POL 001- Política de Segurança da Informação

Dezembro 2023

Sumário

1. Objetivo

Orientar e estabelecer o padrão de Segurança da Informação da Unidas, fornecendo as diretrizes de conduta aos colaboradores, terceiros e prestadores de serviços da Unidas no uso adequado e seguro de recursos de informação, assim como as responsabilidades e deveres de todos os envolvidos nas atividades da empresa.

Todas as diretrizes estabelecidas neste documento são construídas para preservar os três aspectos básicos de segurança, sendo eles:

a) **Confidencialidade:** É o aspecto relacionado a divulgação não autorizada, acesso e uso indevido da informação corporativa;

b) **Integridade:** A propriedade de que a informação não foi modificada ou corrompida, ou seja, preserva sua exatidão; e

c) **Disponibilidade:** A propriedade de que a informação esteja disponível para o uso devido dos usuários autorizados.

2. Âmbito de Aplicação

2.1 A presente Política aplica-se à Unidas Locações e Serviços S.A., Unidas Valoriza Ltda, Unidas Locadora S.A., e demais entidades controladas, cada uma delas doravante designada simplesmente por “Empresa” ou “Unidas”.

2.2 O conteúdo desta Política é aplicável e deve ser conhecido e cumprido por todos os colaboradores sem distinção de cargo ou função, sendo o seu descumprimento passível de aplicação das medidas legais e disciplinares mencionadas no Código de Conduta Ética Profissional da Unidas, terceiros e partes externas da Unidas e das organizações subsidiárias.

3. Considerações Gerais

3.1 O conteúdo desta Política é propriedade da Unidas e é destinado para uso e divulgação pública.

3.2 Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente Política, os colaboradores, terceiros e prestadores de serviço devem consultar o seu gestor imediato ou a área de Segurança da Informação.

3.3 Esta Política dá ciência de que, os ambientes, sistemas, computadores, e-mails, internet e redes (privadas e pública), poderão ser monitorados.

3.4 Os casos omissos serão decididos pelo Gerente Geral da Segurança da Informação.

4. Vínculos / Documentação Complementar

Além das diretrizes estabelecidas na presente Política, os seguintes documentos complementam e detalham as regras vinculadas a Segurança da Informação:

POL-I TI 009 Política de Continuidade de Negócios e Gestão de Crises;

POL-I TI 010 Política de Utilização e Controle de Acesso USB em Ativos Tecnológicos (notebooks e desktops);
POL-I TI 011 Política de Conscientização de Segurança da Informação;
POL-I TI 012 Política de Gestão de Riscos de SI de Fornecedores e Parceiros;
POL-I TI 014 Política de Utilização de Recursos Tecnológicos;
POL-I TI 015 Política de Gestão de Patches e Vulnerabilidades;
POL-I TI 016 Política de Desenvolvimento Seguro;
POL-I TI 017 Política de Segurança em Dispositivos Móveis;
POL-I TI 018 Política de Gestão de Acesso Lógico;
POL-I TI 019 Política de Gestão de Incidentes de Segurança; e
Código de Conduta Ética Profissional da Unidas.

5. Conceitos

5.1. BACKUP - Refere-se a cópias de segurança dos dados que são armazenados no ambiente de produção da Unidas, para que possam ser restaurados em caso de perda de dados originais, oriundos de uma exclusão acidental ou corrupção de dados.

5.2. CONTEUDO INADEQUADO/ IMPRÓPRIO - É considerado como inadequado:

a) Ilícitos, conteúdos violentos ou degradantes;

b) Protegido por direitos autorais, segredo comercial, industrial ou de Terceiros, a menos que o usuário tenha permissão do titular de tais direitos para divulgar o conteúdo;

c) Nocivo, abusivo, difamatório, pornográfico, libidinoso ou que de qualquer forma represente assédio, invasão de privacidade ou risco a menores;

d) Que represente assédio, degradação, intimidação ou ódio em relação a um indivíduo ou grupo de indivíduos com base na religião, sexo, orientação sexual, raça, origem ética, idade, deficiência, ou qualquer outra condição;

e) Que inclua informações pessoais ou que permitam a identificação de terceiro sem seu expresso consentimento;

f) Falso, fraudulento, enganoso ou que represente informação enganosa;

g) Que contenha referência a link ilícito, spam, correntes ou esquemas de pirâmide; e

h) Que contenha vírus ou qualquer outro código malicioso, arquivos ou programas projetados para interromper, destruir ou limitar a funcionalidade de qualquer software ou hardware.

