POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

CÓDIGO:	**PSI 01**
VERSÃO:	1.0
DATA DA VERSÃO:	20/01/2023
CRIADO POR:	RMSAfe
APROVADO POR:	
NÍVEL DE CONFIDENCIALIDADE:	**INTERNO/EXTERNO**

HISTÓRICO DE ALTERAÇÕES

DATA	VERSÃO	CRIADO POR	DESCRIÇÃO DA ALTERAÇÃO
20/01/2023	1.0	RMSAfe	DOCUMENTAÇÃO INICIAL DA POLÍTICA

S U M Á R I O

1. INTRODUÇÃO

Os primeiros passos para a implementação de uma **Política de Segurança da Informação**, definida e aprovada pelo Comitê de Privacidade. A eficácia deste documento depende da combinação de requisitos do negócio, de estrutura de processos, do uso de tecnologias e mecanismos de proteção e, o mais importante, depende do comportamento de seus colaboradores e prestadores de serviço, independentemente do nível hierárquico ou da atividade desenvolvida para ampliar a cultura de segurança da informação e privacidade, alinhada as boas práticas e normas internacionalmente aceitas, criou sua **Política de Segurança da Informação**, a fim de adequá-la à legislação nacional vigente e garantir a proteção de todos os seus ativos tangíveis e intangíveis.

2. OBJETIVOS

Declarar formalmente internamente, por meio da Direção e do Comitê de Privacidade, as diretrizes da WAY DATA que visam à proteção de dados pessoais e informações com eficiência, eficácia e competitividade, de modo seguro, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade, assim como dos ativos de TI que as sustentam, de forma alinhada aos requisitos legais.

Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da WAY DATA como resultado de falhas de segurança ou violação de dados pessoais.

Esta Política se aplica a todos os colaboradores da WAY DATA, estagiários, parceiros, fornecedores, terceiros, prestadores de serviços e visitantes.

3. DIRETRIZES GERAIS

A WAY DATA por meio dessa Política, busca:

- ✓ Assegurar o cumprimento de todas as suas obrigações legais, para atender aos requisitos regulamentares e contratuais pertinentes às suas atividades, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD), 13.709 de agosto de 2018.
- ✓ Empregar medidas técnicas e organizacionais adequadas no tratamento de dados pessoais, e envidar esforços para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses.
- ✓ Garantir a confidencialidade, integridade e disponibilidade das informações de seus clientes e da própria WAY DATA, protegendo os

sistemas de informação contra acessos indevidos e modificações não autorizadas;

- ✓ Assegurar que somente pessoas autorizadas tenham acesso às instalações da WAY DATA, às informações e aos sistemas de informação;
- ✓ Conscientizar as pessoas das possíveis consequências para a WAY DATA e para os seus colaboradores, sobre incidentes de segurança da informação ou violação as políticas de segurança e privacidade;
- ✓ Garantir a continuidade de seus negócios, protegendo os processos críticos contra falhas ou desastres significativos;
- ✓ Assegurar o treinamento contínuo e atualizado nas políticas e nos procedimentos de segurança da informação e privacidade, enfatizando as obrigações das pessoas pela proteção de dados;
- ✓ Garantir que todas as responsabilidades pela segurança da informação e privacidade, estão claramente definidas e que as pessoas indicadas são competentes e capazes de cumprir com as atribuições;
- ✓ Melhorar continuamente o Programa de Segurança e Privacidade.

4. RISCOS

A não observância dos princípios e diretrizes constantes nesta Política e seus documentos complementares, podem impactar seriamente os clientes da WAY DATA, possibilitar a violação de leis e regulamentos, e afetar negativamente a reputação e a estabilidade financeira da WAY DATA.

Desvios e exceções devem ser tratados pelo Comitê de Privacidade.

5. RESPONSABILIDADES

5.1 COLABORADORES

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT, estagiário, menor aprendiz ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da WAY DATA.

