Tabla de conteúdo

APRESENTAÇÃO DO MANUAL

A direção da World Travel Assist, compreendendo a importância de uma gestão adequada da sua informação, comprometeu-se com a implementação de um sistema de gestão da segurança da informação, procurando adotar um quadro de confiança no exercício das suas funções junto do Estado e dos cidadãos, todo enquadrado no estrito cumprimento das leis, regulamentos internacionais ISO NTC IEC 27001:2013 e conforme a missão e visão da entidade.

Para a World Travel Assist, a proteção da informação procura reduzir os riscos gerados nos seus ativos, identificando-a de forma sistemática, para manter um nível de exposição que permita preservar a sua integridade, confidencialidade e disponibilidade, conforme as necessidades dos diferentes grupos de interesse identificados.

Segundo o exposto, esta política aplica-se à Entidade definida no âmbito, aos seus dirigentes, terceiros, estagiários, estagiários, fornecedores e cidadãos em geral, tendo em conta que os princípios em que se baseia o desenvolvimento das ações ou a tomada de decisões em torno do SGSI será determinada pelas seguintes premissas:

· Minimizar o risco em todas as funções da entidade.
· Cumprir os princípios de segurança da informação.
· Cumprir os princípios da função administrativa.
· Mantenha a confiança de seus clientes, parceiros e funcionários.
· Apoiar a inovação tecnológica.
· Proteger ativos tecnológicos.
· Estabelecer políticas, procedimentos e instruções relativas à segurança da informação.
· Fortalecer a cultura de segurança da informação entre funcionários, terceiros, estagiários, estagiários e clientes da World Travel Assist.
· Garantir a continuidade dos negócios perante os incidentes.

A World Travel Assist decidiu definir, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação, apoiado em diretrizes claras, conforme as necessidades do negócio e requisitos regulamentares.
Abaixo estão 12 princípios de segurança que apoiam o World Travel Assist ISMS:

• As responsabilidades relativas à segurança da informação serão definidas, compartilhadas, publicadas e aceitas por cada um dos funcionários, fornecedores, parceiros de negócios ou terceiros.

• A World Travel Assist protegerá a informação gerada, processada ou salvaguardada pelos processos de negócio, a sua infraestrutura tecnológica e ativos do risco gerado pelo acesso concedido a terceiros (por exemplo, fornecedores ou clientes), ou como resultado de um serviço interno.

• A World Travel Assist protegerá as informações criadas, processadas, transmitidas ou salvaguardadas pelos seus processos de negócio, para minimizar os impactos financeiros, operacionais ou legais devido ao seu uso incorreto. Para isso, é fundamental aplicar controles conforme à classificação das informações possuídas ou custodiadas.

• O World Travel Assist protegerá suas informações contra ameaças provenientes de funcionários.

• O World Travel Assist protegerá as instalações de processamento e a infraestrutura tecnológica que dão suporte aos seus processos críticos.

• A World Travel Assist controlará o funcionamento dos seus processos de negócio, garantindo a segurança dos recursos tecnológicos e das redes de dados.

• A World Travel Assist implementará controle de acesso a informações, sistemas e recursos de rede.

• A World Travel Assist garantirá que a segurança seja parte integrante do ciclo de vida dos sistemas de informação.

• A World Travel Assist garantirá, através da gestão adequada dos eventos de segurança e das fragilidades associadas aos sistemas de informação, uma melhoria efetiva do seu modelo de segurança.

• A World Travel Assist garantirá a disponibilidade dos seus processos de negócio e a continuidade da sua operação em função do impacto que os eventos podem gerar.

• A World Travel Assist garantirá o cumprimento das obrigações legais, regulamentares e contratuais estabelecidas.

NOTA: Estas políticas serão revisadas e atualizadas, se necessário, semestralmente, ou antes, no caso de uma eventualidade que o justifique.

1. OBJETIVO

O objetivo deste manual é definir uma estrutura para o desenvolvimento do sistema de gestão de segurança da informação, a fim de protegê-lo e aos seus ativos contra uso não autorizado, divulgação, modificação, dano ou perda e garantir a conformidade com os regulamentos e leis aplicáveis ao mundo. TRAVEL ASSIST LATAM S.A.S.

2.ÂMBITO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta política é aplicável aos processos descritos no mapa de processos da World Travel Assist Latam SAS, que deve atender a este requisito sem prejuízo de ter políticas adicionais ou mais restritivas, a fim de melhorar a segurança da informação. O âmbito desta política abrange também fornecedores, clientes, terceiros e todas as partes interessadas.

Cada um dos processos da organização desenvolverá esta política em suas atividades e deverá reportar sua adequação ao processo de melhoria de monitoramento do sistema de gestão de segurança da informação.

A política deverá estar disponível no site corporativo da WTA https://wtabyhas.com/, bem como em repositório comum da empresa e afixada nas instalações da organização.

1. DEFINIÇÕES

Ativo: De acordo com [ISO IEC 13335-12004]: qualquer coisa que tenha valor para a organização. Também é entendido como qualquer informação ou sistema relacionado ao seu processamento que tenha valor para a organização. É qualquer bem que contenha informação, que tenha valor e seja necessário para a realização dos processos missionários e operacionais do DAPRE. Eles podem ser classificados da seguinte forma:

Acordo de Confidencialidade: é um documento no qual os funcionários da WORLD TRAVEL ASSIST LATAM S.A.S ou aqueles fornecidos por terceiros expressam sua disposição de manter a confidencialidade das informações da empresa, comprometendo-se a não divulgar, usar ou explorar as informações confidenciais a quem tiver acesso em virtude do trabalho que realizam.

