POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Classificação da Informação: INTERNA

RESPONSAVEIS	ÁREA
ELABORADO POR:	Rodrigo Wellausen
REVISADO POR:	Waldomiro Junior

Histórico de Revisões:

VERSÃO	DATA	DESCRIÇÃO	ELABORADO POR:
01	17/08/2023	Primeira Versão	Rodrigo Wellausen
02	25/08/2024	Primeira Revisão	Rodrigo Wellausen
03	05/08/2025	Segunda Revisão	Rodrigo Wellausen

Aprovações:

Nome	Área
Maristela Garcias	Diretoria de RH
Adriano Marques Garcias	Diretoria Financeira
Rafael Pianucci Benedicto	Diretoria de TI
Mauricio Garcias	Superintendente de Startups
Rodrigo Barbosa Wellausen	Encarregado de Dados / DPO

1. OBJETIVO

Estabelecer diretrizes que devem ser seguidas por todos os colaboradores, no que diz respeito à adoção de mecanismos relacionados à segurança da informação e utilização de ativos de tecnologia da informação adequados às necessidades do negócio e da proteção da empresa e de seus colaboradores.

Esta política representa as definições mínimas para segurança da informação que todos os processos da Tecnologia Única devem seguir, inclusive quando executados por terceiros. Além disso, as áreas devem incorporar processos e controles de segurança da informação como complemento ao cumprimento dos padrões da informação no que tange a Integridade, Confidencialidade, Disponibilidade e Privacidade.

2. ABRANGÊNCIA

A presente política aplica-se a toda informação do ambiente de tecnologia e do ambiente convencional da Tecnologia Única, e tem como público-alvo toda estrutura de gestão e colaboradores, incluindo funcionários, estagiários, fornecedores, prestadores de serviços e parceiros de negócio, que tenham acesso em algum momento às informações de propriedade da empresa ou custodiadas por ela.

É responsabilidade de cada colaborador entender o conteúdo deste documento e procurar o suporte necessário antes de iniciar qualquer atividade que envolva o uso de informações proprietárias.

3. CONCEITOS / DEFINIÇÕES

- **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano para companhia;
- **Ativo:** é qualquer coisa que tenha valor para a Tecnologia Única e precise ser adequadamente protegido;
- **Ativo Intangível:** é todo elemento que possui valor para a Tecnologia Única e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à dados, reputação, imagem, marca e conhecimento;
- **Autenticidade:** Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;
- **Colaborador:** Membros da alta administração, funcionários, estagiários (na forma da Lei de Estágio – Lei 11.788/2008) e jovens aprendizes (na forma da Lei de Aprendizagem, Lei 10.097/2000), prestadores de serviços terceirizado, fornecedores e parceiros;
- **Confidencialidade:** é um princípio que está atrelado à privacidade das informações. Ou seja, garantia de que os dados da Tecnologia Única não estarão

disponíveis nem serão divulgados a indivíduos, entidades ou processos sem autorização;

- **Disponibilidade:** é a propriedade de manter a informação disponível para usuários autorizados, quando estes dela necessitarem;
- **Equipe de Resposta a Incidentes:** é o grupo responsável por analisar e responder, com rapidez e precisão, os incidentes de segurança da Tecnologia Única. É previamente definido e imediatamente acionado para efetuar as análises necessárias, pois o tempo de resposta é fundamental para minimizar as consequências e proteger as informações críticas;
- **Incidente de Segurança:** é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade, tais como invasões de computador, ataques de negação de serviços, furto de informação por pessoal interno e ou terceiros, vazamento de dados, atividades em rede não autorizadas ou ilegais;
- **Informação:** é um ativo estratégico e de alto valor para a Tecnologia Única, de sua propriedade ou sob sua responsabilidade e deve ser protegida, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas da segurança da informação;
- **Resposta a Incidentes:** é o processo previamente definido que descreve como a Tecnologia Única deverá lidar com um incidente de segurança;
- **Risco:** Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;
- **Segurança da Informação:** constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, independentemente do meio de armazenamento, processamento ou transmissão que seja utilizado;
- **Segurança Cibernética (Cyber Security):** é utilizado para designar o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição da informação ocasionados por ataques cibernéticos e está integralmente inserido na presente Política;
- **Violação:** Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos da Tecnologia Única;
- **Intranet:** rede local de computadores, circunscrita aos limites internos da Tecnologia Única, na qual são utilizados os mesmos programas e protocolos de comunicação empregados na Internet. As principais aplicações e diretórios de documentos estão lá publicadas;
- **Sala de Resposta a Incidentes:** é o local físico ou virtual, onde a Equipe de Resposta a Incidentes se reunirá no caso da ocorrência de um Incidente de Segurança. Contém os recursos necessários para a Equipe atuar com eficiência e eficácia;