É dever dos colaboradores:

- ✓ Respeitar e cumprir esta **Política de Segurança da Informação** e seus documentos complementares;
- ✓ Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição durante seu horário de trabalho;
- ✓ Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- ✓ Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software;

- ✓ Relatar prontamente à área responsável, qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, violação de dados pessoais, fragilidade, mau funcionamento, presença de vírus etc.;
- ✓ Assegurar que as informações e dados de propriedade da WAY DATA não sejam disponibilizados a terceiros, ou sem a devida autorização por escrito do responsável hierárquico;
- ✓ Comprometer-se em não auxiliar terceiro e ou provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro. **Art. 154**-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)

5.2 RECURSOS HUMANOS / DEPARTAMENTO DE PESSOAS

Ter postura exemplar em relação à segurança da informação e privacidade, servindo como modelo de conduta para os colaboradores e prestadores de serviço sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a **responsabilidade do cumprimento da PSI e de seus documentos complementares.**

Exigir dos colaboradores a assinatura do **Termo de Confidencialidade**, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da WAY DATA.

Antes de conceder acesso às informações da WAY DATA, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

5.3 TECNOLOGIA DA INFORMAÇÃO

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes e violação de dados pessoais.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a WAY DATA.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

Proteger continuamente todos os ativos de informação da WAY DATA contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

5.4 JURÍDICO

Atuar previamente nos processos, validando as minutas que devem estar alinhadas aos controles de segurança da informação e privacidade aplicáveis, especialmente os Termos de Confidencialidade.

Fornecer ao Comitê orientações a respeito da conformidade legal nos seguintes temas:

a) Direitos de propriedade intelectual;
b) Proteção de registros organizacionais;
c) Proteção de dados e privacidade de informações pessoais;
d) Prevenção de mau uso de recursos de processamento de informação;
e) Segurança da Informação e Comunicação;
f) Guarda de registros de conexão e dados cadastrais; e
g) Combate a corrupção.

6. BACKUP E CÓPIAS DE RESTAURAÇÃO

Critérios de utilização:

Conforme estipulado pela Política de Segurança da Informação, a execução de backup das informações, incluindo dados pessoais e sistemas da WAY DATA deve, essencialmente, garantir a proteção do atributo da disponibilidade.

Devem ser igualmente preservadas a confidencialidade e a integridade dos backups realizados.

Para que seja possível atender as diferentes necessidades de salvaguarda de informações e sistemas, os backups serão executados mediante o emprego de variadas:

- ✓ Ferramentas, tais como, mas não se limitando a, drivers de gravação, robôs de controle de fitotecas, servidores de storage, nuvem e softwares de gerenciamento de rotinas de Backup; e
- ✓ Mídias, tais como, mas não se limitando a, a fitas magnéticas (DAT, DLT, DDS) e discos óticos (HDs; CDs, DVDs, Blurays, etc.).

Devido à instabilidade para o armazenamento de longo prazo, microcircuitos ou memórias de computador (especialmente Pendrives), não deverão ser empregadas como mídias de backup.

Rotinas de backup

Ao processo recorrente de realização de salvaguarda de informações, dados pessoais, sistemas, bases de dados, diretórios ou mesmo ao conteúdo integral de servidores de rede, para os fins desta Política será empregado o termo rotina.

Toda rotina de execução de backups deve ser definida pela TI a partir:

Da criticidade da disponibilidade de uma Informação e/ou Sistema para a normalidade/continuidade dos processos de negócio e operacionais da WAY DATA, mediante a classificação realizada pelo Gestor da Informação;

Toda rotina de execução de backups deve especificar e definir claramente:

- ✓ Quais as Informações e/ou os Sistemas que deverão ser salvaguardados conjuntamente em uma mesma rotina (Conteúdo Programado);
- ✓ O local onde as informações e/ou sistemas se encontram armazenadas e/ou instalado o Conteúdo Programado;
- ✓ O nível de acesso necessário para que as rotinas de backup automatizadas sejam capazes de acessar e reproduzir o Conteúdo Programado;
- ✓ A frequência da geração das cópias de segurança de modo que os Indicadores de Tempo e Ponto de Recuperação (ITPRs) sejam devidamente atendidos;
- ✓ As ferramentas de backup disponíveis, bem como os tipos de mídias que serão empregadas;
- ✓ O mapeamento da estimativa de duração média das execuções completa (Total) e parcial (Incremental ou Diferencial) da rotina, considerando o tamanho do Conteúdo Programado (incluindo, eventualmente, a taxa de crescimento esperada) frente à capacidade de processamento e velocidade de comunicação dos Ativos de Tecnologia da Informação e Comunicação (ATICs) e das ferramentas específicas de backup envolvidas;
- ✓ Os períodos ideais para execução da rotina, considerando o período de menor carga de utilização e impacto aos processos operacionais (Janela de Execução).