Aplicativos: É todo o software utilizado para gerenciamento de informações. Exemplo: SIGEPRE.
Autenticação: Processo que visa garantir a identificação de uma pessoa ou sistema.

Autenticidade: Os ativos de informação só podem ser disponibilizados através da verificação

da identidade de um sujeito ou recurso, é a propriedade que garante que a identidade de um sujeito ou recurso é aquela declarada e aplicada a entidades como utilizadores, processos, sistemas de informação.

Confidencialidade: Acesso à informação apenas por quem está autorizado, segundo com [ISO IEC 13335-1:2004]: "característica/propriedade pela qual a informação não está disponível ou divulgada a indivíduos, entidades ou processos não autorizados.

Controle: são todas aquelas políticas, procedimentos, práticas e estruturas organizacionais destinadas a manter os riscos de segurança da informação abaixo do nível de risco assumido (Nota: Controle também é usado como sinônimo de salvaguarda).

Dados: São todos aqueles elementos básicos de informação (em qualquer formato) que são gerados, coletados, gerenciados, transmitidos e destruídos no DAPRE. Exemplo: arquivo Word "lista de pessoal.docx".

Equipamentos auxiliares: São todos aqueles bens que suportam os sistemas de informação e que não se enquadram em nenhuma das tipologias previamente definidas. Exemplo: Ar condicionado, trituradora de papel.

Informação: Refere-se a um conjunto organizado de dados contidos em qualquer documento que os sujeitos obrigados gerem, obtenham, adquiram, transformem ou controlem. Constitui um ativo importante, essencial para as atividades de uma organização e, consequentemente, necessita de proteção adequada. A informação pode existir de diversas formas, ou seja, pode ser impressa ou escrita em papel, pode ser armazenada eletronicamente, transmitida por correio ou por meio eletrônico, pode ser mostrada em vídeos, ou apresentada oralmente em conversas.

Instalações: São todos os locais onde estão alojados os sistemas de informação. Exemplo: Escritório de Pagamentos.

Integridade: Manter a exatidão e integridade das informações e seus métodos de processamento. De acordo com [ISO IEC 13335-1:2004]: propriedade/característica de salvaguardar a exatidão e integridade dos ativos.

Pessoal: É todo o pessoal da DAPRE, pessoal subcontratado, clientes, usuários e, em geral, todos os que têm acesso, de uma forma ou de outra, aos ativos de informação da DAPRE. Exemplo: Pedro Pérez.

Política de segurança: Definição na qual se estabelece o comprometimento da Administração e o foco da organização na gestão da segurança da informação.

Plano de Continuidade de Negócio: Plano que visa permitir a continuação das principais funções da Entidade em caso de imprevisto que as coloque em perigo.

Segurança da informação: Conforme [ISO IEC 27002:2005]: preservação da confidencialidade, integridade e disponibilidade da informação; além disso, outras propriedades como autenticidade, responsabilidade, não repúdio, rastreabilidade e confiabilidade também podem ser consideradas.

Sistema de Gestão de Segurança da Informação SGSI: De acordo com [ISO IEC 27001:2013]: sistema de gestão global que, com base na análise de risco, estabelece, implementa, opera, monitora, revisa, mantém e melhora a segurança da informação. (Nota: O sistema de gestão inclui uma estrutura organizacional, políticas, planejamento de atividades, responsabilidades, procedimentos, processos e recursos.)

Serviços: São serviços internos, aqueles que uma parte da organização fornece a outra, e serviços externos, aqueles que a organização fornece a clientes e usuários. Exemplo: Publicação de currículos, solicitação de férias.

Tecnologia: São todos os equipamentos utilizados para gerenciar informações e comunicações. MANUAL DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, Processo associado, Código Versão Tecnologias de Informação e Comunicação M-TI-01 10 6 Exemplo: equipamentos informáticos, telefones, impressoras.

Usuário: neste documento, refere-se a gestores, funcionários, prestadores de serviços, terceiros e outros colaboradores, devidamente autorizados a utilizar equipamentos, sistemas ou aplicações informáticas e aos quais é concedido um nome de utilizador e um código de acesso.

Vulnerabilidade: Fraqueza na segurança da informação de uma organização que potencialmente permite que uma ameaça afete um ativo. De acordo com [ISO IEC 13335-1:2004]: fraqueza de um ativo ou conjunto de ativos que pode ser explorado por uma ameaça.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

“A World Travel Assist fornece os recursos necessários para estabelecer e operar um sistema de gestão de segurança da informação que estabeleça as diretrizes para garantir a confidencialidade, integridade e disponibilidade das informações corporativas e de todas as partes interessadas, localizadas nos sistemas de informação e softwares que armazenam, processam e. transmitir informações de todos os nossos processos, atendendo aos requisitos e expectativas de nossos clientes. O objetivo do sistema é proteger as informações por meio da implementação e avaliação da eficácia de planos de tratamento, ações e manutenção de controles físicos, organizacionais, de pessoas e tecnológicos e estabelece os seguintes objetivos:

- Reduzir os riscos aos quais os ativos de informação estão expostos
- Estabelecer uma cultura de segurança da informação na empresa
- Garantir a conformidade com os requisitos legais, contratuais e comerciais atuais
- Adotar as diretrizes de segurança da informação estipuladas neste documento
- Estabelecer ações disciplinares e legais em caso de descumprimento de tais políticas.”

3.POLÍTICA PARA O USO DE DISPOSITIVOS MÓVEIS

A WORLD TRAVEL ASSIST LATAM S.A.S definiu as seguintes condições para a gestão de dispositivos móveis (smartphones, tablets, entre outros) de caráter institucional e pessoal:

A empresa fornece dispositivos móveis exclusivamente empresariais para cada processo da empresa, dotados dos recursos necessários como plano de dados e minutos para cumprir as respetivas funções.