4. DIRETRIZES GERAIS

As diretrizes estabelecidas nesta política têm por objetivo:

- Proteger o valor e a reputação da Tecnologia Única;
- Garantir a confidencialidade, integridade e disponibilidade das informações da Tecnologia Única e de informações de terceiros por ela custodiada, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança da Informação, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes;
- Garantir a continuidade dos negócios da Tecnologia Única, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes à atividade da Tecnologia Única;
- Conscientizar, educar e treinar os usuários na política, normas e procedimentos de Segurança da Informação para que sejam aplicadas às suas atividades diárias;
- Estabelecer e melhorar continuamente um Processo de Gestão de Riscos de Segurança da Informação e Segurança Cibernética;
- Garantir que os dados pessoais não sejam perdidos, roubados, utilizados indevidamente ou vazados por usuários não autorizados;
- Estabelecer controles para prevenção de perda de dados, visando mitigar os riscos usuais, com o estabelecimento de mecanismos de governança e, a avaliação e melhoria contínua de todos os aspectos específicos de privacidade e proteção de dados pessoais;

Na aplicação das diretrizes citadas deve ser considerado que:

- Toda informação e documentos, produzidos pelos colaboradores como resultados de suas atividades profissionais contratadas pela Tecnologia Única pertencem à referida instituição. As exceções, quando existirem, devem ser tratadas à parte de forma explícita e formalizada via contrato entre as partes;
- A Tecnologia Única disponibiliza equipamentos, sistemas e demais recursos de tecnologia da informação de sua propriedade, por meio da área de Tecnologia da Informação (TI), a seus colaboradores, para utilização de forma exclusiva por eles na execução e produção de suas atividades laborais;
- Além dos ativos de tecnologia da informação propriamente ditos (desktops, notebooks, smartphones etc.), todas e quaisquer informações, arquivos e mensagens criadas, armazenadas, recebidas e/ou enviadas, são e permanecem, a qualquer tempo, de propriedade exclusiva da Tecnologia Única;

- A Tecnologia Única manterá um comitê multidisciplinar responsável pela gestão da segurança da informação, designado como Comitê Privacidade e Segurança da Informação;
- Todo e qualquer incidente que afete a segurança da informação deverá ser comunicado à Área de Tecnologia da Informação através do sistema de chamados disponível;
- A Tecnologia Única é isenta de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, tecnologias e serviços concedidos a seus colaboradores, se reservando ao direito de analisar dados e evidências para obtenção de provas a serem utilizadas em um processo investigatório, bem como adotar quaisquer medidas legais cabíveis;
- Cada colaborador é responsável por manter sob sigilo suas credenciais, informações e senhas. Caso o sigilo seja violado por terceiros, por responsabilidade exclusiva do colaborador, este será responsável pela utilização indevida dos ativos;
- O não cumprimento dos requisitos descritivos nesta Política de Segurança da Informação será interpretado como violação às regras internas da empresa e sujeitará o colaborador às medidas administrativas e legais cabíveis;

4.1. IDENTIFICAÇÃO E AUTENTICAÇÃO

Cada usuário é responsável por toda atividade desempenhada com sua identificação de usuário designada através *login* e senha associado à sua identidade nos sistemas, equipamentos ou no uso da rede corporativa e/ou outros recursos aos quais a Tecnologia Única disponibilize acesso.

O usuário também é responsável por verificar as permissões as quais tem direito, notificando a Área de Tecnologia da Informação e gestor direto sobre quaisquer não conformidade a serem corrigidas.

Todas as senhas disponibilizadas pela Tecnologia Única e/ou seus respectivos fornecedores para uso em suas respectivas atividades profissionais por meio de qualquer sistema, são consideradas pessoais e intransferíveis.

Ao realizar transferências de colaboradores entre departamentos, os gestores responsáveis pelo colaborador deverão se certificar de todos os direitos de acesso aos sistemas, arquivos de rede departamentais e outros controles de segurança que serão necessários na sua nova função informando à Área de Tecnologia da Informação qualquer modificação necessária.