As medidas alternativas/de contorno para os casos em que a execução da rotina ultrapasse a previsão da Janela de Execução ou naqueles em que a mesma falhe parcial ou completamente. A TI, gestora das salvaguardas e dos ATICs da WAY DATA, é responsável por definir os procedimentos/manuais operacionais (passo-a-passo) específicos, de acordo com as características do Conteúdo Programado e das ferramentas de backup, para:

A construção/programação de rotinas automatizadas;

O desempenho das atividades manuais relacionadas à execução das rotinas;

O registro e auditoria da execução bem sucedida das rotinas de backup;

O registro e análise das falhas de execução de rotinas de backup;

O teste e/ou a verificação de consistência, ao menos por amostragem, para a validação das Cópias de Segurança realizadas;
A recuperação (Restore) das informações contidas em backup;
A instalação, configuração e manutenção das ferramentas de backup;
O controle da disponibilidade e da vida útil das Mídias utilizadas e novas, incluindo a previsão orçamentária para aquisição esporádica de novas mídias;
O controle da capacidade da memória e espaço em disco de storages (especialmente se utilizados em estratégia de espelhamento);
O armazenamento seguro e ambientalmente adequado, local e remoto, das mídias de backup, incluindo a eventual geração de cópias redundantes como suporte às estratégias de Contingência Operacional e Continuidade de Negócios; e
O transporte seguro das mídias de backup que permaneçam armazenadas em localidade remota;
O descarte seguro de mídias e ferramentas de backup obsoletas, depreciadas e/ou danificadas, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

O backup de arquivos ou conteúdo de estações de trabalho individuais é, quando necessário, deve ser solicitado pelo colaborador à TI.

Formas de geração de backup

A rotina, poderá ter as seguintes formas de execução do backup:

- ✓ **Total (Full):** Cópia de todo o Conteúdo Programado;
- ✓ **Diferencial:** Cópia apenas das informações modificadas ou geradas após a última cópia Total realizada; ou
- ✓ **Incremental:** Cópia apenas das informações modificadas ou geradas após a última cópia Incremental ou Total realizada.

A inexistência de critérios específicos para a criação de rotinas de backup implicará na adoção dos seguintes critérios de recorrência e retenção:

- ✓ **Diária**: executada na modalidade "diferencial", de segunda-feira a sexta-feira, quando é processada a cópia de segurança semanal.
- ✓ **Semanal:** executada na modalidade "total", aos sábados e domingos, exceto no último domingo do mês, quando é processada a cópia de segurança mensal.
- ✓ **Mensal:** executada na modalidade "total", no último domingo do mês.

Retenção de mídias

As mídias e demais recursos utilizados para armazenamentos dos dados salvaguardados devem ser acondicionados em ambiente separado do de produção, devidamente protegidos contra riscos físicos, como incêndios, intempéries, líquidos, radiação e outras ameaças que possam comprometer a integridade das mídias ou das informações lá contidas.

O meio de armazenamento deve manter condições ideais para as mídias lá mantidas, dentro das recomendações técnicas específicas e melhores práticas de mercado.

