUENTAS DE USUARIO que contempla la creación, modificación, bloqueo o eliminación de las cuentas de usuario, para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la compañía, estas gestiones deberán realizarse de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, son ascendidos o reubicados.

8. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

El propósito de esta política es delimitar el acceso y uso aceptable de todo el equipamiento computacional, servicios y sistemas de información, así como de las redes de datos de WORLD TRAVEL ASSIST LATAM S.A.S. Estas reglas están orientadas a proteger a los colaboradores y a la organización sobre el uso inapropiado de la información, los servicios de red y equipos informáticos. La compañía motivará estas acciones concientizando e informando al personal de forma continua, de acuerdo al plan de capacitación constante del SGSI, evidenciado en documento FO-MPR-022 PLANIFICACIÓN DEL SISTEMA DE SEGURIDAD EN LA INFORMACIÓN 2024.

Todos los colaboradores, incluso terceros, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la organización. La asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos, para determinar el permiso a los activos de información la alta dirección determina en la DC-MPR-010 MATRIZ DE INVENTARIO Y CLASIFICACION DE ACTIVOS DE INFORMACIÓN la categorización por confidencialidad que especifican los permisos de uso que tiene cada activo y a cuál tiene

autorización de acceso cada proceso o cargo.

Sólo se pueden conceder accesos a externos a la institución, previa autorización del dueño del medio de procesamiento de información y el dueño de la información. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración, el que debe ser controlado por el Proceso de Tecnología y líder del proceso según corresponda.

Los colaboradores deben hacerse responsables del usuario y contraseña asignados para su acceso a los sistemas de información WTAOPS y Communicator, bajo ningún motivo podrán compartir esta información con otros funcionarios o terceros. Con respecto al accesos a los medios de comunicación Skype y cuentas de Gmail, los usuarios podrán acceder a través del proceso de tecnología, quienes serán los responsables de establecer las contraseñas en cada equipo. Las causales de la falta esta responsabilidad está establecidas en DC-MPR-016 ANEXO FALTAS SEGURIDAD EN LA INFORMACION.

Nota: Esta política se amplía en la DC-MPR-013 POLÍTICA DE CONTROL DE ACCESO establecida por la alta gerencia.

9. POLÍTICA DE USO DE CONTRASEÑAS EN WORLD TRAVEL ASSIST

Contraseñas personales:

La organización establece que para los sistemas de información WTAOPS y Communicator las contraseñas iniciales son establecidas por el proveedor, sin embargo, al primer ingreso el usuario debe realizar el cambio de contraseña cumpliendo con la política y acciones para construir contraseñas seguras que se menciona abajo.

Toda contraseña para el ingreso al sistema operativo WTAOPS y al sistema Communicator de la empresa es personal e intransferible, cada colaborador es responsable de la misma, y debe velar por que sus contraseñas no sean vistas o aprendidas por otros colaboradores.

Política y acciones para construir contraseñas seguras:

1. Se deben utilizar al menos 8 caracteres para crear la clave.
2. Se recomienda utilizar en una misma contraseña dígitos, letras y caracteres especiales.
3. Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas. Hay que tener presente el recordar qué letras van en mayúscula y cuáles en minúscula.
4. Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse

rápidamente, preferiblemente, sin que sea necesario mirar el teclado.

5. Las contraseñas hay que cambiarlas con una cierta regularidad, el sistema operativo exige cambio de clave cada 3 meses.
6. Utilizar signos de puntuación si el sistema lo permite. P. ej.: “Tr-.3Fre”. En este caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, dentro de ese consejo se incluiría utilizar símbolos como: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Acciones que deben evitarse en la gestión de contraseñas seguras:

1. Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios. Por ejemplo, debe existir una contraseña para el WTAOPS y una contraseña diferente para el Communicator por usuario.
2. No utilizar información personal en la contraseña: nombre del usuario o de sus familiares, ni sus apellidos, ni su fecha de nacimiento. Y, por supuesto, en ninguna ocasión utilizar datos como el número de identificación o número de teléfono.
3. Hay que evitar utilizar secuencias básicas de teclado (por ejemplo:” qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)
4. No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).
5. Hay que evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
6. No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.
7. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.).
8. No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma. Tampoco se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador),
9. No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. Hoy en día existen programas de ruptura de claves que basan su ataque en probar una a una las palabras que extraen de diccionarios: Este método de ataque es conocido como “ataque por diccionario”.
10. No enviar nunca la contraseña por correo electrónico o en un sms. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
11. No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
12. Cambiar las contraseñas por defecto proporcionadas por desarrolladores (WTAOPS y

Communicator).

Contraseñas de uso compartido gestionadas por tecnología:

Teniendo en cuenta que la información es un activo de alta importancia para la organización, la alta dirección establece que las contraseñas de los medios de comunicación interna como Skype y correos electrónicos de gmail, deben ser creadas, gestionadas y controladas por el proceso de Tecnología, con el fin de evitar daños y perjuicios por el uso malintencionado de los colaboradores. Esta determinación es considerada puesto que los otros sistemas de información como WTAOPS y Communicator generan controles seguros que evitan fuga o pérdida de información.

Ningún colaborador de la organización cuenta con autorización para realizar cambios de claves o contraseñas de Skype o cuentas de Gmail, en caso de ser necesario, deberá solicitar el cambio a través del líder del proceso quien deberá transmitir la solicitud al proceso de tecnología.

Los medios de comunicación que la organización dispone a los colaboradores son para uso estrictamente laboral, siendo así, la divulgación de cualquier información de carácter personal es responsabilidad del colaborador y no acarreará sanciones para la organización, por lo mismo, la alta dirección establece que en caso de necesidad el proceso de tecnología tiene la autoridad de realizar revisiones o verificaciones de la información transmitida por Skype o cuentas Gmail con previa solicitud del líder del proceso o de la gerencia.

Herramientas y soluciones informáticas:

Con el objetivo de cumplir con la política y acciones para construir contraseñas seguras, la herramienta utilizada por nuestro proceso de tecnología para la creación de las mismas es: https://www.lastpass.com/es/features/password-generator#generatorTool

La organización establece los siguientes controles para la gestión de las contraseñas:

1. Frecuencia de cambio de claves: Cada 3 meses
2. Encargado de creación y actualización de claves: Analista de tecnología
3. Control de contraseñas diferentes para Skype y cuentas Gmail
4. Las contraseñas quedarán guardadas en cada equipo solo por parte del proceso de tecnología, cualquier necesidad o solicitud que requiera el uso de contraseñas se solicitará la intervención a tecnología.
5. Tecnología efectuará revisiones de contraseñas aleatorias por cada proceso de manera mensual, dejando registro en el CRM de tecnología.

10. POLÍTICA DE SEGURIDAD Y MANTENIMIENTO PARA LOS EQUIPOS INSTITUCIONALES

Para evitar la pérdida, alteración o daño de los recursos tecnológicos de la compañía, la Dirección deTecnología de WORLD TRAVEL ASSIST LATAM S.A.S ha determinado los siguientes mecanismos y estrategias para proteger su integridad, dentro y fuera de las instalaciones:

Generación de actas de entrega con firma de responsabilidad por parte del usuario final del equipo y del líderdel proceso correspondiente. FO-ITS-016 ACTA DE ENTREGA Y RECIBO DE EQUIPOS DE CÓMPUTO O HERRAMIENTAS DE TRABAJO.

Configuración inicial del equipo, conforme a lo establecido en el procedimiento PR-ITS-009 CONFIGURACIÓN DE EQUIPOS PARA USO EMPRESARIAL, respecto aconfiguración de contraseñas y credenciales de acceso.