Cada gestor é responsável por manter a Área de Tecnologia da Informação informada sobre a necessidade de acessos ou bloqueios que cada colaborador de sua área tenha acesso.

Em quaisquer ausências do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, e se possível efetuar o "*logout/logoff*" da rede ou bloqueio do computador através de senha.

Todos os sistemas implantados pela Tecnologia Única deverão, sempre que possível, utilizar um sistema de troca periódicas de senhas, para garantir a segurança da informação da companhia.

4.2. AUTORIZAÇÃO E CONTROLE DE ACESSO

Cada gestor é responsável pelas informações produzidas por sua área e os direitos de acesso de cada colaborador de sua área.

Eventuais terceiros sob a responsabilidade de um gestor somente terão acesso às informações da Tecnologia Única após assinatura do contrato de prestação de serviço, o qual regulará as regras relacionadas à confidencialidade das informações da Tecnologia Única. Caso a prestação de serviço seja formalizada somente por ordem de compra, deverá o fornecedor assinar o termo de responsabilidade, vinculado a esta política.

As mudanças nos direitos de acesso existentes devido a transferências e mudanças nas funções de trabalho devem ser imediatamente e formalmente comunicadas à Área de Tecnologia da Informação. A comunicação deve ocorrer através da ferramenta de chamados, e informar explicitamente os direitos de acesso, a identificação do usuário e a data efetiva para realizar as alterações pelo gestor responsável que receberá a transferência.

4.3. ACESSO REMOTO EXTERNO

O acesso remoto aos serviços e sistemas corporativos somente devem ser disponibilizados aos colaboradores da Tecnologia Única desde que autorizados de forma explícita por seus gestores.

O acesso remoto à rede corporativa da Tecnologia Única só pode ser realizado através do uso de Client VPN (*Virtual Private Network*) e com as devidas aprovações do gestor responsável pelo colaborador solicitante.

Os administradores da rede lotados na área de Tecnologia da Informação, para desempenho de suas atividades, poderão ter permissão de acesso remoto a todos os recursos computacionais da Tecnologia Única, quando necessário, para atividades de suporte e atendimento de incidentes.

A liberação de acesso remoto, só será efetivada após avaliação e aprovação pela Área de Tecnologia da Informação, para que se evitem ameaças a integridade e confidencialidade das informações contidas na rede da Tecnologia Única. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança da rede.

É vedada a utilização do acesso remoto para fins não relacionados às atividades da Tecnologia Única e para terceiros.

4.4. UTILIZAÇÃO DE CORREIO ELETRÔNICO

A Tecnologia Única disponibiliza contas individualizadas ou coletivas de correio eletrônico (“e-mail”) aos colaboradores que porventura necessitem dos serviços para o cumprimento de suas atividades (a solicitação deverá ser explícita por meio da Área de Pessoas e Cultura no momento da contratação do colaborador ou em caso de uma transferência para uma nova função).

A utilização do serviço de correio eletrônico para fins pessoais não é permitida, o e-mail deve ser utilizado apenas para fins profissionais e é de propriedade exclusiva da Tecnologia Única, podendo ser monitorado a qualquer momento sem prévio aviso.

Fica vedada a cópia e/ou distribuição de materiais protegidos por direitos autorais através de correio eletrônico ou de quaisquer outros meios, sem a confirmação prévia de que a Tecnologia Única detém o direito de copiar e distribuir tais materiais, nos termos da Lei dos Direitos Autorais e demais legislações aplicáveis. Em caso de dúvida, o Colaborador deve solicitar esclarecimentos ao seu superior hierárquico.