A empresa garantirá que os funcionários façam uso responsável dos equipamentos fornecidos, conforme as disposições da DC-MPR-018 LINHAS CELULARES CORPORATIVAS E POLÍTICA DE EQUIPAMENTOS. Essas revisões de bom uso são realizadas pelo responsável pela segurança da informação segundo o cronograma de revisão, deixando evidências das constatações no formato FO-MPR-020 REGISTROS DE CHAMADA DE ATENÇÃO.

A administração estabelece a seguinte lista de pessoal autorizado a utilizar dispositivos móveis pessoais dentro da organização:

Processo	Nome do diretor autorizado
Gerência geral	Sabrina Morales
Melhora de processos	Carolina Jaramillo
Contabilidade	Carolina León
Fidelização de clientes	Mariana Vega
Talento humano	Paula Cocomá
Claims	Erika Rengifo
Qualidade	Luisa Mejía
TPA e informação dos seguros	Felipe Navarrete
Tecnologia	Andrés Ramírez
Provedores	Andrés Mejía
Segurança e saúde no trabalho	Vanessa Restrepo
Reembolsos	Catalina Moribe
Operações	Julio Carvajal
Departamento médico	David Ñañez

Capacitação e treinamento	Steven Castaño
Desenvolvimentos digitais	Arturo Álvarez

4. POLÍTICA DE ACESSO ÀS REDES E RECURSOS DE REDE

O Departamento de Tecnologia da WORLD TRAVEL ASSIST LATAM S.A.S, como responsável pelas redes de dados e recursos de rede da empresa, utilizou diversos mecanismos lógicos de controle de acesso, para estarem protegidos contra qualquer acesso não autorizado.

As redes sem fio da empresa possuem métodos de autenticação que impedem o acesso não autorizado, incluindo o uso do firewall e do documento HOST com domínios listados aos quais o acesso é restrito. Adicionalmente, sobre a utilização da plataforma KASPERSKY e os bloqueios que ela gerencia, a descrição detalhada do procedimento de administração da rede encontra-se no documento DC-ITS-003 ADMINISTRAÇÃO DE REDES E PLATAFORMAS TECNOLÓGICAS.

Os equipamentos de informática que desejarem se conectar às redes de dados da empresa deverão atender a todos os requisitos e/ou controles para autenticação aos mesmos (Credenciais de Usuário), listados no procedimento PR-ITS-009 CONFIGURAÇÃO DE EQUIPAMENTOS PARA USO EMPRESARIAL e somente poderão para desempenhar as funções para as quais foram autorizados.

A conexão de terceiros ou visitantes às redes da empresa será realizada conforme o disposto no procedimento PR-ITS-012 PROCEDIMENTO DE ENTRADA NA REDE WTA DE TERCEIROS.

Os sites de lazer que não correspondam à atividade laboral da empresa são restritos, no entanto, existe uma rede com ligação a um portal cativo (rede GUEST), distinto do IP público corporativo, que permite o acesso a estes sites para fins recreativos e apenas nos horários não laborais (horário de almoço e respetivos períodos de descanso).

5. POLÍTICA DE ADMINISTRAÇÃO DO ACESSO DE USUÁRIOS

A WORLD TRAVEL ASSIST LATAM S.A.S determinou privilégios para o controle lógico de acesso de cada usuário ou grupo de usuários sobre os recursos tecnológicos e sistemas de informação da empresa. Garantir que os funcionários e pessoal fornecido por terceiros tenham acesso apenas às informações necessárias para a realização do seu trabalho.

A Diretoria de Tecnologia instituiu o procedimento PR-ITS-016 CRIAÇÃO, MODIFICAÇÃO E DESATIVAÇÃO DE CONTAS DE USUÁRIOS, que contempla a criação, modificação, bloqueio ou eliminação de contas de usuários, para administração de usuários em redes de dados, recursos tecnológicos e sistemas de informação da empresa, esses procedimentos devem ser realizados em tempo hábil, quando os funcionários saem, se afastam, são promovidos ou postos em outras posições dentro da operação da empresa.

6. POLÍTICA DE RESPONSABILIDADES DE ACESSO DOS USUÁRIOS

O objetivo desta política é delimitar o acesso e uso aceitável de todos os equipamentos de informática, serviços e sistemas de informação, bem como das redes de dados da WORLD TRAVEL ASSIST LATAM S.A.S. Estas regras visam proteger os colaboradores e a organização da utilização inadequada de informação, serviços de rede e equipamentos informáticos. A empresa motivará estas ações através da sensibilização e informação contínua do pessoal, conforme o plano de formação constante do SGSI, evidenciado no documento FO-MPR-022 PLANEJAMENTO DO SISTEMA DE SEGURANÇA DA INFORMAÇÃO 2024.

Todos os colaboradores, incluindo terceiros, devem ter acesso apenas às informações de que necessitam para o legítimo desenvolvimento das suas funções e atividades dentro da organização. A atribuição de privilégios e acesso aos ativos de informação (e-mail institucional, softwares, aplicativos, pastas compartilhadas, etc.) deve ser baseada nas necessidades das áreas e aprovada pelo proprietário dos ativos, para determinar a permissão aos usuários dos ativos de informação. A alta administração determina na MATRIZ DE INVENTÁRIO E CLASSIFICAÇÃO DE ATIVOS DE INFORMAÇÃO DC-MPR-010 a categorização por confidencialidade que especifica as permissões de uso que cada ativo possui e qual possui autorização de acesso para cada processo ou posição.