La Dirección de Tecnología realizará mantenimientos preventivos y correctivos de los equipos de cómputo y dispositivos móviles de la compañía de acuerdo a lo establecido en el procedimiento PR-ITS-001 MANTENIMIENTO PREVENTIVO DE EQUIPOS E INFRAESTRUCTURA TECNOLOGICA.

La Dirección de Tecnología es la única autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la compañía.

Cuando se presente una falla o problema de hardware/software en una estación de trabajo u otro recurso tecnológico, el usuario responsable debe informar al proceso de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

11. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

WORLD TRAVEL ASSIST LATAM S.A.S protegerá los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información. Como responsable de los datos personales obtenidos a través de sus distintos canales de atención, la compañía ha establecido los términos y condiciones que empleará para el tratamiento de la información de

todas las personas que, en algún momento, por razones de la actividad que desarrolla la empresa, hayan suministrado datos personales, velando porque dicha información almacenada en bases de datos o cualquier otro almacenamiento:

- Sea utilizada únicamente para funciones propias de la empresa, de acuerdo a la legislación nacional vigente Ley 1581 del 2012.
- No sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.
- No sea divulgada, alterada o eliminada sin la autorización requerida.

Las áreas que procesan datos personales de los beneficiarios o usuarios finales deben obtener la autorización para el tratamiento de estos datos (Record Release Form firmada) con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la compañía.

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima, es decir, información necesaria para el desarrollo de las actividades laborales, puedan tener acceso a dichos datos. Para lo anterior, se dispone de las siguientes herramientas de almacenamiento seguro de la información:

- Sistema operativo WTAOPS: información de clientes, usuarios finales
- Unidades de almacenamiento en red locales (compartidas seguras): información de funcionarios, documentación interna de procesos, proveedores

A dichas unidades (compartidas seguras) solo tienen acceso los colaboradores propios del proceso y de esta manera ningún otro interfiere en la información, con respecto a los datos de los clientes, estos se manejan directamente y de manera segura en los servidores de nuestro sistema de información.

La organización determina la DC-MPR-022 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES, con el fin de garantizar el cumplimiento de la ley 1581 del 2022.

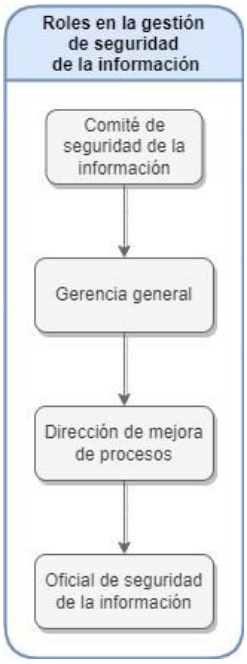
12.POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

La gerencia de la compañía, en cumplimiento al compromiso del Sistema de Gestión de

Seguridad de la Información se ha comprometido a la asignación de recursos necesarios para el desarrollo y cumplimiento del Sistema de Gestión de Seguridad en la información. De igual manera ha definido y establecido roles y responsabilidades que involucran las actividades de operación, gestión y administración de la seguridad de la información, así como la existencia del Comité de Seguridad de la Información definida en su respectiva acta de conformación.

Adicionalmente, la gerencia también designa a todos los directores de procesos como responsables del cumplimiento de actividades y políticas propias del sistema al interior de su área, así mismo reportar cualquier incidencia al oficial de seguridad de la información para su respectivo plan de acción.

