ÍNDICE DE REVISÕES

REVISÃO	STATUS	DESCRIÇÃO
0	AP	Elaboração inicial do documento.

PA - PARA APROVAÇÃO	CA - CANCELADO	PR - PRELIMINAR
PI - PARA INFORMAÇÃO	AP - APROVADO	LI - LIBERADO

REVISÃO	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G
DATA	12/04/2022							
ELABORAÇÃO	CARLOS C.							
ANÁLISE CRÍTICA	ADRIANA S.							
PADRONIZAÇÃO	ADRIANA S.							
APROVAÇÃO	PAULO M.							

Sumário

1. ATA DE APROVAÇÃO

A ata de aprovação desta política encontra-se devidamente assinada e arquivada na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, acessível a todos os públicos.

URL de Acesso: https://univoce.com.br/enrol/index.php?id=46

2. ABRANGÊNCIA

Abrangência interna e externa, para todos os colaboradores, clientes, fornecedores, parceiros e demais utentes que queiram conhecer esta Política.

3. POLÍTICA

3.1 Introdução

3.1.1 A Política de Segurança da Informação está baseada nas recomendações da Agência Nacional de Proteção de Dados (ANPD) sobre segurança da informação em pequenas empresas e nos controles da norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como código de boas práticas para controles de segurança da informação;

3.1.2 Essa política deverá ser seguida pela Diretoria e por todos os colaboradores da empresa em conjunto com as regras previstas na Política de Privacidade e Proteção de Dados Pessoais e na Política de Segurança no Desenvolvimento de Software.

3.2 Propósito

3.2.1 Estabelecer diretrizes e normas de segurança da informação que permitam aos empregados, colaboradores e prestadores de serviço da empresa adotar padrões de comportamento seguro, adequados às metas e necessidades da empresa;

3.2.2 Orientar quanto à adoção de controles e processos para atendimento dos requisitos de segurança da informação a serem seguidos dentro da empresa;

3.2.3 Resguardar os ativos de informações da empresa, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

3.2.4 Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, colaboradores, prestadores de serviço, clientes e parceiros;

3.2.5 Minimizar os riscos de perdas financeiras, de redução de participação no mercado, de redução da confiança dos clientes ou de qualquer outro impacto negativo no negócio da empresa como resultado de falhas de segurança.

3.3 Escopo

Esta política se aplica a todos os usuários da informação, incluindo qualquer indivíduo ou organização que possua ou tenha possuído vínculo com a empresa, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuam ou venham a possuir acesso às informações da empresa e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da empresa.

3.4 Classificação da Informação

3.4.1 As informações tratadas pelos setores devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

- **Pública:** informações aprovadas pelo seu responsável para consulta irrestrita e cuja sua divulgação externa não compromete o negócio da organização;
- **Interna:** informações disponíveis para a execução de suas tarefas rotineiras, não se destinando, portanto, ao público externo;
- **Confidencial:** informações de acesso restrito a um colaborador ou a um grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros;
- **Restrita:** informações de acesso restrito a um colaborador ou grupo de colaboradores **que obrigatoriamente constam como destinatários**, em geral, associadas ao interesse estratégico da organização e restrita a superintendentes, gerentes, supervisores e funcionários cujas funções demandem conhecê-las.

3.5 Medidas necessárias para o cumprimento da Política de Segurança da Informação

3.5.1 Os colaboradores devem assumir uma postura proativa no que diz respeito à proteção das informações da empresa e devem estar atentos às ameaças, bem como fraudes, sabotagens, roubos de informações e acessos indevidos aos sistemas de informação;

3.5.2 As informações não podem ser transportadas em qualquer meio físico sem as devidas proteções;

3.5.3 Assuntos confidenciais são de uso exclusivo e não devem ser expostos publicamente;

3.5.4 A empresa se compromete a adotar sistemas de controles de segurança da Informação que deverão sempre ser aperfeiçoados objetivando reduzir os riscos de segurança da informação presentes em suas operações.

3.6 Segurança da informação em aplicativos e softwares

3.6.1 O usuário somente pode utilizar aplicativo homologado pelo setor de Tecnologia da Informação (TI), que seja adquirido, desenvolvido internamente ou de propriedade de terceiros;

3.6.2 É expressamente vedada a instalação e o uso de software não licenciado (pirata) nas instalações da empresa;

3.6.3 Os termos de licença de aplicativos de uso corporativo devem ser mantidos pelo setor de TI. Não havendo termo, deve existir documento que comprove a legalidade do aplicativo;

3.6.4 Qualquer necessidade de aquisição de aplicativos identificada por um setor deve ser submetida ao setor de TI para homologação e inventário;

3.6.5 O controle de acessos de todos os aplicativos, sejam eles dedicados ou não, passa a ser de responsabilidade compartilhada entre o setor de TI e o gestor de setor, caso o aplicativo a ser utilizado seja de gestão direta do gestor de setor, cabendo, neste caso ao último, a criação e extinção de novos usuários, bem como mudanças de perfil de acessos. Aplicativos sob gestão exclusiva do setor de TI passam a ser de responsabilidade única e exclusiva deste setor;

3.6.6 Os usuários não podem utilizar ou mesmo armazenar jogos, aplicativos de entretenimento, arquivos com imagens gráficas e filmes não relacionados ao trabalho;

3.6.7 Aplicativos de propriedade ou licenciados pela empresa não podem ser copiados pelos usuários.

3.7 Segurança da informação no que diz respeito ao armazenamento e compartilhamento de arquivos

3.7.1 O usuário não poderá criar ou remover arquivos nos discos dos servidores, fora da área especificamente alocadas para ele no setor;

3.7.2 Materiais não relacionados às atividades da empresa não poderão ser gravados, compartilhados, distribuídos, nem utilizar, de qualquer forma, os recursos computacionais da instituição;

3.7.3 Não é permitido o armazenamento de arquivos de músicas, vídeos que não sejam de atividades de trabalho, conteúdo pornográfico, profano, obsceno, fraudulento, difamatório e racialmente ofensivo. Todo e qualquer material citado acima que for encontrado na rede ou localmente na estação do usuário incorrerá nas medidas disciplinares a serem aplicadas pelo Comitê Gestor de Proteção de Dados Pessoais da empresa.

3.7.4 Não é permitido o compartilhamento de pastas nos computadores de colaboradores. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando-se para as permissões de acesso.

3.8 Segurança da informação no uso de correio eletrônico (e-mail)

3.8.1 A troca de mensagens entre usuários via correio eletrônico deve estar relacionada a assuntos de interesse da organização;

3.8.2 É vedada a utilização do correio eletrônico para envio de correntes, piadas, arquivos contendo imagens e figuras não relacionadas ao trabalho realizado dentro da empresa, bem como sua utilização com propósitos comerciais, religiosos, políticos ou outros quaisquer não relacionados aos interesses e negócios da organização;

3.8.3 É proibido enviar, transmitir, manusear ou disseminar informações sigilosas, segredos de negócio ou qualquer outra informação confidencial da empresa. A violação a esta regra implicará em aplicação de punição pelo Comitê Gestor de Proteção de Dados Pessoais;

3.8.4 É proibido acessar a caixa postal de outro usuário sem a sua autorização, exceto em casos de auditoria, investigação de procedência e desligamentos de colaboradores realizados pelos setores competentes;

3.8.5 É responsabilidade do usuário o acompanhamento diário e a leitura dos e-mails em sua caixa postal, bem como exclusão periódica de mensagens não utilizadas;

3.8.6 Mensagens eletrônicas suspeitas recebidas por link de acesso, anexos ou qualquer outro tipo de arquivo devem ser excluídos ou, em caso de dúvidas, consultar o setor de TI antes de realizar qualquer ação;

3.8.7 Para evitar extrapolação do limite máximo de seu espaço em disco, bem como o acúmulo de arquivos desnecessários no servidor, comprometendo dessa forma o desempenho do correio, o usuário deve proceder à limpeza em suas pastas de itens não usados ou antigos, caso não seja efetuada a limpeza, o usuário ficará impossibilitado de enviar e receber novas mensagens;

3.8.8 Somente os usuários autorizados pelos respectivos gestores de setor poderão enviar mensagens via correio eletrônico para fora da organização.

3.8.9 Somente os usuários autorizados pelos respectivos gestores de setor poderão acessar o correio eletrônico após o horário de expediente.

3.9 Segurança da informação na estação de trabalho

3.9.1 O usuário não pode apagar arquivos do sistema operacional, de programas e aplicativos instalados em sua estação de trabalho;

3.9.2 O usuário deve zelar pela conservação dos equipamentos de informática sob sua responsabilidade;

3.9.3 O usuário não pode instalar ou remover programas em sua estação de trabalho sem a devida autorização e orientação do gestor de setor e do setor de TI;

3.9.4 O usuário não poderá efetuar qualquer alteração nas configurações de hardware (peças) dos equipamentos de informática;

3.9.5 Ao deixar a sua estação de trabalho, o usuário deverá bloquear o acesso à sua máquina (Windows + L) para evitar que sua estação de trabalho esteja em risco;

3.9.6 O usuário não deve deixar anotações com informações sensíveis ou qualquer outro dado em arquivos físicos em cima da sua mesa de trabalho;

3.9.7 Nenhuma informação confidencial deve ser deixada à vista, seja em papel, mídias (CD, pen drive, HD externo), dispositivos, eletrônicos ou qualquer outro meio que seja de fácil acesso;

3.9.8 Nunca escrever senhas em lembretes, cadernetas ou qualquer outro meio que seja de fácil acesso e possa violar a confidencialidade da informação.

3.10 Segurança da informação nos equipamentos de informática

3.10.1 Equipamentos de informática só devem ser adquiridos mediante estudo de investimento, homologação e/ou parecer técnico do setor de TI. Este procedimento visa fazer adequações em casos que possam causar impacto ao ambiente tecnológico.

3.10.2 Os processos de aquisição que não forem submetidos ao setor de TI devem ser anulados e considerados como sem validade, inclusive poderão ficar sem qualquer suporte do setor de TI;

3.10.3 Equipamentos de propriedade de terceiros estão obrigatoriamente sujeitos a procedimentos de segurança específicos, relativos ao controle de vírus e ao controle de acesso lógico à rede corporativa;

3.10.4 Somente podem ser conectados à rede corporativa equipamentos configurados e homologados pelo setor de TI;

3.10.5 A movimentação de equipamentos de informática somente poderá ser feita pelo setor de Logística/Almoxarifado, mediante prévia solicitação e abertura de chamado;

3.10.6 A configuração de equipamentos de informática somente pode ser feita pelo setor de TI, mediante prévia solicitação e abertura de chamado;

3.10.7 Todos os equipamentos de informática de propriedade da empresa devem ser inventariados pelo setor de Logística/Almoxarifado.

3.11 Segurança da informação no que diz respeito ao acesso externo (remoto)

3.11.1 O acesso remoto à rede corporativa será provido mediante solicitação ao setor de TI via sistema de chamados informando data e horário de início e término do acesso e também os motivos.

3.11.2 O acesso remoto à rede corporativa deverá ser realizado preferencialmente através de VPN (Virtual Private Network) sendo os demais casos tratados diretamente com o setor de TI;

3.11.3 As credenciais de acesso remoto do usuário são de uso exclusivo e intransferível;

3.11.4 O usuário deve fechar a sessão de trabalho após conclusão das atividades evitando a exposição de informações a pessoas não autorizadas.

3.11.5 Acessos remotos serão auditados pelo setor de TI.

3.12 Segurança da informação na utilização da internet

3.12.1 A liberação do acesso à internet será concedida a todos os colaboradores da empresa que necessitem fazer uso de ferramentas corporativas disponibilizadas na internet;

3.12.2 O usuário não poderá utilizar recursos da empresa para distribuir software não legalizado;

3.12.3 A empresa se reserva ao direito de gerar relatórios demonstrativos dos sites visitados pelos usuários e de bloquear acesso àqueles cujos conteúdos não sejam compatíveis com as atividades de trabalho;

3.12.4 O usuário não poderá acessar sites que contenham conteúdo pornográfico, profano, obsceno, fraudulento, difamatório, racialmente ofensivo, websites de bate-papo, jogos, sites de relacionamento, redes sociais, dentre outros que não sejam para uso exclusivo das atividades de trabalho;

3.12.5 O usuário não poderá utilizar softwares e/ou websites com o intuito de burlar o sistema de controle de acesso à internet para acessar conteúdos não autorizados;

3.12.6 É importante ressaltar que, mesmo que um determinado website não esteja bloqueado, não significa que este possa ser acessado pelos usuários. Observar-se-ão todos os preceitos desta política, desde a proibição de acesso a websites indevidos, contrários à lei da moral e dos bons costumes, ao uso da internet para assuntos que não são pertinentes às rotinas de trabalho;

3.12.7 Caso haja necessidade de acesso a algum website que esteja bloqueado e este seja relacionado a assuntos de trabalho, o usuário poderá recorrer ao seu gestor imediato para que este tome ciência e solicite liberação de acesso ao setor de TI.

3.13 Segurança da informação no que diz respeito ao uso da rede wireless - corporativa

3.13.1 Apenas equipamentos com código de patrimônio da empresa serão inseridos na rede wireless - corporativa da empresa.

3.13.2 É expressamente proibido que clientes ou fornecedores realizem a conexão de dispositivos em redes corporativas da organização.

3.14 Segurança da informação no que diz respeito ao uso da rede wireless – visitantes

O acesso à rede wireless - visitantes estará disponível para funcionários e visitantes, lembrando que o usuário será monitorado e deve seguir as regras de utilização da EMPRESA.

3.15 Segurança da informação na definição de logins e senhas

3.15.1 As senhas dos usuários são pessoais e intransferíveis, pois asseguram que apenas ele, devidamente identificado, as utilize e as mantenha de acordo com as necessidades de acesso aos sistemas;

3.15.2 O usuário não deve escolher senhas óbvias, baseadas em nomes próprios, datas de aniversários, siglas conhecidas, nome da organização, data de nascimento, etc.;

3.15.3 É recomendada a alteração da senha de acesso à estação de trabalho a cada seis meses por medidas de segurança, seguindo orientações para que a senha contenha, no mínimo, oito caracteres com letra maiúscula, números e com, no mínimo, um caractere especial;

3.15.4 Colaboradores e terceiros devem ter suas chaves de acesso bloqueadas, de acordo com a data de expiração do contrato de trabalho firmado;

3.15.5 Cadastro de novos usuários, inativação de acessos, mudança de função, devem ser registrados em chamado pelo setor de Desenvolvimento Humano e Organizacional (DHO);

3.15.6 Senhas de uso compartilhado por um ou mais setores devem ser de uso restrito desses setores, não devendo ser divulgadas a outrem sem as devidas permissões dos respectivos gestores.

3.16 Segurança da informação no que diz respeito ao uso de dispositivos móveis

3.16.1 É expressamente proibida a utilização de dispositivos móveis para atividades particulares ou que não são de interesses da organização;

3.16.2 O acesso à rede corporativa através de dispositivos móveis apenas pode ser realizado mediante o registro de chamado pelo gestor de setor com justificativa plausível. É de responsabilidade do setor de TI a liberação do acesso.

3.17 Papéis e Responsabilidades

3.17.1 Comitê Gestor de Proteção de Dados Pessoais

As funções e atribuições do Comitê Gestor de Proteção de Dados Pessoais estão definidas na Política de Privacidade e Proteção de Dados Pessoais da empresa.

3.17.2 Gestores de Setor

É responsabilidade dos gestores de setor:

- Gerenciar as informações geradas ou sob a responsabilidade de seu setor durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte, conforme as normas estabelecidas pela empresa;
- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme os critérios descritos no item 4 desta política;
- Periodicamente, revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das documentações de acordo com o item 3.4 desta política;
- Autorizar e revisar os acessos à informação e/ou a sistemas de informação sob sua responsabilidade;
- Solicitar a concessão ou revogação de acesso à informação e/ou a sistemas de informação de acordo com os procedimentos adotados pela empresa.