É proibido aos colaboradores o uso do correio eletrônico da Tecnologia Única para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagens por correio eletrônico em nome de sua área ou usando o nome de outro colaborador ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Tecnologia Única vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas e documentos. Em casos excepcionais ou necessários, uma solicitação formal via e-mail de uso da informação deverá ser submetida ao Comitê de Segurança da Informação que irá analisar o caso e apresentar um parecer;
- Adulterar informações de endereçamento, alterar cabeçalhos para ocultar a identidade de remetentes e/ou destinatários, com o objetivo de evitar as sanções previstas;
- Encaminhar e-mails contendo informações de propriedade da Tecnologia Única para o e-mail particular do colaborador ou para e-mails de terceiro não vinculado a Tecnologia Única.
- Produzir, transmitir ou divulgar mensagens que:
    - Contenha ameaças eletrônicas, como: spam, vírus de computador etc.;
    - Contenha atos ou forneça orientações que conflite ou contrarie os interesses da Tecnologia Única;
    - Contenha arquivos executáveis (Por exemplo: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer extensão que represente risco à segurança;
    - Vise obter acessos não autorizados a outro computador, servidor, rede ou sistemas;
    - Tenha como objetivo interromper um serviço, servidores, rede ou sistemas por meio de qualquer método ilícito ou não autorizado;
    - Tenha como objetivo observar, vigiar ou assediar outro usuário;
    - Tenha acesso a informações confidenciais sem explícita autorização do proprietário;
    - Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - Contenha anexo(s) superior(es) a 50MB para envio (interno e internet) e 50MB para recebimento (internet);
    - Possua conteúdo classificado como impróprio, obsceno, antiético ou ilegal;
    - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Possua fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do autor ou detentor dos direitos.

4.5. ACESSO A INTERNET

A Tecnologia Única, em total conformidade legal, de forma a mitigar riscos significativos para os ativos de informação, se reserva o direito de monitorar e registrar todos os acessos à Internet realizados pelos seus colaboradores com uso dos ativos de tecnologia da informação disponibilizados por ela.

Os equipamentos, tecnologia e serviços fornecidos para acesso à Internet são de propriedade da Tecnologia Única, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na Internet, estejam eles em disco local, nos equipamentos dos colaboradores ou em áreas reservadas da rede, visando acima de tudo assegurar o cumprimento desta política.

A disponibilização do acesso à Internet, para os colaboradores da Tecnologia Única é para uso profissional e no cumprimento das suas tarefas. Serão concedidas exceções para o acesso de interesse particular quando ele resultar na otimização do tempo (por exemplo pagamentos de contas bancárias) ou quando houver autorização específica por outros casos devidamente documentado junto ao gestor imediato e em conformidade com a Área de Tecnologia da Informação.

A Tecnologia Única, ao monitorar suas redes internas, tem como objetivo garantir a integridade dos dados e sistemas internos. Toda tentativa de alteração de parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será interpretada como inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer equipamento/recurso para atividades ilícitas poderá acarretar ações administrativas e nas penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Os sites ou serviços fornecidos pela Internet, que a Tecnologia Única classifique como inadequados ao ambiente de trabalho, terão seu acesso bloqueado, sem aviso prévio.

É proibida a divulgação e/ou compartilhamento indevido de informações de qualquer área da Tecnologia Única, mesmo de forma parcial, em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia similar que venha a surgir na Internet.

É expressamente proibida a realização de qualquer tipo de download de arquivos, cujo conteúdo não se tenha conhecimento da origem e/ou de sua confiabilidade, sob pena de responsabilidade pelos danos que possam vir a ocorrer ao sistema, rede e equipamentos.

Colaboradores com acesso à Internet não poderão realizar upload (subida) de quaisquer dados pertencentes a Tecnologia Única, parceiros e clientes, sem expressa autorização do responsável pelos dados.

Em casos excepcionais de necessidade de acesso de terceiros, todos os itens acima são aplicados.

4.6. USO DE EQUIPAMENTOS, SERVIDORES E SOFTWARES

Os equipamentos de informática (Desktop, Notebooks, Smartphones etc.) e os servidores são de propriedade da Tecnologia Única, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da Tecnologia Única. É proibido todo procedimento de manutenção física ou lógica, instalação e desinstalação de software e programas (mesmo gratuitos), configuração ou modificação, sem conhecimento prévio e o acompanhamento de um analista da Área de Tecnologia da Informação, qualquer procedimento dessa categoria deverá ser solicitado por meio de e-mail enviado à Área de Tecnologia da Informação.

Não será permitida a utilização dos equipamentos de informática para outros fins, inclusive, para armazenamento de arquivos particulares, fotos, músicas, vídeos dentre outros arquivos não relacionados com às atividades da Tecnologia Única.

Os computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O colaborador, em caso de suspeita de contaminação de vírus ou problemas na funcionalidade, deverá acionar a Área de Tecnologia da Informação por meio de chamado enviado à Área de Tecnologia da Informação.