5.3. DADOS PESSOAIS - Qualquer informação que identifique ou que permita identificar, direta ou indiretamente um indivíduo.

5.4. DISPOSITIVO MÓVEL - Trata-se do dispositivo de acesso remoto a qualquer dado da Unidas, incluindo, mas não se limitando à smartphone, tablet e notebook.

5.5. INFORMAÇÃO CONFIDENCIAL - Constituem Informações Confidenciais:

a) Dados ou informações da Unidas (ainda que não sejam de propriedade da Empresa, mas que a mesma tenha recebido em razão de uma oportunidade de negócio, por exemplo) ou desenvolvidos pela Unidas e que o colaborador

venha a tomar conhecimento por qualquer forma, incluindo, mas não se limitando a, informações de natureza técnica, comercial, financeira, jurídica, estratégica, tecnológica, know-how, desenhos, modelos, dados, cadastros, especificações, relatórios, compilações, análises, previsões, estudos, reproduções, sumários, comunicados, fórmulas, patentes, dados financeiros e econômicos, informações relacionadas a clientes, fornecedores atuais ou potenciais, operações financeiras, planos comerciais, demonstrações ou planos financeiros, estratégias de marketing e outros negócios, contratos, produtos existentes ou futuros e quaisquer outras informações de propriedade da Unidas reveladas em confiança para o Empregado;

b) Outros dados ou informações necessárias para o exercício das funções do Colaborador relativos à Unidas, incluindo, mas não se limitando aos dados de natureza societária, objetivos de investimentos, estrutura jurídica e segredos de negócio;

c) Todas as anotações, análises, compilações, estudos, materiais ou quaisquer outros documentos elaborados pela Unidas e/ou por seus conselheiros, diretores, administradores, colaboradores, representantes, prepostos, consultores jurídicos, consultores contábeis, consultores financeiros, auditores internos e independentes, que contenham ou reflitam de outra maneira Informações Confidenciais

5.6. INFORMAÇÃO - É todo e qualquer dado, informe, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não com a expressão “confidencial”, em decorrência do desenvolvimento das atividades profissionais da Empresa.

5.7. SEGURANÇA DA INFORMAÇÃO - Refere-se a uma proteção de dados da empresa contra diversas ameaças.

5.8. SOFTWARE - Um software é um serviço computacional utilizado para realizar ações nos sistemas de computadores. Ou seja, um software é todo programa presente nos diversos dispositivos (computadores, celulares, televisores, entre outros).

5.9. TECNOLOGIA DA INFORMAÇÃO (TI) - Conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir o processamento, armazenamento, acesso e uso das Informações.

5.10. TERCEIRO - Excetuando-se os Prestadores de Serviços, conforme definição abaixo, refere-se, mas não se limitando, a todo e qualquer fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, seja pessoa física ou jurídica, independentemente de contrato formal ou não, incluindo aquele que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com o governo ou com outros em nome da Unidas.

5.11. UPLOAD - Ato de enviar um arquivo para a internet, ou seja, envio de dados de um computador local para um computador remoto, fora da rede corporativa.

5.12. USUÁRIO - É todo e qualquer Colaborador, Prestador de Serviço ou visitante que utilize os Recursos de TI disponibilizados pela Empresa.

6. Diretrizes

6.1. Gerais

a) A Informação[1], é propriedade da Unidas, ressalvadas aquelas Informações[1] de terceiros que sejam obtidas pela Unidas através de um acordo de confidencialidade ou documento equivalente, pois são ativos valiosos que devem ser gerenciados com o devido cuidado. As informações da Unidas, devem ser utilizadas exclusivamente para fins empresariais.

b) Não é permitida a cópia de Informações da Unidas sem prévia autorização expressa da área da Segurança da Informação.