Los funcionarios responsables designados por la dirección son:



Cargo	Nombre	Responsabilidades	Rol / Función
Dirección de mejora de procesos	Carolina Jaramillo López	• Notificar de manera oportuna los cambios y mejoras realizados en su proceso que	• Creación de estrategias que conlleven al cumplimiento de los

		impacten los sistemas de gestión • Participar de manera activa de los procesos de auditoría interna de la organización • Tomar acciones de manera oportuna frente a las no conformidades identificadas en los procesos de auditoría interna de los sistemas de gestión • Actualizar la documentación de su proceso frente al sistema de gestión • Dirigir la implementación y operación del Sistema de seguridad de la información. (SGSI) • Cumplir con la política general de Seguridad de la información y las normas definidas para dar cumplimiento el Sistema de seguridad de la información. (SGSI) • Cumplir con las capacitaciones de seguridad en la información	objetivos definidos • Creación de estrategias que incrementen la productividad y la optimización de los recursos • Gestionar los riesgos empresariales y de seguridad de la información que permita establecer una matriz de análisis de riesgos con su tratamiento. • Coordinar actividades y acciones de auditoría interna en seguridad de la información. • Coordinación conjunta con otros procesos de la aplicación de controles organizaciones y controles de seguridad de la información. • Revisar y evaluar los indicadores de gestión correspondientes a la atención de incidentes de seguridad para ser presentados a la alta dirección

Oficial de seguridad de la información	Brayan Moncada Hincapié	• Mantener una política de seguridad integral • Desarrollo, ejecución y supervisión de las estrategias de seguridad de la información • Gestión, manejo y vigilancia del control de acceso a la información de la compañía • Potenciar la cultura de seguridad de la información • Dar buen uso y manejo a las herramientas y equipos designados por la organización para el desempeño de sus funciones. • Cumplir las normas de Seguridad y Salud en el Trabajo y reglamentos propios de la empresa. • Estar informado de las novedades del sector y mantener una constante actualización de conocimientos para dar una respuesta flexible y ágil a cualquier incidente cibernético que afecte	• Implementar y verificar el cumplimiento del sistema de gestión de seguridad. • Verificar el cumplimiento de las políticas de seguridad por parte de todos los colaboradores • Supervisar los incidentes relativos a la seguridad • Garantizar la máxima protección y privacidad de los datos e informaciones corporativa • Estar a cargo de la planificación de respuesta de incidentes, así como la investigación de vulneración de la seguridad • Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios. • Efectuar planes de capacitación del sistema de seguridad

		a la empresa Implementar y hacer seguimiento al plan de capacitación del sistema de seguridad en la información	en la información

Comité de seguridad de la información		
Proceso	**Nombre**	**Rol / Función**
Recursos Humanos	Cesar Lopez	• Apoyar la implementación y operación del Sistema de seguridad de la información. (SGSI) • Verificar el cumplimiento de las políticas de seguridad en la información, al interior de cada proceso • Transmitir toda la información relacionada con el SGSI, al interior de cada proceso • Exponer o compartir, posibles nuevos riesgos relacionados con la seguridad en la información
Proveedores	Christian Rodas	
Calidad	Valentina Correa-Dana Ramos	
SG-SST	Sara Agudelo	
Customer	Paulina Jaramillo	
Médico	Manuel Ramirez	
Capacitación	Manuel Cuyato	
Reembolsos	Juan Manuel Betancurt	
Contabilidad	Laura Sánchez	
TPA	Jacobo Herrera	
Operaciones	Angela Gañan	

Usuarios:

Los usuarios de SGSI son todos los colaboradores de la organización y tienen las siguientes responsabilidades:

- Cumplir con las políticas de seguridad de la información
- Reportar incidentes de seguridad que atenten contra la confidencialidad, integridad o disponibilidad de la información o evidencien un incumplimiento de las políticas
- Participar activamente de todas las campañas de sensibilización y capacitación del sistema

- Apoyar el desarrollo de las auditorías internas y externas al sistema

Nota: Se relaciona con esta política el ACTA DE CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN y el MN-MPR-002 MANUAL DE FUNCIONES DE OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Gestión de desviaciones y exclusiones del sistema de seguridad de la información:

La gerencia efectúa análisis y revisión de los controles del anexo A de la NTC ISO 27001:2022 y dando cumplimiento a los controles organizacionales aplicables en función de las actividades de la organización genera el documento DC-MPR-017 DECLARACION DE APLICABILIDAD para el manejo de desviaciones y exclusiones.