O acesso só poderá ser concedido a pessoas externas à instituição, mediante autorização prévia do proprietário do meio de processamento da informação e do proprietário da informação. As contas de acesso de terceiros devem ter um prazo de validade especificado, que deve ser controlado pelo Processo de Tecnologia e pelo líder do processo, conforme apropriado.

Os colaboradores deverão ser responsáveis pelo nome de usuário e senha atribuídos para acesso aos sistemas de informação WTAOPS e Communicator; em nenhuma hipótese poderão compartilhar essas informações com outros funcionários ou terceiros; em relação ao acesso de mídia às contas Skype e Gmail, os usuários poderão acessar por meio do processo tecnológico, que será responsável por estabelecer senhas em cada computador. As causas da falta desta responsabilidade estão estabelecidas no ANEXO DC-MPR-016 FALHAS DE SEGURANÇA DA INFORMAÇÃO.

Nota: Esta política é ampliada na POLÍTICA DE CONTROLE DE ACESSO DC-MPR-013 estabelecida pela alta administração.

7.POLÍTICA DE USO DE SENHAS NA WORLD TRAVEL ASSIST

Senhas pessoais:

A organização estabelece que para os sistemas de informação WTAOPS e Communicator as senhas iniciais são estabelecidas pelo provedor, porém, na primeira entrada, o usuário deverá alterar a senha conforme à política e ações para construção de senhas seguras mencionadas abaixo.
Qualquer senha de acesso ao sistema operacional WTAOPS e ao sistema Communicator da empresa é pessoal e intransferível, cada funcionário é responsável por ela, devendo garantir que suas senhas não sejam vistas ou aprendidas por outros funcionários.

Política e ações para construir senhas seguras:

1. Pelo menos 8 caracteres devem ser usados para criar a chave.
2. Recomenda-se a utilização de dígitos, letras e caracteres especiais na mesma senha.
3. Recomenda-se que as letras alternem aleatoriamente entre maiúsculas e minúsculas. Você deve ter em mente quais letras são maiúsculas e quais são minúsculas.
4. Escolha uma senha que possa ser facilmente lembrada e de preferência anotada rapidamente, de preferência sem precisar olhar para o teclado.
5. As senhas devem ser alteradas com certa regularidade, o sistema operacional exige uma alteração de senha a cada 3 meses.
6. Use sinais de pontuação se o sistema permitir. Por exemplo: “Tr-.3Fre”. Neste caso de incluir outros caracteres que não sejam alfanuméricos na senha, este conselho incluiria o uso de símbolos como: ! " # $% & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

Ações a evitar ao gerenciar senhas fortes:

1. Você deve evitar usar sempre a mesma senha em todos os sistemas ou serviços. Por exemplo, deve haver uma senha para WTAOPS e uma senha diferente para o Communicator por usuário.

2. Não utilize informações pessoais na senha: nome do usuário ou de seus familiares, nem sobrenomes,

nem data de nascimento. E, claro, em hipótese alguma utilize dados como número de identificação ou telefone.
3. Evite usar sequências básicas de teclado (por exemplo: “qwerty”, “asdf” ou as sequências de numeração típicas: “1234” ou “98765”)
4. Não repita os mesmos caracteres na mesma senha. (ex.: “111222”).
5. Você também deve evitar usar apenas números, letras maiúsculas ou minúsculas na senha.
4. O nome de usuário associado ao nome não deve ser usado como nome ou conteúdo.
5. Não utilize dados relacionados ao usuário que sejam facilmente dedutíveis ou derivados deles. (por exemplo, não use apelidos, nome do ator ou personagem fictício favorito, etc.) como senha.
6. Não escreva ou reflita a senha em um papel, ou documento onde ela esteja registrada. Elas também não devem ser salvas em documentos de texto no computador ou no próprio dispositivo (por exemplo, não salve senhas de cartão de débito/crédito em seu celular ou senhas de e-mail em documentos de texto em seu computador).
7. Não devem ser utilizadas palavras contidas em dicionários de qualquer idioma. Hoje em dia existem programas de cracking de chaves que baseiam o seu ataque no teste das palavras que extraem dos dicionários, uma por uma: este método de ataque é conhecido como “ataque de dicionário”.
8. Nunca envie a senha por e-mail ou mensagem de texto. Nem deve ser fornecido ou mencionado numa conversa, ou comunicação de qualquer tipo.
9. Não escreva senhas em computadores cujo nível de segurança seja desconhecido e possa ser monitorado, ou em computadores de uso público (bibliotecas, cibercafés, telecentros, etc.).
10. Altere as senhas padrão fornecidas pelos desenvolvedores (WTAOPS e Communicator).

Senhas de compartilhamento gerenciado por tecnologia:

Levando em consideração que a informação é um ativo de grande importância para a organização, a alta administração estabelece que as senhas dos meios de comunicação interna, como e-mails Skype e Gmail, devem ser criadas, gerenciadas e controladas pelo processo de Tecnologia, a fim de evitar danos e perdas por uso malicioso por colaboradores. Esta determinação é considerada uma vez que outros sistemas de informação, como WTAOPS e Communicator geram controles seguros que evitam vazamento ou perda de informações.

Nenhum funcionário da organização tem autorização para realizar alterações nas senhas das contas do Skype ou Gmail. Caso seja necessário, deverá solicitar a alteração através do líder do processo, que deverá transmitir a solicitação ao processo tecnológico;

Os meios de comunicação que a organização disponibiliza aos colaboradores são de uso estritamente profissional, portanto, a divulgação de qualquer informação pessoal é de responsabilidade do colaborador e não acarretará sanções para a organização, portanto, a alta administração estabelece que se for necessário, a área de tecnologia tem autoridade para realizar revisões ou verificações das informações transmitidas pelas contas Skype, ou Gmail mediante solicitação prévia do líder, ou gerenciamento do processo.