6.2. Responsabilidades e Deveres

a) É responsabilidade e dever de todos os colaboradores, terceiros e prestadores de serviços:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da Unidas;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Formalizar a ciência através do aceite da Política e das Normas de Segurança da Informação, assumindo responsabilidade por seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela Unidas;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;
- Tomar todas as medidas razoáveis para garantir a segurança de cópias de Informações Confidenciais;
- Ter discrição ao falar sobre assuntos envolvendo a Unidas em locais públicos, tais como elevadores, copa, restaurantes, aviões ou ao utilizar seu telefone ou e-mail fora do escritório;
- Zelar para que os materiais (documentos, informações utilizadas em salas de reuniões etc.) utilizados internamente não sejam expostos, armazenado, distribuído, editado ou gravado; e
- Reportar imediatamente ao Gestor, todo incidente que coloque em risco a Segurança da Informação.

[1]Informações confidenciais ou não confidenciais

b) É responsabilidade e dever dos gestores:

- Tomar todos os cuidados para que Informações Confidenciais não estejam acessíveis para pessoas não autorizadas;

- O Gestor de cada departamento é o responsável pelas Informações Confidenciais nele produzidas e pela autorização do acesso dos usuários à estas Informações, bem como o armazenamento conforme recursos disponibilizados pelo Departamento de TI para tal.

c) É responsabilidade da área de Segurança da Informação:

- Estabelecer, publicar, manter e disseminar políticas de segurança da informação relevantes;

- Revisar e aprovar materiais de conscientização anualmente ou sempre que houver mudanças significativas; e

- Se reunir regularmente para rever o status corrente da segurança, aprovar e revisar posteriormente projetos de segurança da informação, aprovar políticas de segurança novas ou modificadas e executar outras atividades necessárias de gerenciamento de segurança da informação.

7. Classificação da Informação

a) Toda informação deve ser classificada com base na confidencialidade e níveis que a informação exige, que são eles:

- **Confidencial:** Informações internas a pessoas específicas (nível mais alto de confidencialidade);

- **Restrita:** Informações internas de área específica (nível médio de confidencialidade);

- **Uso Interno:** Somente membros da organização podem ter acesso (nível mais baixo de confidencialidade); e

- **Pública:** Todos podem ter acesso à informação.

b) Toda informação deve possuir um proprietário, papel que é atribuído ao Gerente responsável pela área que produz a informação. O proprietário é responsável por classificar a informação e garantir que esta receba a proteção adequada em todo o seu ciclo de vida.

c) Toda informação classificada deve ser rotulada de modo que evidencie a sua sensibilidade. Na ausência da classificação da informação, o nível restrito deverá ser considerado.

8. Controle de Acesso

a) Deverão ser estabelecidas diretrizes para o controle de acesso e senhas, baseadas nos requisitos de negócios e de segurança. As diretrizes devem ser reavaliadas regularmente e conter as devidas parametrizações e complexidades contendo caracteres maiúsculos, minúsculos, alfanuméricos e especiais.

8.1. Segregação de Funções

a) Funções conflitantes e áreas de responsabilidades devem ser segregadas para reduzir conflitos de acessos indevidos, risco a fraude, proteger ativos da organização e garantir a integridade dos processos e sistemas.

b) Administradores de sistemas devem ser responsáveis por garantir que os controles de acessos e permissões sejam adequadamente documentados, restritos e configurados em sistemas para restringir o acesso em funções e informações específicas, incluindo, mas não se limitando ao monitoramento regular de logs de acesso crítico para identificar possíveis violações.

c) Deve ser delegado a uma área a responsabilidade em identificar os riscos relacionados à segregação de função e na implementação de controles para mitigar esses riscos, incluindo, mas não se limitando a notificar os administradores em melhorias, atualizações e em efetuar revisões periodicamente para avaliar a eficácia das práticas de segregação, identificar vulnerabilidades, fornecer recomendações e garantir a conformidade.

8.2. Autorização para Acesso

a) O acesso aos sistemas de informação deve ser autorizado pelos superiores imediatos, de acordo com as diretrizes do proprietário do sistema de informação. Isto inclui os direitos de acesso e privilégios que os acompanham. As autorizações só devem ser concedidas baseadas na necessidade de conhecimento ou uso regulado por cargo e função.

b) O superior imediato deve solicitar ao administrador do sistema a concessão de acesso e alterações, de acordo com as diretrizes do proprietário do sistema.