13. POLÍTICA DE RELACIONES CON LOS PROVEEDORES

Conscientes de la importancia de mantener la seguridad de la información y de los servicios de procesamiento de información a los cuales tienen acceso terceras partes o entidades externas, la compañía ha establecido los siguientes mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información o servicios a la que tengan acceso o que sean provistos por los proveedores o contratistas, cumplan con los estándares de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido en los contratos o acuerdos con los proveedores y/o contratistas se ha incluido una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información. Esta información se maneja de acuerdo al procedimiento PR-RSC-002 Selección, evaluación y reevaluación de proveedores

Para lo anterior la Organización determina la siguiente DC-MPR-020 POLITICA DE RELACIÓN CON PROVEEDORES donde se establecen los lineamientos de seguridad de la información necesarios.

14. POLÍTICA DE ESCRITORIO LIMPIO Y BLOQUEO DE PANTALLAS

La compañía ha definido la presente política con el objetivo de prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral:

- Todos los escritorios deben permanecer despejados y libres de documentos físicos o medios extraíbles que contengan información sensible, restringida o confidencial, a excepción de los procesos Recursos humanos, Contabilidad y Seguridad y salud en el trabajo, ya que, de acuerdo a la naturaleza de sus labores, requieren manejar información en medio físico. Los informes impresos que contienen información sensible, restringida o confidencial deben ser retirados inmediatamente de las impresoras, deben ser almacenados o en su defecto eliminados de forma inmediata.

- Solo los equipos de los procesos de recursos humanos, seguridad y salud en el trabajo y contabilidad tienen autorización para tener configurado el uso de impresora, fotocopiadoras o escáneres. En caso de que otros procesos requieran estos servicios deben solicitarlo a través de recursos humanos.

- La información confidencial que se encuentre de forma física debe estar guardado en oficinas con llave.

- Todos los computadores deben ser bloqueados cuando el puesto de trabajo esté desocupado o desatendido mediante las teclas Windows + L. El proceso de Tecnología es responsable de la configuración de inactividad de los equipos, se establece que después de un minuto de inactividad el computador debe quedar bloqueado.

- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias descritas en el procedimiento PR-ITS-009 CONFIGURACIÓN DE EQUIPOS PARA USO EMPRESARIAL.

- Esta completamente prohibido el consumo de comida en los puestos de trabajo

15. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Se ha implementado el programa de seguridad física para el acceso a las instalaciones, lo cual permite fortalecer la confidencialidad, disponibilidad e integridad de la información, a través de controles de acceso y monitoreo en áreas de oficina e instalaciones donde reside información restringida o confidencial o activos tecnológicos de valor, explícitamente las áreas que representan mayor riesgo de vulneración o acceso a la información no autorizado son: Tecnología (cuarto de servidores o data center, oficina de tecnología y dirección), cuarto eléctrico - planta eléctrica, oficina Recursos Humanos (analistas y dirección) y Contabilidad (analistas y dirección), por lo tanto, estas áreas cuentan con medios de acceso seguro que pueden ser biométricos o cerraduras. Se enuncian a continuación las directrices establecidas por la alta dirección:

- Se determina que las áreas de mayor riesgo mencionadas anteriormente deben permanecer cerradas mientras se encuentren solas, se encuentra prohibido el acceso a estas sin acompañamiento o autorización de personal propio del proceso.

- Los medios de almacenamiento de información que contienen datos sensibles, restringidos o confidenciales se encuentran conservados en el área protegida del proceso de tecnología, este sector cuenta con un control de acceso físico por medio de biométrico al que solo tienen acceso directo los colaboradores del proceso.

- Los equipos de la organización se encuentran instalados en ambientes seguros, monitoreados en tiempo real por medio el CCTV.

- La organización determina la impermeabilización de estos cuartos con pintura anti inflamable para garantizar la seguridad física del lugar y la prevención de incendios.