3.17.3 Usuários da Informação

É responsabilidade dos usuários da informação:

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação da empresa, suas normas e procedimentos ao encarregado de dados pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais;
- Comunicar aos gestores de setor qualquer evento que viole esta política ou coloque ou possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da empresa;
- Assinar o Termo de Uso dos Sistemas da Informação da empresa, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
- Responder pela inobservância da Política de Segurança da Informação, além de normas e procedimentos de segurança, conforme definido no item 3.19 Sanções e Punições.

3.18 Auditorias Internas

3.18.1 Para verificação do cumprimento das normas definidas nessa e nas demais políticas internas, será responsável o setor de Auditoria Interna, que poderá implementar rotinas, eventuais ou programadas, de auditoria.

3.18.2 Será de responsabilidade dos gestores de setor contribuir para a realização das auditorias citadas no item anterior fornecendo todos os dados necessários aos responsáveis pela sua realização.

3.19 Sanções e Punições

3.19.1 As violações, mesmo que por mera omissão ou tentativa não consumada desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

3.19.2 A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Proteção de Dados Pessoais, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê Gestor de Proteção de Dados Pessoais, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

3.19.3 No caso de terceiros contratados ou de prestadores de serviço, o Comitê Gestor de Proteção de Dados Pessoais deverá analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

3.19.4 Para o caso de violações que impliquem em atividades ilegais ou que possam incorrer em dano à empresa, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

3.20 Casos Omissos

3.20.1 Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação;

3.20.2 As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da empresa adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da empresa.

3.21 Glossário

3.21.1 **Ameaça**: causa potencial de um incidente que pode vir a prejudicar a empresa;

3.21.2 **Ativo**: tudo aquilo que possui valor para a empresa;

3.21.3 **Ativo de informação**: patrimônio intangível da empresa, constituído por suas informações de qualquer natureza, incluindo as de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos ou legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas à empresa por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenadas, trafegadas ou transitadas pela infraestrutura computacional da empresa ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico ou mídia eletrônica transitados dentro e fora de sua estrutura física.

3.21.4 **Comitê Gestor de Proteção de Dados Pessoais**: grupo de trabalho multidisciplinar permanente, efetivado pela Diretoria da empresa, que tem por finalidade tratar questões ligadas à segurança da informação.

3.21.5 **Confidencialidade**: propriedade dos ativos da informação da empresa de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

3.21.6 **Controle**: medida de segurança adotada pela empresa para o tratamento de um risco específico.

3.21.7 **Disponibilidade**: propriedade dos ativos da informação da empresa de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

3.21.8 **Incidente de segurança da informação**: evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da empresa.

3.21.9 **Integridade**: propriedade dos ativos da informação da empresa de serem exatos e completos.

3.21.10 **Risco de segurança da informação**: efeito da incerteza sobre os objetivos de segurança da informação da empresa.

3.21.11 **Segurança da informação**: preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da empresa.

3.21.12 **Usuário da informação**: empregados com vínculo empregatício de qualquer área da empresa ou terceiros alocados na prestação de serviços da empresa, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar ou manipular qualquer ativo de informação da empresa para o desempenho de suas atividades profissionais.

3.21.13 **Vulnerabilidade**: causa potencial de um incidente de segurança da informação que pode vir a prejudicar as operações ou ameaçar as informações da empresa.

3.22 Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Proteção de Dados Pessoais.

3.23 Gestão da Política

3.23.1 A Política de Segurança da Informação é aprovada pela Diretoria da empresa, em conjunto com o Comitê Gestor de Proteção de Dados Pessoais.

3.23.2 Essa Política precisa estar atualizada em sua última versão na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, conforme acesso anteriormente citado.

4. DIRETRIZES

4.1 Objetivo

O objetivo da gestão de segurança da informação da empresa é garantir um gerenciamento sistemático e efetivo de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos para a instituição.

4.2 Atribuições e Responsabilidades

A Diretoria Executiva e os gestores de setor devem estar comprometidos com uma gestão efetiva de segurança da informação dentro da empresa. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da empresa.