Sobre o uso de computadores (Desktop e Notebooks) e recursos de informática, existem algumas definições e regras a serem seguidas:

- Todos os computadores individuais deverão ter senha de rede para restringir o acesso de colaboradores não autorizados.
- Os colaboradores devem sempre informar a Área de Tecnologia da Informação qualquer identificação de dispositivo estranho conectado ao seu computador.
- É proibida a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela Área de Tecnologia da Informação ou por terceiros devidamente contratados e autorizados para o serviço.
- É expressamente proibido o consumo de alimentos e bebidas próximos aos equipamentos, acidentes dessa magnitude serão classificados como mau uso dos equipamentos.
- Todos os recursos tecnológicos adquiridos pela Tecnologia Única devem ter imediatamente suas senhas padrões (default) alteradas.

Além disso, acrescentamos situações que são estritamente vedadas:

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, moral, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes, ética e a ordem pública.
- Acessar informações confidenciais sem autorização explícita do proprietário.

- Infringir quaisquer sistemas de segurança.
- Realizar atividades de vigilância secreta por dispositivos eletrônicos ou software e colaboradores, equipamentos de informática e da rede (analisando pacotes da rede – *sniffers*).
- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Instalar ou utilizar software sem licenciamento (piratas) nos equipamentos da Tecnologia Única, em afronta à Lei nº 9.609/98 (Lei de Software).

4.7. ARMAZENAMENTO DAS INFORMAÇÕES E ARQUIVOS

Todos os colaboradores devem periodicamente realizar manutenções no seu diretório pessoal mapeado na rede, evitando assim armazenamento de informações desnecessárias para a Tecnologia Única e as suas atividades individuais;

É obrigatório armazenar os arquivos inerentes à Tecnologia Única no servidor de arquivos para garantir a cópia de segurança deles;

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;

4.8. USO DOS DISPOSITIVOS MÓVEIS E MÍDIAS REMOVÍVEIS

A Tecnologia Única se reserva o direito de inspecionar dispositivos móveis e mídia removíveis, quando permitidos, a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O uso de *pen drives* são vedados para todos os colaboradores da Tecnologia Única, salvo exceções explicitamente autorizadas pela Diretoria sendo que a atividade de leitura, cópia e/ou gravação será realizada pela Área de Tecnologia da Informação, por meio de abertura de chamado.

Todo colaborador deverá utilizar senhas de bloqueio automáticos para seu dispositivo móvel.

O suporte técnico aos dispositivos móveis de propriedade da Tecnologia Única deverá seguir o mesmo fluxo das demais atividades da Área de Tecnologia da Informação.

Uso de rede em diferentes locais só será permitido nos seguintes casos: residência do colaborador, hotéis, órgãos públicos, fornecedores, parceiros estratégico e clientes. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico de Tecnologia da Informação.

Em caso de roubo ou furto de um dispositivo móvel fornecido pela Tecnologia Única, é de responsabilidade do colaborador notificar imediatamente seu gestor imediato e a Área de Tecnologia da Informação. Além disso deverá procurar ajuda das autoridades policiais

registrando, assim que possível, um boletim de ocorrência (BO) que deverá ser enviado para a Área de Tecnologia da Informação.

O colaborador deverá estar ciente que se realizar o uso indevido do dispositivo móvel caracterizará que ele assumirá todos os riscos da má utilização, desta forma o único responsável por quaisquer danos, diretos ou indiretos, que venha causar a Tecnologia Única. Sendo assim totalmente responsável pelos custos dos reparos, seguindo esta norma, ou até mesmo substituição do dispositivo caso identificado a necessidade pela Área de Tecnologia da Informação.

4.9. USO DE EQUIPAMENTOS PARTICULARES

Equipamentos portáteis, tais como notebooks, smartphones, pen drives e outras tecnologias similares de qualquer espécie, quando não fornecidos ao colaborador pela Tecnologia Única, não serão validados para uso e conexão em sua rede corporativa (mesmo que apenas para uso da Internet).

A Companhia não fornecerá acessórios, software ou suporte técnico, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software particular.

A Tecnologia Única não se compromete a fornecer equipamentos de informática para consultores ou terceiros, para atividades particulares ou que sejam desenvolvidas fora das suas dependências.

4.10. CONFIDENCIALIDADE E INTEGRIDADE DA INFORMAÇÃO

Todas as informações armazenadas, transmitidas ou manuseadas por equipamentos, sistemas, processos e colaboradores da Tecnologia Única são de propriedade da mesma. Sempre que for necessário, a Tecnologia Única se reserva ao direito de revisar e monitorar essas informações para fins administrativos, de segurança ou legais.