- Se determina que las dos entradas a la organización cuentan con recepción y servicio de vigilancia para controlar el acceso físico solo a las personas autorizadas (colaboradores y visitantes).

- Se instalan cámaras de seguridad en la organización que están monitoreadas por el proceso de tecnología

- Se encuentra prohibido el consumo de tabaco en el interior, portería o mesas de madera de la organización, solo puede realizar el consumo al frente de las instalaciones

- Se encuentra de igual forma establecido el PLAN DE PREPARACION, PREVENCION Y RESPUESTA ANTE EMERGENCIAS, así como el PLAN DE CONTINUIDAD DE NEGOCIOS BCP, para actuar frente a amenazas ambientales, físicas o sociales.

La alta dirección efectúa un análisis de la locación física de la organización y establece la no necesidad de controles como alarmas de intrusión, detectores de movimiento, sensores sensibles al sonido, alarmas para puertas externas y otros debido a que la empresa se encuentra en un complejo de bodegas con servicio privado de vigilancia 24 horas y restricción de acceso a personas no autorizadas, adicionalmente, la empresa contrata servicio privado de vigilancia exclusivo también 24 horas, es importante mencionar que la organización labora las 24 horas al día los 365 días del año por lo tanto nunca se encuentra desalojada completamente.

Controles físicos:

- **Cuarto eléctrico:** Solo almacena UPS, tableros de distribución.
- **Planta eléctrica:** Debidamente cerrada y sin materiales inflamables en zonas cercanas
- **Data center:** Solo almacena servidores

16. POLÍTICA PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:

La compañía ha realizado un análisis detallado de los diferentes riesgos a los cuales se encuentra la continuidad del negocio, para esto se ha estipulado un documento en el cual están consignadas las directrices que se deberán manejar para estos casos. Plan de continuidad de negocio o BCP (por sus siglas en inglés Business Continuity Plan).

17. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA INFORMACIÓN

La organización ha estipulado los lineamientos necesarios para la adecuada gestión de posibles incidentes, el cual está establecido en el procedimiento para prevenirlos y para saber cómo tratarlos, PR-MPR-011 PROCEDIMIENTO DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA

INFORMACIÓN, estos lineamientos se han divulgado y socializado con todos los colaboradores en los diferentes procesos de la organización, con el fin de garantizar un oportuno reporte de estos incidentes, y así mismo dar tratamiento de manera ágil, generando un FO-MPR-025 INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

18. OBLIGACIONES DE LOS COLABORADORES

a. Guardar absoluta confidencialidad, incluso después de terminado el contrato de trabajo respecto a: procedimientos, métodos, características, lista de clientes, claves de seguridad, suministros, software, base de datos de cualquier índole, valores de bienes y servicios, información técnica, financiera, económica o comercial del contratante o sus clientes y demás que **WORLD TRAVEL ASSIST LATAM S.A.S**, utiliza en el desarrollo de su objeto social frente a clientes o terceros.

   Parágrafo Uno: El incumplimiento de esta obligación no sólo es causal de terminación de los vínculos laborales existentes entre las partes, sino que podría conllevar a iniciar acciones judicialesen contra del **Trabajador** por los perjuicios materiales e inmateriales que cause, además del cobro de la cláusula penal que más adelante se describe.

b. No ejercer actos de Competencia desleal frente a **WORLD TRAVEL ASSIST LATAM S.A.S**, porlo que el **Trabajador** se compromete a no utilizar, incluso después de terminado el contratode trabajo para sí o para beneficio de terceros: la lista de clientes, base de datos de cualquier índole, software, o procedimientos, claves secretas, métodos, características, estudios, estadísticas, proyectos, suministros utilizados por **WORLD TRAVEL ASSIST LATAM S.A.S** interna y externamente frente a sus clientes o terceros, información técnica, financiera, económica o comercial de **WORLD TRAVEL ASSIST LATAM S.A.S** o sus clientes.

   Parágrafo Dos: Es obligación del **Trabajador**, devolver inmediatamente a la terminación de su contrato, lista de clientes, claves, bases de datos, equipos, información técnica, financiera, económica o comercial y todo lo demás que tenga el **Trabajador** de **WORLD TRAVEL ASSIST LATAM S.A.S** y que haya recibido para poder ejecutar su labor.

   Parágrafo Tres: El incumplimiento de esta obligación no sólo es causal de terminación de los vínculos laborales existentes entre las partes, sino que podría conllevar a iniciar acciones judicialesen contra del **Trabajador** por los perjuicios materiales e inmateriales que

cause, además del cobro de la cláusula penal que más adelante se describe.

c. Adoptar todas las precauciones necesarias y apropiadas para la guarda de la confidencialidad de la información que tenga el **Trabajador** de la empresa, esto es, lista de clientes, base de datos de cualquier índole, su software, o procedimientos, claves secretas, métodos, características, estudios, estadísticas, proyectos, suministros utilizados por **WORLD TRAVEL ASSIST LATAM S.A.S** interna y externamente frente a sus clientes o terceros, información técnica, financiera, económica o comercial de **WORLD TRAVEL ASSISTLATAM S.A.S** o sus clientes.

Parágrafo Cuatro: La omisión del **Trabajador** en prevenir la fuga de información confidencial o exclusiva de la empresa, esto es, lista de clientes, base de datos de cualquier índole, software, o procedimientos, claves secretas, métodos, características, estudios, estadísticas, proyectos, suministros utilizados por **WORLD TRAVEL ASSIST LATAM S.A.S** interna y externamente frente a sus clientes o terceros, información técnica, financiera, económica o comercial del **WORLD TRAVELASSIST LATAM S.A.S** o sus clientes, es causal de despido con justa causa, sin perjuicio de las acciones legales en su contra por los perjuicios causados y el cobro de las sanciones por incumplimiento, además de la cláusula penal por incumplimiento.

19.SANCIONES POR INCUMPLIMIENTO

Fuera de ser causal de terminación de la relación contractual por incumplimiento de cualquiera de las obligaciones especiales que tiene el Trabajador mediante este Acuerdo de Confidencialidad, dará derecho aWORLD TRAVEL ASSIST LATAM S.A.S a exigir a título de Cláusula Penal, la suma de diez (10) salarios mínimos mensuales legales vigentes, pena que se podrá exigir vía ejecutiva, para lo cual se acepta que la presente cláusula y el acuerdo todo contenido en este acuerdo, constituyen una obligación clara, expresa y exigible, que presta mérito ejecutivo en los términos del Código de Procedimiento Civil, sin perjuicio de todas las acciones judiciales para cobrar los perjuicios ocasionados a WORLD TRAVEL ASSIST LATAM S.A.S. Como quiera que la cláusula penal pactada es a título de pena o sanción, se podrá exigir tanto la pena como la indemnización de los perjuicios a que haya lugar.

20. VIGENCIA

Esta política se mantendrá en el tiempo, así la relación laboral o de cualquier tipo haya terminado, pues su incumplimiento causará perjuicios a WORLD TRAVEL ASSIST LATAM S.A.S y le dará derecho a cobrar la cláusula penal establecida por el sólo hecho de su incumplimiento y sin perjuicio de las acciones judiciales del caso por los perjuicios causados.

La alta dirección designa a la gerencia general y director de mejora de procesos para la revisión y/o actualización anual de las políticas, o antes en caso de ser necesario

21. APROBACIÓN

El presente manual de políticas se establece y se aprueba por la gerencia el 25 de octubre del 2023

X

Sabrina Morales
Gerente general

Se comprometen con el control y cumplimiento de las políticas

X

Carolina Jaramillo López
Directora de mejora de procesos

X

Brayan Ramón Moncada Hincapié
Oficial de Seguridad de la información