Restauração (Restore)

As atividades de restauração das salvaguardas (restore) são responsabilidade da TI, que deve definir os procedimentos e os manuais operacionais para:

- ✓ O mapeamento da estimativa de duração média para a recuperação completa de backups ou de determinados conteúdos solicitados, considerando o seu tamanho, frente à capacidade de processamento e velocidade de comunicação ativos e das ferramentas específicas de backup envolvidas;
- ✓ O encaminhamento, registro e arquivamento das solicitações de restore por colaboradores ou gerentes;
- ✓ A análise da pertinência da solicitação e os requisitos de aprovação aplicáveis;
- ✓ O desempenho das atividades operacionais relativas à recuperação do conteúdo solicitado e de encaminhamento ao solicitante inclusive, quando necessário, mediante transposição em mídia; e
- ✓ Garantir que todas as atividades realizadas no processo de restore disponham de controles de segurança compatíveis, especialmente no que tange ao trânsito e manuseio de mídias, bem como à eliminação segura de qualquer conteúdo temporário/transitório eventualmente gerado.

Testes

Todos os procedimentos supracitados deverão ser periodicamente verificados e testados, visando garantir a eficiência e a efetividade das rotinas de Backup e das atividades de restauração.

Nesse sentido, a seu critério, esporadicamente o Comitê de Segurança da Informação e Privacidade poderá solicitar a realização de backups específicos ou o *restore* de mídias escolhidas aleatoriamente.

Todos os testes devem ser documentados, com a data/hora da execução, responsável pela execução e detalhamento das atividades, se foi concluída com sucesso, sem sucesso, etc.

Responsabilidades da TI

Definir quais serão as ferramentas usadas para realizar as diferentes atividades de backup dos sistemas e informações da Instituição;
Definir as rotinas de execução dos backups de acordo com esta Política;
Definir a necessidade, periodicidade e forma de execução de backup para cada categoria de informações e/ou dados pessoais, mantidos em rede ou em estações individuais;
Definir os procedimentos/manuais operacionais específicos para execução do backup e do *restore*;
Estabelecer mecanismos que garantam a salvaguarda das mídias e recursos utilizados para o armazenamento dos dados;
Executar os procedimentos definidos e zelar pela retenção adequada, integralidade e disponibilidade dos dados guardados.

7. CONTROLES CRIPTOGRÁFICOS

O uso de ferramentas de cifragem e criptografia de dados visa garantir a proteção da confidencialidade, da integridade e da autenticidade das informações da WAY DATA, além do não-repúdio.

A Diretoria de TI tem a responsabilidade exclusiva por adquirir, administrar e fornecer aos colaboradores da organização quaisquer tipos de ferramentas de criptografia que se fizerem necessárias para proteger as informações da mesma.

A Diretoria de TI apoiada pelo Comitê de Privacidade, define quais ativos da WAY DATA precisam ter encriptação de discos, ou qualquer outra ferramenta de criptografia, de acordo com a criticidade do ativo.

As ferramentas de criptografia propostas, deverão ser submetidas à análise e aprovação prévia do Comitê de Privacidade.

Ferramentas de criptografia

As ferramentas de criptografia, sejam simétricas ou assimétricas, deverão:

- Ser adquiridas de fornecedores reconhecidos pelo mercado por sua credibilidade e confiabilidade de seus produtos;
- Empregar algoritmos compatíveis com os padrões internacionalmente reconhecidos;
- Ser realizadas a partir de consultas de especialistas a fim de identificar os controles criptográficos adequados para atender aos objetivos no negócio;
- Empregar tamanhos de chave (em bits) compatíveis com os níveis aceitáveis de resistência a ataques virtuais.

Aplicam-se tais condições, também:

- Às ferramentas de criptografia com código aberto e/ou gratuitas;
- Às ferramentas com funções análogas, tal como a esteganografia;
- Aos recursos de criptografia nativos de sistemas e aplicações adquiridos ou desenvolvidos (internamente ou sob encomenda) pela WAY DATA.

Cabe ao Comitê de Privacidade com apoio da TI, definir os procedimentos de gerenciamento das chaves de criptografia que garantam:

- A geração, armazenamento, arquivo, recuperação, distribuição, retirada e destruição adequada das chaves;
- A proteção das chaves contra modificação e perda;
- O registro e auditoria das atividades relacionadas ao gerenciamento das chaves;
- A definição de datas de ativação e desativação de chaves de forma que possam ser utilizadas apenas por um período de tempo;
- O uso, quando necessário, de um sistema de gerenciamento de chaves, de acordo com as necessidades do negócio.