As informações devem ser classificadas como “Confidencial”, “Restrita”, “Interno” ou “Público”.

NÍVEL DE CONFIDENCIALIDADE	RÓTULOS	CRITÉRIOS DA CLASSIFICAÇÃO	RESTRIÇÃO DE ACESSO
Confidencial	[CONFIDENCIAL]	O acesso não autorizado à informação pode causar danos aos negócios e/ou à reputação da organização. Considerar esta classificação para os dados pessoais.	A informação é disponibilizada somente para colaboradores autorizados, órgãos reguladores e em caso de demandas judiciais.
Uso Restrito	[RESTRITA]	O acesso não autorizado à informação pode causar danos aos negócios e/ou à reputação da organização.	A informação deve ser limitada ao grupo de usuários envolvidos com o assunto/tema.
Uso Interno	[INTERNO]	O acesso não autorizado à informação pode causar danos pequenos e /ou inconveniências à organização.	A informação é disponibilizada internamente a todos os colaboradores, órgãos reguladores, demandas judiciais e para terceiros autorizados.

NÍVEL DE CONFIDENCIALIDADE	RÓTULOS	CRITÉRIOS DA CLASSIFICAÇÃO	RESTRIÇÃO DE ACESSO
Público	[PÚBLICO]	Tornar a informação pública não prejudica a organização de qualquer forma.	A informação está disponível para o público em geral.

Toda Informação que não possuir uma classificação explícita deve ser considerada como Informação interna.

Na classificação de um conjunto de informações que apresentem diversos níveis de confidencialidade, deve-se adotar a classificação de maior nível presente naquele conjunto.

A classificação das informações se pautará pelos critérios de grau de confidencialidade e necessidade de utilização da Informação. O primeiro refere-se ao potencial de risco e prejuízos que a sua divulgação não autorizada ou acidental possa causar. O segundo refere-se aos objetivos e pessoas a que se destina a Informação.

Todas as informações classificadas como confidenciais para a Tecnologia Única, independentemente do modo de armazenamento (mídia ou ambiente de rede), devem ser protegidas contra acessos indevidos ou não autorizados.

Para proteção adequada das informações armazenadas na Tecnologia Única que estão sendo utilizadas nas estações de trabalho, sempre que o colaborador se ausentar de sua posição deve bloquear sua estação (Notebook, Desktop, Smartphone e Tablets).

4.11. MONITORAÇÃO E CONTROLE

A Tecnologia Única se reserva o direito de monitorar, a qualquer tempo e sem aviso prévio, a utilização dos seus equipamentos, dependências e recursos à disposição de todos os seus colaboradores e terceiros.

Como forma de garantir todas as diretrizes desta política a Tecnologia Única poderá:

- Implantar sistemas de controle e monitoramento dos recursos, servidores, smartphones, tablets, correio eletrônico, fluxo de informação de rede/conexão com a internet e outros dispositivos tecnológicos similares ou de sua propriedade – toda informação gerada por esses sistemas poderá ser utilizada na identificação do colaborador e respectivos acessos realizados, bem como arquivos utilizados, incluindo imagens e vídeos;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

4.12. GESTÃO DE VULNERABILIDADE

Softwares de antivírus devem ser instalados e mantidos em todos os computadores e em todos os servidores e outros dispositivos que armazenam dados da Tecnologia Única.

Todos os ativos de informação devem ser continuamente protegidos contra código malicioso, e todos os novos ativos só devem entrar para ambientes de produção após estarem dentro dos processos padrões adotados para proteção dos ativos e das informações.

Informações oriundas de terceiros deverão seguir os mesmos requisitos mínimos, citados nesse item.

Os controles nas áreas de tecnologia devem ser capazes de assegurar que:

- Sejam disponibilizados para execução apenas sistemas operacionais e softwares suportados por fornecedor aprovado ou que tenham uma ativa e apropriada liberação de correções (patches) e de atualizações de configuração para tratar das questões de segurança.
- Todas as correções (patches) e configurações de segurança requeridas sejam aplicadas dentro dos prazos especificados pelo processo de gerenciamento de vulnerabilidades estabelecido.

4.13. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃ

4.13.1. Sanções

Qualquer colaborador que pratique violação desta Política estará sujeito às medidas disciplinares, tais como, advertências verbal ou escrita, suspensão e demissão por justa causa, as quais em nada prejudicarão as sanções previstas em lei.

A aplicação das sanções trabalhistas e administrativas não isenta o colaborador de vir a responder civilmente pelos danos que porventura causar em virtude de uma conduta inadequada e de responder criminalmente, se aplicáveis.

Qualquer caso de não cumprimento da Política de Segurança da Informação da Tecnologia Única, quer seja por uma área, cliente ou colaborador, deverá ser documentado, indicando a razão do não cumprimento/violação, os controles compensatórios, os riscos residuais relacionados, e deverá ser submetido à aprovação do Comitê de Segurança da Informação.

5. RESPONSABILIDADES

5.1. DE TODOS OS COLABORADORES

Será de inteira responsabilidade de cada colaborador, todo e qualquer prejuízo que vier a sofrer ou causar à Tecnologia Única e/ou terceiros, pelo motivo de não cumprimento desta política.

Zelar pelas informações que manipulam, desta forma devem informar imediatamente à Área de Tecnologia da Informação qualquer violação/incidente de segurança que tenha conhecimento.

Formalizar por meio da ferramenta de chamado, qualquer comunicação ou solicitação com a Área de Tecnologia da Informação, de forma a registrar as demandas, auxiliando planejamento da equipe, a auditoria e o cumprimento dos prazos estabelecidos entre os colaboradores e a Área de Tecnologia da Informação (SLA).

Em caso de solicitações via contato telefônico, por meio de aplicativos de mensagens ou contatos pessoais não serão considerados como demandas da Área de Tecnologia da Informação, evitando assim possível falhas humanas em relação aos prazos reais e as expectativas criadas pelos colaboradores.

5.2. DOS GESTORES DE PESSOAS E/OU PROCESSOS

Os gestores da Tecnologia Única devem:

- Ter conduta exemplar em relação à segurança da informação, servindo como modelo de postura para os colaboradores sob a sua gestão.
- Certificar de que todos os colaboradores sob sua gestão, na fase de contratação e de formalização dos contratos individuais de trabalho ou de prestação de serviços ou ainda de parceria, tomaram ciência desta Política e da responsabilidade por seu cumprimento;
- Antes de liberar acesso às informações da empresa, exigir a assinatura do Acordo de Confidencialidade (NDA) dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.
- Autorizar e revisar os acessos à informação de sua área.
- Fiscalizar os terceiros que armazenam, processam, gerenciam ou acessam as informações ou recursos de rede da Tecnologia Única, para que os mesmos cumpram os padrões de segurança definidos.

5.3. ÁREA DE TECNOLOGIA DE INFORMAÇÃO

- Manter os servidores e softwares em local físico confinados, com controle de acesso lógico e demais procedimentos que assegurem a inviolabilidade do sistema, dos equipamentos e dos programas utilizados.
- Disponibilizar sistemática com alternativas de localização física de sistemas automáticos e semiautomáticos de preservação de dados (backup).
- Manter suporte técnico adequado e atualizado com as melhores práticas de segurança de Tecnologia de Informação disponíveis aplicáveis aos negócios da companhia.
- Disponibilizar sistemas de proteção e substituição de senhas com definição de prazo de validade, com o bloqueio automático do sistema em caso de inatividade e/ou não atendimento aos procedimentos definidos.
- Manter sistemática de apuração de incidentes e violações no sistema permitindo a rastreabilidade de acessos virtuais e físicos ao sistema.
- Assegurar a disponibilização, a atualização e a manutenção de todas as licenças de uso de softwares fornecidos pela Tecnologia Única para uso profissional e instalados pela equipe de TI, conforme legislação específica.
- Assegurar a aquisição e/ou desenvolvimento dos sistemas de informática necessários, bem como manter sua atualização.
- Fornecer contas individualizadas de correio eletrônico (“e-mail”) aos colaboradores para facilitar a comunicação e o cumprimento de suas tarefas profissionais, a critério das gerências.
- Garantir que não sejam introduzidas vulnerabilidade ou fragilidades no ambiente de produção.
- Criar login dos colaboradores e terceiros.

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Colher assinatura do Termo de Disponibilização de Equipamentos de TI dos colaboradores no caso de entrega, substituição ou troca de equipamentos de TI, além de repassar ao RH uma cópia do documento para que o prontuário do colaborador em questão seja mantido devidamente atualizado.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação.
- Garantir que os acessos sejam concedidos aos respectivos colaboradores de acordo com os pedidos e indicações feitas pelos gestores da Tecnologia Única, desde que não descumpram com as diretrizes internas e de segurança da informação.
- Analisar detalhadamente incidentes em conjunto com o Comitê de Privacidade e Segurança da Informação.
- Assegurar os servidores e softwares armazenados em local físico apropriado, com controle de acesso lógico e demais procedimentos que garantam a inviolabilidade do sistema, dos equipamentos e dos programas utilizados.
- Manter suporte técnico adequado e atualizado com as melhores práticas de segurança de Tecnologia de Informação disponíveis.
- Manter sistemática de apuração de incidentes e violações no sistema permitindo a rastreabilidade de acessos virtuais e físicos ao sistema.
- 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 sob a anuência da Diretoria da área e, na ausência de Diretoria, do Gestor da área, mas nunca à revelia ou sem o consentimento do(s) mesmo(s).
- Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os privilégios e autorizações 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.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário, mantendo uma cópia do ativo em poder da tecnologia da informação.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
    - Os usuários (*logins*) individuais de colaborador serão de responsabilidade do próprio colaborador ou do gestor responsável.

- Assegurar a disponibilização, a atualização e a manutenção de todas as licenças de uso de softwares, conforme legislação específica.
- Assegurar a aquisição e/ou desenvolvimento dos sistemas de informática necessários, bem como manter sua atualização.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
    - Uso da capacidade instalada da rede e dos equipamentos;
    - Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
    - Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5.4. DO COMITÊ DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, nomeados pela Alta Administração. As deliberações do Comitê são tomadas pela maioria dos membros que o compõe e a função dos integrantes do comitê são indelegáveis.

A composição mínima deve incluir um colaborador de cada uma das áreas: Pessoas e Cultura, Financeiro, Tecnologia da Informação, Processos e Privacidade.

O Comitê deverá se reunir formalmente, trimestralmente, com o objetivo de manter a segurança em todas as áreas da organização.

Reuniões adicionais devem ser realizadas sempre que houver necessidade de uma deliberação sobre algum incidente grave ou definição relevante para a Tecnologia Única.

Em caso de necessidade, o comitê poderá utilizar especialistas, internos e externos, para apoiarem nos assuntos que exijam conhecimentos técnicos específicos.

As responsabilidades do comitê incluem, mas não estão limitadas a:

- Aprovar políticas, normas e procedimentos de segurança da informação.
- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos.
- Propor alterações nas versões da Política de Segurança da Informação e a inclusão, exclusão ou a mudança de normas complementares.
- Aprovar novos controles de segurança para melhoria contínua das medidas de proteção.

- Avaliar os incidentes de segurança e deliberar sobre ações.
- Analisar exceções da política.
- Definir as medidas cabíveis nos casos de descumprimentos da Política de Segurança da Informação.
- Deliberar sobre temas ou ações não definidos/incluídos em nenhuma política ou norma já publicada.

5.5. ÁREA DE PESSOAS E CULTURA

- Orientar os novos colaboradores, no evento de Integração Organizacional, sobre as melhores práticas de boa utilização/conservação dos ativos da Tecnologia Única sob sua responsabilidade, inclusive equipamentos de TI;
- Requerer a todos os colaboradores a assinatura do Termo de Ciência das Políticas e Normas;
- Solicitar a Área de Tecnologia da Informação o bloqueio de acesso de usuários (de forma imediata) por motivo de desligamento da Tecnologia Única, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

6. REFERÊNCIAS

Além desta Política, aplicam-se à Tecnologia Única outras diretrizes e normas, inclusive:

(i) Política de Privacidade

No Brasil, as principais leis e regulamentos aplicáveis à Tecnologia Única no que se refere aos temas tratados nesta Política, entre outros, são:

- A Lei nº 13.709/2018, a LGPD;
- A Lei nº 12.965/2014, o Marco Civil da Internet;
- A Lei nº 12.527/2011, a Lei de Acesso à Informação;
- Os regulamentos e normas publicados pela ANPD.

7. DISPOSIÇÕES FINAIS

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

Esta política será avaliada criticamente de forma anual e revisada no mínimo bienalmente pela área responsável, ou sempre que necessário, diante de alterações significativas na empresa e ambiente tecnológico.