Ferramentas e soluções de TI:

Para cumprir a política e ações para construção de senhas seguras, a ferramenta utilizada pelo nosso processo tecnológico para criá-las é: https://www.lastpass.com/es/features/password-generator#generatorTool

A organização estabelece os seguintes controles para gerenciamento de senhas:
1. Frequência de alteração de senha: A cada 3 meses
2. Responsável pela criação e atualização de chaves: Analista de tecnologia
3. Controle diferentes senhas para contas do Skype e Gmail
4. As senhas serão salvas em cada computador apenas pelo processo tecnológico; qualquer necessidade ou solicitação que exija o uso de senhas exigirá intervenção da tecnologia.
5. A tecnologia realizará mensalmente revisões aleatórias de senhas de cada processo, deixando um registro no CRM da tecnologia.

8. POLÍTICA DE SEGURANÇA E MANUTENÇÃO PARA OS APARELHOS INSTITUCIONAIS

Para evitar a perda, alteração ou dano dos recursos tecnológicos da empresa, o Departamento de Tecnologia da WORLD TRAVEL ASSIST LATAM S.A.S determinou os seguintes mecanismos e estratégias para proteger sua integridade, dentro e fora das instalações:

Geração de atas de entrega com assinatura de responsabilidade do usuário final do equipamento e do líder do processo correspondente. FO-ITS-016 REGISTRO DE ENTREGA E RECEBIMENTO DE EQUIPAMENTOS DE INFORMÁTICA OU FERRAMENTAS DE TRABALHO.

Configuração inicial do equipamento, conforme disposto no procedimento PR-ITS-009 CONFIGURAÇÃO DE EQUIPAMENTOS PARA USO EMPRESARIAL, no que diz respeito à configuração de senhas e credenciais de acesso.

O Departamento de Tecnologia realizará manutenções preventivas e corretivas nos equipamentos de informática e dispositivos móveis da empresa de acordo com o disposto no procedimento PR-ITS-001 MANUTENÇÃO PREVENTIVA DE EQUIPAMENTOS E INFRAESTRUTURA TECNOLÓGICA.

A Diretoria de Tecnologia é a única autorizada a realizar movimentações e cessões de recursos tecnológicos; consequentemente, é proibida a disposição de qualquer funcionário dos recursos tecnológicos da empresa.

Quando ocorrer falha ou problema de hardware/software em uma estação de trabalho ou outro recurso tecnológico, o usuário responsável deverá informar o processo de Tecnologia, a fim de prestar a assistência adequada. O usuário não deve tentar resolver o problema.

9.POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A WORLD TRAVEL ASSIST LATAM S.A.S protegerá os dados pessoais de seus beneficiários, fornecedores e demais terceiros que recebem e gerenciam informações. Enquanto responsável pelos dados pessoais obtidos por meio de dois canais de atendimento distintos, a empresa estabelece os termos e condições que utilizará para o tratamento dos dados pessoais que, a qualquer momento, por motivos da atividade desenvolvida pela empresa, tenha fornecido dados pessoais , garantindo que as informações acima mencionadas sejam armazenadas em bancos de dados ou qualquer outra configuração:

-Ser utilizado apenas para funções empresariais, conforme a legislação nacional vigente, Lei

1.581 de 2012.
- Não ser publicado, revelado ou entregue a funcionários públicos, ou terceiros sem autorização.
- Não ser divulgado, alterado ou excluído sem a necessária autorização.

Nas áreas de tratamento de dados, os beneficiários ou usuários finais deverão obter autorização para o tratamento de dados (atribuído Formulário de Liberação de Cadastro) para coletar, transferir, armazenar, utilizar, circular, excluir, compartilhar, atualizar e transmitir esses dados a usuários não públicosno desenvolvimento das atividades da empresa.

Nas áreas que tratamos, devemos garantir que as pessoas beneficiárias, funcionários, fornecedores ou outros terceiros tenham uma necessidade laboral legítima, ou que a informação necessária ao desenvolvimento das atividades laborais esteja acessível a esses dados. Para o acima exposto, estão disponíveis as seguintes ferramentas seguras de armazenamento de informações:

-Sistema operacional WTAOPS: informações do cliente, usuários finais
-Armar unidades em rede local (compartilhadas de forma segura): informações de funcionários, documentação interna de processos, fornecedores.
Somente os colaboradores do processo têm acesso a essas unidades (compartilhadas de forma segura) e desta forma não interferem mais nas informações, não que isso diga respeito aos dois clientes dados, estes só são tratados de forma direta e segura nos servidores do nosso sistema de segurança da informação.
A organização determina a POLÍTICA DE PROCESSAMENTO DE DADOS DE PESSOAIS DC-MPR-022, a fim de garantir o comprimento da Lei 1.581 de 2022.

10.POLÍTICA DE ESTRUTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

A gestão da empresa, conforme o compromisso do Sistema de Gestão de Segurança da Informação assume o compromisso de disponibilizar os recursos necessários ao desenvolvimento e conformidade do Sistema de Gestão da Segurança da Informação. Da mesma forma, definiu e estabeleceu funções e responsabilidades que envolvem as atividades de operação, gestão e administração de segurança da informação, bem como a existência do Comitê de Segurança da Informação, definido em sua respectiva ata de constituição.
Adicionalmente, a administração também designa todos os diretores de processos como responsáveis pelo cumprimento das atividades e políticas do sistema dentro de sua área, bem como reportar qualquer incidente ao diretor de segurança da informação para seu respectivo plano de ação.