Se empregada pelos colaboradores, as ferramentas de criptografia devem utilizar obrigatoriamente chaves assimétricas (Public Key Infrastructure) e serem compatíveis com o sistema de gestão de identidades e autenticação, de acordo com as definições estabelecidas pela TI.

USO DAS FERRAMENTAS DE CRIPTOGRAFIA

O uso da criptografia para a comunicação, troca ou transmissão de informações com partes externas, caberá ao **líder do departamento** solicitar formalmente à TI que a assessore na escolha da ferramenta de criptografia mais adequada para proteção das informações da WAY DATA.

A transmissão de informações com partes externas deve usar obrigatoriamente soluções de criptografia com chaves assimétricas (Public Key Infrastructure).

Cabe à TI definir os procedimentos relativos:

- À aquisição/emissão e uso de certificados digitais e a assinatura eletrônica de documentos;
- Ao acesso e o uso de websites que utilizem métodos de criptografia de comunicação baseada em certificados digitais (tais como, SSL e/ou TLS);

- Ao acesso e o uso de túneis criptografados de acesso remoto à Rede (especialmente, a VPN);
- À configuração e uso de recursos de criptografia de dispositivos móveis, nativos ou instalados de forma complementar.

VEDAÇÕES

- É vedada a aquisição de ferramentas de criptografia que utilizem algoritmos proprietários que não tenham sido testados e revisados por grupos de trabalho/estudo de criptologia, mediante comprovação da publicação dos resultados.
- É vedado ao colaborador adquirir para uso profissional ou instalar por conta própria qualquer ferramenta de criptografia não homologada pela TI nos ativos da WAY DATA, ou para cifrar informações da organização.
- Cabe à TI inspecionar os ativos corporativos, incluindo dispositivos móveis, removendo imediatamente qualquer ferramenta e/ou recurso de criptografia que não tenha sido formalmente concedido ou instalado pela WAY DATA.

TRATAMENTO DE INCIDENTES

Caso seja constatado, mediante os controles tecnológicos de monitoramento do ambiente lógico da WAY DATA ou prevenção de vazamento de dados, o recebimento ou envio de qualquer conteúdo criptografado em desconformidade com esta Política, o evento será tratado como um incidente de Segurança da Informação, e se procederá com o seguinte tratamento:

- A TI solicitará formalmente ao gerente do colaborador o esclarecimento do ocorrido;
- A TI realizará cópia dos dados criptografados e o colaborador deverá fornecer os meios necessários para descriptografar o conteúdo, se necessário, mediante o fornecimento das chaves correspondentes;

O caso deve ser reportado formalmente ao Comitê de Privacidade para que este apure as eventuais violações e correspondentes penalidades aplicáveis.

8. E-MAIL E OUTROS MÉTODOS DE TROCA DE MENSAGENS

O recebimento de mensagens na caixa postal corporativa pode ocorrer em horário diverso da jornada de trabalho do colaborador, contudo, as solicitações por este canal devem ser executadas no expediente normal, salvo se houver comando expresso que diga o contrário ou em razão de cargo específico.

O acesso ao correio eletrônico institucional (Ex. webmail) pode ficar disponível mesmo em períodos em que o colaborador não esteja efetivamente desempenhando suas atividades profissionais. Nessas hipóteses a prova de requisição de trabalho somente se dará por meio da utilização de meios adequados, conforme os termos dos controles determinados pela Direção.

Não é permitida a utilização de serviços de mensagens particulares para a transmissão ou recebimento de arquivos da WAY DATA ou de comunicações em seu nome.

Da mesma forma, é proibido o uso de serviços de correio eletrônico baseados em tecnologia de nuvem não autorizados ou não homologados previamente pela WAY DATA para finalidade corporativa e/ou transmissão de informações da WAY DATA, a exemplo, mas não se limitando a Gmail, Hotmail, Yahoo, ProtonMail ou plataformas que possibilitem a transmissão de dados e comunicação entre seus usuários, tal qual, mas não somente Facebook, Skype, WhatsApp e Telegram.