8.3. Gerenciamento de Acesso de Usuário

a) Devem ser estabelecidas diretrizes para o controle de acesso e senhas, baseadas nos requisitos de negócios e de segurança. As diretrizes devem ser reavaliadas regularmente, incluindo, mas não se limitando aos parâmetros de senha (frequência da troca, quantidade e tipos de caracteres que podem ser utilizados etc.).

b) O gerenciamento de acesso de usuários deve incluir os seguintes itens:

- Autenticação dos usuários no acesso aos sistemas;
- Combinação única e individual definidas para o nome de usuário e senhas;
- Determinar um prazo para troca de senha; e
- Alertar que o usuário é responsável por qualquer uso de suas credenciais de acesso e senhas e não deve divulgá-las.

9. Política de Senhas

a) O gerenciamento das senhas de acesso aos recursos de processamento de informação deve atender aos seguintes requisitos de segurança:

- Os usuários devem ter a permissão de definir e alterar suas próprias senhas;

- Os usuários devem ser obrigados a definir senhas complexas (contendo caracteres maiúsculos, minúsculos, alfanuméricos e especiais);

- As senhas devem ser compostas por, no mínimo, 8 caracteres;

- As senhas de acesso a servidores e as senhas de contas administrativas ou privilegiadas devem ser compostas por, no mínimo, 8 caracteres;

- As senhas devem expirar a cada 90 dias, com isto ajuda a reduzir a probabilidade de que as senhas se tornem comprometidas por exposição prolongada;

- Os usuários devem ser obrigados a alterar senhas temporárias ao efetuarem o primeiro log-on;

- O bloqueio da conta deve ocorrer após 5 tentativas de logon inválidas;

- Não deve ser permitida a reutilização das últimas 12 senhas;

- As senhas devem ser armazenadas de forma segura e de forma não reversível.

Para os requisitos de segurança em relação a complexidade de senhas citada anteriormente (conter caracteres maiúsculos, minúsculos, alfanuméricos e especial), o sistema Nexxera tem a obrigatoriedade em ter 3 destes 4 parâmetros configuráveis.

b) O uso adequado das senhas garante a preservação da responsabilidade sobre os acessos a sistemas e informações confiados ao usuário, bem como a preservação das informações e negócios da empresa.

c) As seguintes diretrizes devem ser obedecidas pelos usuários:

- Devem ser responsáveis por todas as ações realizadas com as suas contas de acesso e as suas senhas;

- Devem manter suas senhas em sigilo. As senhas são pessoais e intransferíveis;

- Não devem anotar, emprestar ou divulgá-las;

- Não devem deixar lembretes de senhas em teclados, monitores, mesas ou em qualquer outro lugar;

- Devem certificar-se de não estar sendo observado ao digitar uma senha;

- Não devem criar senhas iguais a própria conta, nomes, sobrenomes, datas comemorativas, números de telefones, placas de carros, números de documentos ou outros dados que possam ser facilmente obtidos ou associados à sua pessoa ou atividade;

- Não devem utilizar as mesmas senhas cadastradas em sites de Internet para efetuar cadastros de senhas na Unidas; e

- Devem trocar suas senhas periodicamente para manter suas contas de acesso sempre em segurança.

10. Segurança Física e do Ambiente

a) Áreas que abriguem equipamentos de processamento ou armazenamento de informação são considerados como área segura e precisam ter controle de acesso adequado para garantir que somente as pessoas autorizadas tenham acesso.

b) Essas áreas devem obedecer aos seguintes requisitos:

- Possuir listagem de usuários que precisam do acesso permanente ao ambiente;
- Registro de acesso contendo data, hora, nome, empresa e área;
- Retenção dos logs de acesso por no mínimo 90 dias;
- Revisões trimestrais das pessoas com acesso a essas áreas;
- Possuir sistemas de detecção e combate de incêndio; e
- Equipamentos de prevenção e detecção de acesso não autorizado.

c) Qualquer colaborador que autorizar o ingresso de visitantes na empresa, torna-se responsável pela supervisão destes durante toda a sua permanência na empresa.

10.1. Área de Acesso Restrito

a) As áreas de negócios ou operações da Unidas devem, preferencialmente, restringir o acesso físico. Ficam estabelecidas as seguintes áreas de acesso restrito:

- Centros de Processamento de Dados (“CPD”); e
- Sala de Elétrica.
- Sala estoque de equipamentos tecnológicos;
- Sala Back Bone;
- Locais de hospedagem de data centers, incluindo se terceirizados;

b) Somente colaboradores de TI ou pessoas autorizadas pelo Departamento podem ter acesso a estas áreas restritas e se necessário conceder o acesso, o mesmo deverá ser acompanhado por alguém autorizado.

c) Procedimentos para a autorização de acesso às áreas restritas devem ser estabelecidos, incluindo a aprovação de um gerente responsável.

11. Mesa Limpa e Tela Protegida

a) É necessário que os colaboradores de todos os departamentos da Unidas tenham a consciência em manter suas mesas limpas, sempre organizadas e livres de documentos confidenciais, arquivos ou quaisquer informações sensíveis quando não estiverem em uso.

b) A prática de tela protegida deve ser adotada por todos quando se afastarem de suas estações de trabalho, reduzindo o risco de perda e danos à informação.
c) Papéis, mídias de computadores, agendas, livros ou qualquer material quando não estiverem sendo utilizados, devem ser guardados de maneira adequada, em gavetas ou locais seguros.

d) Informações de usuário e senha de sistemas e/ou rede não podem ser anotadas em papel, ou registradas em meios de fácil acesso.

12. Dispositivos Móveis e Trabalho Remoto

a) Todo acesso remoto deve ser minunciosamente analisado e a sua concessão ocorrerá mediante solicitação formal e aprovação. É necessário que o requisitante assine o termo de responsabilidade de ativos fornecido pela empresa e seja passível de sanções disciplinares e ações cíveis por parte da Unidas.

13. Transferência de Informação

a) Devem ser estabelecidos procedimentos e controles para proteção adequada na geração, manuseio, armazenamento, transporte e descarte de informações.

b) A troca de informações com terceiros, quer sejam clientes ou fornecedores requer o cumprimento de procedimentos acordados com a Unidas.

14. Gestão de Ativos

a) Convém que todos os ativos da informação sejam claramente nomeados a um proprietário, identificados de forma individual, inventariados, protegidos de acessos indevidos, com a documentação e planos de manutenção atualizados sempre que houver mudanças.

15. Política de Antivírus

a) Todos os recursos de informação aplicáveis devem estar configurados com software antivírus aprovados pelo Área de Segurança da Informação. A solução antivírus deve ser capaz de detectar, remover e proteger contra todos os tipos de software malicioso tais como vírus, trojans, worms, spyware, adware e rootkits. O software deve estar configurado para receber atualizações automáticas, executar varreduras periódicas, registrar eventos com vírus em uma solução central de logging, e os usuários finais não devem ser capazes de configurar ou desabilitar o software.

b) Todos os sistemas com software antivírus devem estar configurados para atualizar as assinaturas de vírus e realizar varreduras ao menos semanalmente.

c) O software antivírus deve alertar a Área de Segurança da Informação em tempo real sobre a detecção de qualquer vírus e gravar tais eventos em um servidor de log central.

16. Gestão de Vulnerabilidades

a) A área de Segurança da Informação deve ser informada sobre questões de segurança da informação e vulnerabilidades aplicáveis aos sistemas informáticos da Unidas. Quando problemas de segurança são identificados, a Área de Segurança da Informação é responsável por notificar o pessoal apropriado, incluindo o administrador do sistema.

b) O principal método para identificação de novas ameaças à medida que elas aparecem será através de fornecedores e de listas específicas de segurança na Internet. Apesar de incompletas, as seguintes listas também devem ser subscritas da mesma forma que outras listas de fornecedores aplicáveis aos pacotes de software e sistemas da Unidas:

- CERT;
- NT BUGTRAQ;
- Exploit DB;
- Microsoft Security Content; e
- Outras fontes.

c) Além de identificar novas vulnerabilidades, os membros da Área de Segurança da Informação devem atribuir uma classificação de risco para todas as vulnerabilidades aplicáveis ao ambiente da Unidas. A classificação de risco deve ser utilizada para priorizar atividades como instalação de patches e atualizações de equipamentos. A classificação atribuída a um patch ou vulnerabilidade deve ser baseada em melhores práticas da indústria, tais como o Common Vulnerability Scoring System Versão 2 (CVSSv2). No caso do CVSSv2, uma vulnerabilidade deve ser classificada como “alta” quando alcança uma pontuação maior ou igual a 8.0. Além disso, vulnerabilidades relacionadas a SQL Injection ou Cross-Site Scripting devem ser automaticamente classificadas como “alta”. Sempre que possível, a classificação de risco deve levar em conta a classificação do fornecedor, onde alertas classificados como “crítico”, “execução remota de código” ou “Excepcional”, devem ser classificadas como de alto risco.

d) Além das informações de fontes e listas externas, também deverá ser utilizado ferramentas ou scanners para identificar vulnerabilidades, e estas são classificadas de acordo com o critério atribuído pelo fabricante da ferramenta.

e) As avaliações de fontes de segurança reconhecidas pela indústria também devem ser monitoradas, com todas as vulnerabilidades que podem levar ao comprometimento remoto de sistemas classificadas como alto risco.

17. Backup

a) É necessário que a área de TI realize regularmente os backups e teste de restauração desses backups, bem como o armazenamento dos dados nos sistemas da Unidas de acordo com a sua classificação.

b) Os backups devem ser armazenados externamente ou em uma área separada do arquivo original e apropriadamente protegida, sendo somente acessível por pessoas autorizadas.

18. Restrições Sobre o Uso e Instalação de Software

a) A aquisição, contratação e/ou instalação de equipamentos de TI e software devem ser solicitadas para área de TI.

b) Todos os contratos referentes aos sistemas de TI terceirizados devem incluir:

- Requisitos de segurança da informação, incluindo a confidencialidade, integridade e disponibilidade;

- Uma descrição do nível de segurança acordado;
- Requisitos para a notificação de incidentes de segurança;
- Uma descrição de como a Unidas pode garantir que terceiros estão cumprindo seus contratos;
- Uma descrição do direito da Unidas para auditar terceiros.

19. Segurança em Recursos Humanos

a) A área de Recursos Humanos da Unidas é responsável em emitir e controlar os documentos físicos dos colaboradores, incluindo mais não se limitando ao termo de confidencialidade assinado e o conhecimento sobre a disponibilidade das políticas e procedimentos relacionados à Segurança da Informação.

20. Conscientização em Segurança da Informação

a) Todos os colaboradores devem receber treinamento adequado, a fim de conscientizar e ser atualizado sobre a política e procedimentos da Unidas.

b) Os colaboradores devem participar do processo de integração para que tenham o conhecimento das Políticas e Procedimentos gerais em relação à Segurança da Informação, bem como o uso correto dos recursos de processamento da informação, confidencialidade e sigilo de assuntos pertinentes a organização, acesso somente a sistemas autorizados, sigilo de senhas de acesso, prática de mesa limpa e tela protegida, descarte seguro de informação etc.

c) As campanhas corporativas de conscientização de Segurança da Informação devem ser realizadas para que todos os colaboradores reconheçam a importância dos aspectos de Segurança da Informação e como contribuir para estes processos.

21. Relacionamento da Cadeia de Suprimentos

a) A Unidas deve assegurar a proteção dos ativos da organização e que são acessados pelos fornecedores. Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

b) A gestão da cadeia de suprimentos não se restringe à movimentação de materiais, mas também presume em uma troca eficiente de informações, permitindo ações coordenadas.

22. Conformidade com Requisitos Legais e Contratuais

a) A Unidas deve cumprir a legislação, bem como outras diretrizes externas, como por exemplo:

- As leis e regulamentações trabalhistas, relativas ao ambiente de trabalho, horário de trabalho, proteção do emprego etc.;
- Regulamentos relacionados às atividades de saúde, ambientais e de segurança na empresa;
- Leis e regulamentações relativas ao tratamento de dados de caráter pessoal;
- Legislação aplicável ao setor em que atua; e
- Requisitos contratuais.

23. Continuidade

a) Quando necessário, devem existir planos de continuidade e contingências que abranjam os sistemas de informação, de infraestrutura críticos e outros essenciais.

b) Os planos de continuidade do negócio devem ser focados nos riscos operacionais, estar alinhados com todos os planos de contingências e planos gerais da Unidas, ser testados regularmente para assegurar a adequação e que a gestão e os colaboradores compreendem a sua execução.

c) Os sistemas de produção e outros sistemas classificados como risco "alto" devem ter soluções de backup.

24. Uso Aceitável dos Ativos

a) Os colaboradores e prestadores de serviços são responsáveis pelo uso adequado das informações, dispositivos eletrônicos e recursos de rede utilizados ou que interajam com redes internas e devem estar com sua configuração em conformidade.

b) É obrigatório a todos os colaboradores e prestadores a observância das seguintes condições de uso:

- Preservar e proteger os ativos da organização, incluindo sistemas, equipamentos, informações e mobiliário de escritório;
- Comunicar assim que possível qualquer incidente suspeito ou eventos que afetem ou possam afetar a Segurança da Informação; e
- Acessar apenas informações e recursos a que esteja autorizado para o acesso.

c) Em caso de descumprimento, a Unidas agirá de acordo com as medidas disciplinares previstas na legislação vigente.

25. Acesso à Internet

a) O uso dos recursos da internet deve ser feito de forma consciente. O recurso disponibilizado pode ser empregado para uso pessoal, desde que não viole nenhuma regra dessa ou qualquer outra política em vigência na organização.

b) O conteúdo que pode ser acessado poderá ser controlado e limitado de acordo com posição hierárquica ou área de atuação de cada colaborador. Todo acesso deverá ser registrado e poderá ser monitorado a fim de bloquear conteúdo que viole essa ou qualquer política em vigência.

c) É expressamente proibido o uso e/ou acesso de:

- Softwares de compartilhamento de arquivos (ex.: Torrents, P2P, etc.);
- Softwares de coleta e análise de rede;
- Jogos online ou offline; e
- Softwares de anonimização ou proxy.
- Atividades ilegais, como o acesso a conteúdo pirateado, envio de spam ou envolvimento em atividades fraudulentas.

26. E-mail e Teams

a) O uso do e-mail e do Teams da Unidas deve ser feito somente para fins corporativos e relacionados às atividades do colaborador. Os e-mails enviados e recebidos de endereços externos e internos poderão ser monitorados para bloqueio de conteúdos que violem as diretrizes dessa política e/ou para fins de auditoria e investigação.

b) Em caso de recebimento de mensagens suspeitas, o usuário deve denunciar para o time de Segurança da Informação investigar e dar o devido direcionamento.

27. Disposições Finais

a) Esta norma entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

28. Controle e Histórico de Versões

Data	Versão	Sumário
21/08/2019	01/2019	Criação do Instrumento Normativo
31/05/2021	01/2021	Revisão do Instrumento Normativo
23/12/2021	01/2022	Revisão do Instrumento Normativo, para adequação aos processos da Lei Geral de Proteção de Dados (LGPD n° 13.709/18)
19/12/2022	02/2022	Revisão do Instrumento Normativo
04/08/2023	01/2023	Revisão do Instrumento Normativo
29/12/2023	02/2023	Revisão item 9-Política de Senhas

29. Aprovações

Código	Descrição	Versão	Vigência
POL-001	Política de Segurança da Informação	02/2023	Indeterminado a partir de 29/12/2023

Emissor(es): Willian Ferreira dos Santos (Emitido eletronicamente em 29/12/2023).

Revisor(es): Leila Angelica Grachekoski (Revisado eletronicamente em 29/12/2023)
Gilson Massateru Matsuda (Revisado eletronicamente em 29/12/2023).

Aprovador(es): Laura Rymsza Barbosa (Aprovado eletronicamente em 29/12/2023);
Carlos Issao Minami (Aprovado eletronicamente em 29/12/2023); e
Alexei Korb (Aprovado eletronicamente em 29/12/2023).
Claudio Jose Zattar (Aprovado eletronicamente em 29/12/2023);