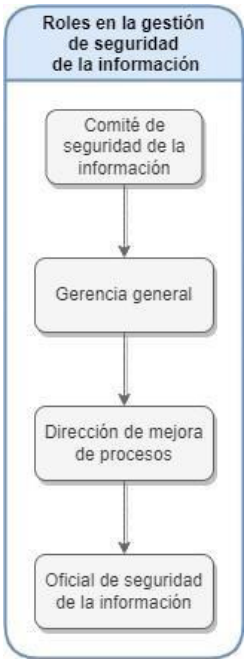
Gerência geral

Oficial de segurança da informação

Direção de melhora de processos

Os funcionários responsáveis designados pela administração são:

Funções na gestão da segurança da informação



Cargo	Nome	Responsabilidades	Função
Direção de melhora de processos	Carolina Jaramillo López	-Notificar em tempo hábil duas alterações e melhorias feitas em. seu processo que impacta os sistemas de gestão. -Participar ativamente nos processos de auditoria interna da organização. -Tomar medidas tempestivamente contra não conformidades identificadas nos processos de auditoria interna dos sistemas de gestão -Atualize a documentação do seu processo em relação ao sistema de gestão -Dirigir a implementação e operação do sistema de segurança da informação. (ISMS) -Cumprir a política geral de	-Criação de estratégias que levam ao cumprimento dos objetivos definidos - Criação de estratégias que aumentarão a produtividade e otimizarão os recursos -Gerenciar riscos de negócio e de segurança da informação que permitam estabelecer uma matriz de análise de risco com seu tratamento. -Coordenar atividades e ações de auditoria interna em segurança da informação -Coordenação conjunta com outros processos de aplicação de controles organizacionais e controles de segurança da informação.

		segurança da informação e os padrões definidos para o cumprimento do sistema de segurança da informação. (ISMS) • Cumprir a política geral de segurança da informação e os padrões definidos para cumprimento do sistema de segurança da informação. (ISMS)	• Revisar e avaliar os indicadores de gestão correspondentes à atenção dos incidentes de segurança a serem apresentados à alta administração.

Oficial de segurança da informação	Brayan Moncada Hincapié	-Manter uma política de segurança abrangente -Desenvolvimento, execução e supervisão de estratégias de segurança da informação -Gestão, gestão e vigilância do controle de acesso às informações da empresa -Fortalecer a cultura de segurança da informação. -Fazer bom uso e gestão das ferramentas e equipamentos designados pela organização para o desempenho de suas funções. -Cumprir as normas de Saúde e Segurança Ocupacional e os regulamentos próprios da empresa. -Estar informado sobre os últimos desenvolvimentos do setor e manter uma atualização constante de conhecimentos para fornecer uma resposta flexível e ágil a qualquer incidente cibernético que possa afetar o funcionamento da empresa. -Implementar e monitorar o plano de treinamento do sistema de segurança nas informações	• Implementar e verificar a conformidade com o sistema de gestão de segurança. • Verificar a conformidade com as políticas de segurança por parte de todos os colaboradores • Monitorar incidentes de segurança • Garantir a máxima proteção e privacidade dos dados e informações corporativas • Ser responsável pelo planejamento resposta a incidentes, bem como investigação de violação de segurança • Coordenar a implementação de controles específicos de segurança da informação para novos sistemas ou serviços. • Realizar planos de treinamento para sistema de segurança da informção

Grupo de segurança da informação		
Processo	**Nome**	**Função**
Talento Humano	Cesar Lopez	Apoiar a implementação e operação do sistema de segurança da informação. (ISMS) -Verificar o cumprimento das políticas de segurança da informação, dentro de cada processo -Transmitir toda a informação relativa ao SGSI, dentro de cada processo -Expor ou compartilhar possíveis novos riscos relacionados com a segurança da informação
Provedores	Christian Rodas	
Qualidade	Valentina Correa-Dana Ramos	
SG-SST	Sara Agudelo	
Customer	Paulina Jaramillo	
Médico	Manuel Ramirez	
Capacitação	Manuel Cuyato	
Reembolsos	Juan Manuel Betancurt	
Contabilidade	Laura Sánchez	
TPA	Jacobo Herrera	
Operações	Angela Gañan	

Usuários:

Os usuários do SGSI são todos funcionários da organização e têm as seguintes responsabilidades:

-Cumprir as políticas de segurança da informação

-Relatar incidentes de segurança que ameacem a confidencialidade, integridade ou disponibilidade de informações, ou que evidenciem uma violação de políticas

- Participar ativamente em todas as campanhas de sensibilização e formação do sistema

-Apoiar o desenvolvimento de auditorias internas e externas do sistema

Nota: A ATA DE CONFORMAÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO e o MANUAL DE FUNÇÕES DO DIRETOR DE SEGURANÇA DA INFORMAÇÃO MN-MPR-002 estão relacionados a esta política.

Gestão de desvios e exclusões do sistema de segurança da informação:

A Administração realiza análise e revisão dos controles do Anexo A da NTC ISO 27001:2022 e, em atendimento aos controles organizacionais aplicáveis com base nas atividades da organização, gera o documento DC-MPR-017 DECLARAÇÃO DE APLICABILIDADE para gestão de desvios e exclusões .

11. POLÍTICA DE RELAÇÃO COM FORNECEDOR.

Consciente da importância de manter a segurança da informação e dos serviços de tratamento de informação a que terceiros ou entidades externas tenham acesso, a empresa estabeleceu os seguintes mecanismos de controle nas relações contratuais, com o objectivo de garantir que a informação ou serviços a que tenham acesso ou que são fornecidos por fornecedores ou contratados atendem aos padrões de segurança da informação.

Os contratantes, licitantes e/ou fornecedores deverão aceitar e assinar o acordo de confidencialidade estabelecido nos contratos ou acordos com fornecedores e/ou contratados, sendo inclusa a causa de rescisão do contrato ou contrato de serviço, por descumprimento das políticas de segurança da informação. Essas informações são gerenciadas conforme o procedimento PR-RSC-002 de Seleção, avaliação e reavaliação de fornecedores.

Pelo exposto, a Organização determina a seguinte POLÍTICA DE RELACIONAMENTO COM FORNECEDORES DC-MPR-020 onde são estabelecidas as diretrizes de segurança da informação necessárias.

12. POLÍTICA DE ESCRITÓRIO LIMPO E BLOQUEIO DA TELA

A empresa definiu esta política visando prevenir o acesso não autorizado, perda e/ou dano à informação encontrada em postos de trabalho, equipamentos informáticos, suportes amovíveis, dispositivos de impressão e digitalização de documentos, durante e fora do horário de trabalho:

- Todas as mesas deverão permanecer desobstruídas e livres de documentos físicos ou mídias removíveis que contenham informações sensíveis, restritas ou confidenciais, com exceção dos processos de Recursos Humanos, Contabilidade e Saúde e Segurança do Trabalho, uma vez que, de acordo com a natureza do seu trabalho, exige manuseio informações em um ambiente físico. Os relatórios impressos que contenham informações sensíveis, restritas ou confidenciais devem ser imediatamente removidos das impressoras, armazenados ou excluídos imediatamente.

- Somente as equipes dos processos de recursos humanos, segurança e saúde ocupacional e contabilidade estão autorizadas a configurar o uso de impressoras, fotocopiadoras ou scanners. Caso outros processos necessitem destes serviços, deverão solicitá-los através dos recursos humanos.

- As informações confidenciais localizadas fisicamente devem ser armazenadas em escritórios trancados.

- Todos os computadores devem ser bloqueados quando a estação de trabalho estiver desocupada ou desacompanhada através das teclas Windows + L. O processo Tecnologia é responsável pela configuração de inatividade do equipamento, fica estabelecido que após um minuto de inatividade o computador deve ser bloqueado.
- A tela do computador (desktop) não deve conter nenhum tipo de arquivo, exceto atalhos para os aplicativos necessários descritos no procedimento PR-ITS-009 CONFIGURAÇÃO DE EQUIPAMENTOS PARA USO EMPRESARIAL.

- É totalmente proibido o consumo de alimentos no local de trabalho.

13. POLÍTICA DE SEGURANÇA FÍSICA E AMBIENTAL

Foi implementado o programa de segurança física de acesso às instalações, que permite reforçar a confidencialidade, disponibilidade e integridade da informação, por meio de controles de acesso e monitorização em áreas de escritórios e instalações onde reside informação restrita ou confidencial ou ativos tecnológicos valiosos, explicitamente as áreas que representam maior risco de violação ou acesso não autorizado às informações são: tecnologia (sala de servidores ou data center, escritório de tecnologia e gestão), sala elétrica - usina, escritório de Recursos Humanos (analistas e gestão) e Contabilidade (analistas e gestão), portanto, essas áreas possuem meios de acesso seguros que podem ser biométricos ou fechaduras. As diretrizes estabelecidas pela alta administração estão definidas abaixo:

- Fica determinado que as áreas de maior risco mencionadas acima devem permanecer fechadas enquanto não estiverem sendo ocupadas; é proibido o acesso a elas sem acompanhamento ou autorização do pessoal do processo.

- Os meios de armazenamento de informações que contenham dados sensíveis, restritos ou confidenciais são mantidos na área protegida do processo tecnológico; este setor possui controle de acesso físico por meio de biometria, à qual apenas os colaboradores do processo têm acesso direto.

- Os equipamentos da organização são instalados em ambientes seguros, monitorados em tempo real através de CFTV.
- A organização determina a impermeabilização destas salas com tinta anti-inflamável para garantir a segurança física do local e a prevenção de incêndios.
- Fica determinado que as duas entradas da organização disponham de serviço de recepção e vigilância para controlar o acesso físico apenas a pessoas autorizadas (colaboradores e visitantes).
- Câmeras de segurança são instaladas na organização e monitoradas pelo processo tecnológico.
- É proibido o consumo de tabaco no interior, baliza ou mesas de madeira da organização, o consumo só poderá ser realizado em frente às instalações

  É também estabelecido o PLANO DE PREPARAÇÃO, PREVENÇÃO E RESPOSTA A

EMERGÊNCIAS, bem como o PLANO DE CONTINUIDADE DE NEGÓCIOS do BCP, agir contra ameaças ambientais, físicas ou sociais.

A alta direção realiza uma análise da localização física da organização e estabelece a necessidade de controles como alarmes de intrusão, detectores de movimento, sensores sensíveis a som, alarmes para portas externas e outros porque a empresa está localizada em um complexo de armazéns com armazéns do serviço de segurança privada 24 horas e restrição de acesso a pessoas não autorizadas. Além disso, a empresa contrata serviço exclusivo de segurança privada também 24 horas por dia. É importante ressaltar que a organização funciona 24 horas por dia, 365 dias por ano e o prédio nunca é completamente desalojado.

Controles físicos:
-Sala elétrica: Armazena apenas UPS, quadros de distribuição.
- Usina: Devidamente fechada e sem materiais inflamáveis nas áreas próximas.
- Data center: armazena apenas servidores.

14. POLÍTICA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS:

A empresa realizou uma análise detalhada dos diferentes riscos a que está exposta a normal continuidade dos negócios, para isso foi estipulado um documento no qual estão registradas as diretrizes que devem ser gerenciadas para estes casos. Plano de continuidade de negócios ou BCP (Plano de Continuidade de Negócios).

15. POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A organização estipulou as diretrizes necessárias para o gerenciamento adequado de possíveis incidentes, o que está estabelecido no procedimento para preveni-los e saber como tratá-los, PR-MPR-011 PROCEDIMENTO DE GESTÃO DE INCIDENTES DE SEGURANÇA DE INFORMAÇÕES, estas diretrizes foram divulgadas e socializadas com todos os colaboradores nos diferentes processos da organização, a fim de garantir um reporte tempestivo destes incidentes, e também fornecer tratamento de forma ágil, gerando um RELATÓRIO DE INFORMAÇÕES FO-MPR-025 INCIDENTES DE SEGURANÇA

16. OBRIGAÇÕES DOS FUNCIONÁRIOS

a. Manter absoluto sigilo, mesmo após o término do contrato de trabalho, sobre: procedimentos, métodos, características, lista de clientes, chaves de segurança, suprimentos, softwares, banco de dados de qualquer natureza, valores de bens e serviços, informações técnicas e financeiras, econômicas ou comerciais do contratante ou de seus clientes e outros que a WORLD TRAVEL ASSIST LATAM S.A.S utilize no desenvolvimento de seu objeto social perante clientes ou terceiros.

Parágrafo Primeiro: O descumprimento desta obrigação não é apenas causa de extinção dos vínculos trabalhistas existentes entre as partes, mas poderá ensejar a instauração de ações judiciais contra o Trabalhador pelos danos materiais e imateriais causados, além da cobrança da cláusula penal, que será descrita mais adiante.

B. Não exercer atos de concorrência desleal contra a WORLD TRAVEL ASSIST LATAM S.A.S, pelo que o Trabalhador compromete-se a não utilizar, mesmo após o término do contrato de trabalho, para si ou em benefício de terceiros: a lista de clientes, base de dados de qualquer espécie. Software ou procedimentos, chaves secretas, métodos, características, estudos, estatísticas, projetos, suprimentos utilizados pela WORLD TRAVEL ASSIST LATAM S.A.S interna e externamente perante seus clientes ou terceiros, informações técnicas, financeiras, econômicas ou comerciais da WORLD TRAVEL ASSIST LATAM S.A.S ou de seus clientes.

Parágrafo Segundo: É obrigação do Trabalhador devolver imediatamente, no término do seu contrato, a relação de clientes, senhas, bancos de dados, equipamentos, informações técnicas, financeiras, econômicas ou comerciais e tudo mais que o Trabalhador da WORLD TRAVEL ASSIST LATAM possua. .S.A.S, e que recebeu para poder realizar o seu trabalho.

Parágrafo Terceiro: O descumprimento desta obrigação não é apenas causa de extinção do vínculo empregatício existente entre as partes, mas pode levar à instauração de ações judiciais contra o Trabalhador pelos danos materiais e imateriais que causa, além da cobrança da cláusula penal descrita abaixo.

b. Adotar todas as precauções necessárias e adequadas para salvaguardar a confidencialidade da informação detida pelo Trabalhador da Empresa, ou seja, lista de clientes, base de dados de qualquer espécie, seu software, ou procedimentos, chaves secretas, métodos, características, estudos, estatísticas, projetos,. fornecimentos utilizados pela WORLD TRAVEL ASSIST LATAM S.A.S interna e externamente perante seus clientes ou terceiros, informações técnicas, financeiras, econômicas ou comerciais da WORLD TRAVEL ASSISTLATAM S.A.S ou de seus clientes.

Parágrafo Quarto: A omissão do Trabalhador em impedir o vazamento de informações confidenciais ou exclusivas da empresa, ou seja, lista de clientes, banco de dados de qualquer natureza, softwares, ou procedimentos, chaves secretas, métodos, características, estudos, estatísticas, projetos, fornecimentos utilizados pela WORLD TRAVEL ASSIST LATAM S.A.S interna e externamente perante seus clientes ou terceiros, informações técnicas, financeiras, econômicas ou comerciais da WORLD TRAVEL ASSIST LATAM S.A.S ou de seus clientes, constituem motivo de demissão com justa causa, sem prejuízo das ações contra eles pelos danos causados e a cobrança de sanções pelo descumprimento, além da cláusula penal pelo descumprimento.

17. SANÇÕES POR NÃO CONFORMIDADE

Além de ser motivo de rescisão da relação contratual por descumprimento de alguma das obrigações especiais que o Trabalhador tem por meio deste Acordo de Confidencialidade, dará direito à WORLD TRAVEL ASSIST LATAM S.A.S de exigir, como Cláusula Penal, a soma de 10 (dez) salários mínimos mensais legais vigentes, penalidade que poderá ser exigida por via executiva, para a qual se aceita que esta cláusula e o acordo contido neste acordo constituam obrigação clara, expressa e exigível, que proporciona mérito executivo no nos termos do Código de Processo Civil, sem prejuízo de todas as ações judiciais para cobrança dos danos causados à WORLD TRAVEL ASSIST LATAM S.A.S. Sendo a cláusula penal pactuada uma pena ou sanção, poderão ser exigidas tanto a pena como a indenização por eventuais danos.

20. VIGÊNCIA

Esta política será mantida ao longo do tempo, independentemente do término do vínculo empregatício ou de qualquer tipo, pois seu descumprimento causará danos à WORLD TRAVEL ASSIST LATAM S.A.S e lhe dará o direito de cobrar a cláusula penal estabelecida pelo único fato do seu descumprimento e sem prejuízo das ações judiciais do caso pelos danos causados.
A alta administração nomeia o diretor-geral e o diretor de melhoria de processos para revisar e/ou atualizar as políticas anualmente, ou sempre que necessário.

21.APROBAÇÃO

Este manual de políticas foi estabelecido e aprovado pela administração em 25 de outubro de 2023

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