Quanto ao uso do correio eletrônico, o colaborador é responsável por:

Verificar o endereço de correio eletrônico escolhido como destinatário para evitar o envio de mensagens para pessoa errada. Contudo, se isso ocorrer, enviar imediatamente outra mensagem solicitando à pessoa que desconsidere a mensagem anterior e a exclua;

Organizar e efetuar a limpeza de sua caixa postal corporativa periodicamente, eliminando mensagens que tenha certeza que não são mais necessárias para comprovação e documentação das atividades e obrigações em que está envolvido ou que sejam consideradas fora do contexto de trabalho, a exemplo de spam ou phishing;

Não enviar mensagens eletrônicas a partir de endereços diferentes do seu próprio ou utilizar endereço de correio eletrônico que não esteja autorizado;

Não falsificar dados de endereçamento, adulterar cabeçalhos para esconder a identidade do remetente e/ou destinatário(s) ou manipular indevidamente o conteúdo de mensagens;

Não utilizar contas de correio eletrônicos de outros colaboradores ou permitir que estes ou quaisquer outros utilizem-se da sua, sendo que, salvo quando o colaborador esteja devidamente autorizado, não será permitida a exploração das caixas postais alheias;

Não divulgar a conta de e-mail fornecido para o recebimento de mensagens pessoais ou de entidades alheias aos interesses da WAY DATA;

Não encaminhar ou retransmitir qualquer conteúdo que não possa aferir a veracidade (boatos) ou qualquer informação impertinente e/ou não relacionada aos interesses profissionais, tais como correntes;

Não abrir anexos de mensagens que contenham as seguintes extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .scr, .cpl, .reg, .dll, .inf ou qualquer outro arquivo executável que represente um risco à segurança;

Não redirecionar a conta de e-mail corporativa para contas de e-mail particular;

Utilizar contas de correio eletrônico externas para a comunicação, manipulação ou transmissão de qualquer informação, incluindo dado pessoal da WAY DATA;

Redigir as mensagens de forma clara, objetiva e formal, apropriadas ao contexto corporativo, evitando uso de palavras ou expressões de conotação subjetiva ou que possam caracterizar excesso de intimidade ou postura não condizente com ambiente de trabalho;

Incluir a assinatura do colaborador remetente, conforme padrão estipulado pela WAY DATA, além do aviso legal (disclaimer) logo abaixo da assinatura do remetente:

“Confidencial. Sujeito a privilégio legal de comunicação Advogado/cliente.

Privileged and confidential attorney/client comunication.”

No momento do término da relação profissional de um colaborador, a Direção deverá proceder imediatamente ao bloqueio da caixa postal corporativa do colaborador.

As mensagens recebidas na caixa postal bloqueada deverão ser redirecionadas ao gerente ou ao colaborador que tenha sido designado para substituir o anterior e uma resposta automática deverá ser configurada para aviso.

A caixa postal utilizada pelo colaborador sem mais relações contratuais com a WAY DATA deverá ser mantida em armazenamento seguro pelo prazo de 5 (cinco) anos, para fins de auditoria e prova legal das obrigações assumidas de acordo com a função executada e a natureza das informações que tinha acesso, observada a criticidade da disponibilidade da informação, os requisitos legais, fiscais e de auditoria.

9. PROTEÇÃO POR ANTIVÍRUS

Um software de antivírus devidamente licenciado deve estar instalado em todos os computadores com atualizações automáticas ativadas.

Aos terceiros é permitido o uso de laptops, smartphones, tablets e outros dispositivos móveis desde que previsto em contrato. Além disto é de inteira responsabilidade dos supramencionados terceiros o licenciamento de todos os softwares instalados nos dispositivos pessoais, manter atualizado e licenciado o programa de antivírus;

Para acessar a Internet através da estrutura de rede WiFi com dispositivo móvel pessoal, o colaborador deve utilizar suas credenciais de acesso cadastrado;

É de responsabilidade do empregado adquirir e manter atualizado o programa de antivírus em seu equipamento.

Goiânia, 20 de janeiro de 2023.

APROVADO POR: