Política de Segurança da Informação	Versão: 1.0	Data: 06/09/2021
Autor: Unidasul Distribuidora Alimentícia S.A.		
Revisor: Comitê de Segurança da Informação e LGPD		
Classificação da informação: Pública		

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A Política de Segurança da Informação, também chamada de PSI, é o documento que normatiza e orienta as regras corporativas da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A, entende-se que diante da evolução dos meios tecnológicos, da facilitação do acesso à internet, e consequentemente do crescimento dos crimes cibernéticos, é necessário assumir um posicionamento firme e claro quanto à garantia da Segurança da Informação e, para isso, apoia e fomenta este tema, buscando incorporá-lo à sua cultura, para tanto garantindo meios e recursos.

Dessa forma, adota-se critérios técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, ou qualquer forma de tratamento inadequado, conforme previsão do art. 46 da Lei nº 13.709/2018 (LGPD). Para tanto, a empresa deve implementar soluções de natureza multidisciplinar, com observância do descrito na ABNT NBR ISO/IEC.27001:2013, ISO/IEC.27002:2005, ISO/IEC.27005:2011 e ISO/IEC.16167:2013, visando a melhor segurança dos dados pessoais de pessoas naturais. Outrossim, todos da organização devem considerar a informação e equipamentos de informática como sendo um bem da empresa, que agrega, gera negócio e que possui um grande valor para a UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A.

Este documento deverá estar disponível no site institucional e na intranet coorporativa, de sorte a garantir que todas as pessoas tenham consciência acerca de seu teor e a pratiquem na empresa.

2. OBJETIVO

Estabelecer os conceitos e diretrizes de segurança da informação, visando a proteger as informações da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A – e de seus colaboradores, fornecedores, clientes.

Este manual é um documento estratégico, com vistas a promover à utilização segura dos ativos de informação da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A, preservando a confiabilidade, a integridade, a legalidade e a disponibilidade das informações para resolução de incidentes e deliberação de procedimentos a serem adotados.

Assim, tem-se como declaração formal da Diretoria acerca de seu compromisso com a proteção de dados pessoais e informações de sua propriedade e/ou sob sua custódia, devendo ser observada por todos os colaboradores internos e externos da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A.

3. ABRANGÊNCIA

Esta política se aplica a todos os usuários (estagiários, colaboradores, funcionários, gestores, fornecedores e terceirizados) que utilizam as informações constantes nos ativos da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A.

4. PRINCÍPIOS

As informações das quais a UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A tem propriedade ou poder de custódia possuem valor, devendo ser protegidas, cuidadas e gerenciadas de forma adequada, garantindo sua disponibilidade, integridade, confidencialidade, legalidade e autenticidade, independentemente das formas de tratamento de dados utilizados pela empresa.

Dessa forma, destaca-se:

- Confidencialidade – Garantir que as informações não sejam

disponibilizadas ou divulgadas a pessoas ou processos não autorizados, portanto, não alinhados com o propósito do uso daquela informação.

- Integridade – Garantir que as informações estejam protegidas contra modificações ou manipulações não autorizadas, assim como garantir a rastreabilidade sobre modificações autorizadas ou, mesmo, indevidas.
- Disponibilidade – Garantir que todas as informações e serviços relevantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.
- Autenticidade – Garantir que todas as pessoas e objetos são quem realmente dizem ser e que as conexões provêm de fontes legítimas e que não foram alvo de alterações durante o processo.

5. CLASSIFICAÇÃO DE DADOS E DADOS PESSOAIS

Para todos os procedimentos discriminados nesta Política de Segurança da Informação, dados que identificam total, parcialmente, ou façam referência a características ou preferências de pessoas naturais, devem ser considerados, ‘internos’. Assim, todos os procedimentos técnicos de resguardo, sigilo e cuidados de dados classificados como internos são extensíveis aos dados pessoais.

Da mesma forma, para todos os procedimentos discriminados nesta Política de Segurança da Informação dados que denotem preferências, credo, aptidões, estado de saúde ou financeira e outros que possam expor a preconceito qualquer pessoa natural, total ou parcialmente identificável, devem para todos os fins, ser considerados confidenciais. Assim, todos os procedimentos técnicos de resguardo, sigilo e cuidados de dados classificados como confidenciais são extensíveis aos dados sensíveis.

6. CONSCIENTIZAÇÃO E TERMO DE CONFIDENCIALIDADE

Os colaboradores devem a partir de seu ingresso na empresa, ler e estar em pleno entendimento e consciência sobre a Política de Segurança da Informação, assinando o **Termo de aceite da Política de Segurança da Informação.**

6.1. Atribuição de responsabilidades

- GLOBAL: Todos os colaboradores, estagiários, prestadores de serviços e parceiros de negócio tem responsabilidade diretamente atribuída com as melhores práticas de Segurança da Informação, com as informações de clientes e com a conformidade desta PSI.
- ATUALIZAÇÃO E DISTRIBUIÇÃO DA PSI: É de responsabilidade da Segurança da Informação em parceria com os demais departamentos envolvidos nos processos de negócios a atualização e distribuição desta política a todos os colaboradores, estagiários, terceiros e parceiros de negócios.
- GESTÃO DE ACESSOS: A gestão de acessos lógicos e de administração dos demais serviços e ativos da empresa, bem como a definição de papéis e segregação de funções estão descritos nos assuntos específicos citados na norma de Gestão de Acessos, Norma do M365 e Norma de Acesso à Internet, disponíveis para consulta interna aos colaboradores da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A.

6.2. Conscientização e Treinamento de SI

Todos os colaboradores devem periodicamente passar por treinamento sobre Segurança da Informação, bem como os desenvolvedores devem ser submetidos periodicamente a treinamentos sobre desenvolvimento seguro. Adicionalmente, a empresa deve fomentar através da Segurança da Informação com apoio do departamento de Recursos Humanos o assunto Segurança da Informação e boas práticas com o objetivo de conscientizar a todos sobre a necessidade de pensar e agir com segurança, minimizando assim os riscos operacionais da empresa.

6.3. Confidencialidade da informação e política social

A confidencialidade das informações será definida através da Classificação das Informações, garantindo-se o sigilo dos dados. A confidencialidade deve ser mantida por toda a vida útil dos dados pessoais, bem como durante o tratamento realizado pela UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A.

As informações recebidas pelos colaboradores, para fins de prestação de serviços, são confidenciais e, portanto, não devem ser repassadas a colaboradores não autorizados ou a terceiros, sem justo motivo, observando-se as seguintes orientações:

- A informação produzida ou recebida deverá ser utilizada com senso de responsabilidade e de modo ético e seguro, em benefício exclusivo dos negócios corporativos.

- É proibido comentar sobre as políticas de segurança da empresa com terceiros em locais públicos.

- As senhas de acesso são pessoais e intransferíveis.

- É vedada a utilização das senhas de acesso em computadores externos.

- Não execute instruções informáticas recebidas por *e-mail* que não sejam da equipe de TI.

- Relate à chefia e à equipe de TI qualquer orientação em desacordo com as normas previstas nesta política.

6.4. Declaração de privacidade com clientes

O relacionamento contratual da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A com clientes deve compreender declaração de privacidade distinta, ou seja, em destaque, seja através de Termo de Confidencialidade e Não divulgação ou em cláusulas de contratos de prestações de serviços.

Tornando, assim, claro o comprometimento da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A com a privacidade dos dados pessoais, sensíveis, privados e confidenciais, bem como das demais informações a que tenha acesso.

6.5. Consentimento do uso de dados pessoais

O relacionamento contratual da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A com clientes, fornecedores, assim como o contrato de trabalho com colaboradores, deve conter cláusula que verse sobre o consentimento do compartilhamento de informações para uso exclusivo da finalidade descrita no relacionamento profissional. Dentre estas informações, concebe-se a possibilidade do compartilhamento consentido de dados pessoais.

Os contratos firmados devem conter cláusulas que confirmem a ciência e conhecimento das partes sobre as obrigações relacionadas a Lei 13.709, a Lei Geral de Proteção de Dados.

7. DIRETRIZES GERAIS

7.1. Utilização da informação e recursos

A liberação de acesso às informações para os usuários será autorizada através de Controle de Usuários e, levará em consideração a necessidade de utilização por cada colaborador, observando-se o grau de sigilo das informações.

O acesso aos dados pessoais deverá ser autorizado apenas para usuários que deles necessitem para desempenho de suas atividades profissionais na UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A. Cada usuário deverá tratar apenas as informações e ambientes previamente permitidos. A tentativa consciente de acesso a ambientes/dados não autorizados será passível de punição.

O acesso das informações armazenadas e processadas em ambiente virtual é individual e intransferível. O acesso acontecerá mediante identificação e autenticação do usuário, devendo ser mantidos em segredo.

Os recursos de tecnologia fornecidos pela empresa são para uso exclusivo para realização das atividades profissionais. A utilização para fins pessoais é vedada. Em caso de necessidade de uso para fins pessoais, a gerência deve conceder permissão, com descrição do motivo, data e tempo de uso (em horas), com comunicação imediata à equipe de TI, para o devido monitoramento.

A UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A reserva-se o direito de monitorar e registrar o uso das informações, sistemas e serviços pertencentes à empresa.

7.2. Dados pessoais tratados em cada setor e sua finalidade

Os dados pessoais e dados pessoais sensíveis possuem proteção específica, prevista na Lei de Proteção de Dados. Para tanto, é necessário observar os dados aos quais cada área da empresa tem acesso, bem como delimitar sua finalidade exclusiva, visando a mantê-los seguros. A UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S.A. promoveu um mapeamento interno das atividades da organização, tanto a nível administrativo quanto operacional, de modo a identificar quais dados pessoais eram tratados por cada setor da organização no dia a dia de suas atividades. Os relatórios consolidados com identificação dos dados tratados por cada área e seu respectivo fundamento legal, estão disponíveis em documentos internos da empresa, os quais serão disponibilizados a órgãos fiscalizadores e demais entes conforme a necessidade.

7.3. Manuseio e armazenamento de documentação física

Todos os dados e informações – seja físico ou digital – de propriedade da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A ou confiados a ela devem estar sob regras rígidas e controles criteriosos de armazenamento, processamento e descarte, de forma que somente as informações estritamente necessárias e permitidas por lei sejam armazenadas por um período mínimo necessário sendo descartadas de forma segura e definitiva imediatamente após não haver mais necessidade ou uma justificativa de negócio para sua

manutenção, para maior detalhamento consultar a Política de Privacidade presente em nosso site.

Todos os procedimentos que possibilitam a proteção da informação e a continuidade do seu uso devem ser documentados, de tal forma que possibilite a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

Os documentos em meio analógico, que contenham dados pessoais ou dados pessoais sensíveis, devem ser guardados em envelopes/pastas e armazenados em gavetas ou armários com chave.

Não deixe documentos que contenham dados pessoais sobre sua mesa.

Imprima somente o necessário.

Selecione as folhas que serão utilizadas para rascunho e descarte, de forma segura, as que contenham informações confidenciais.

Os documentos que contenham dados pessoais devem ser armazenados em locais com chave, com acesso restrito, formalizado através de termo entre a gestão e o funcionário que tiver a entrada franqueada.

Os documentos arquivados terão regramento específico com base na Classificação Documental e Tabela de Temporalidade.

8. USO ACEITÁVEL DAS TECNOLOGIAS

8.1. Computação pessoal e móvel

Os dados pessoais existentes nos sistemas da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A somente serão utilizados em recursos da própria UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A. É proibido o uso de equipamentos pessoais para tratamento de dados pessoais ou para manuseio de sistemas corporativos, salvo para colaboradores adeptos da Política BYOD, mediante autorização da gerência e comunicação ao setor de TI.

Caberá ao colaborador assinar um termo de responsabilidade pelo equipamento no ato do recebimento deste, assumindo a responsabilidade e comprometendo-se a mantê-lo em perfeito estado de conservação.

Em caso de devolução ou troca do equipamento, deverá ser celebrado um Termo de Devolução assinado pelo colaborador que está devolvendo o equipamento e um funcionário da TI responsável por dar o devido encaminhamento, transferindo assim, a responsabilidade do equipamento para a área de TI.

Todos os ativos devem ser inventariados de modo a facilitar a identificação do ativo, seu proprietário, o departamento, sistemas e aplicações instalados, fabricantes e versões de sistemas, localização na rede e saúde do equipamento.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, realizados sem o conhecimento prévio e o acompanhamento de um técnico da área de TI ou a quem este determinar.

As áreas que necessitarem realizar testes deverão solicitar previamente à área de TI.

Os sistemas e computadores devem ter versões instaladas, ativadas e atualizadas permanentemente de software antivírus. O usuário, em caso de suspeita de vírus ou problemas de funcionalidade, deverá acionar o departamento técnico responsável através de requisições de serviços.

8.2. Utilização de *notebooks* da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A

O setor de Tecnologia da Informação disponibiliza notebooks para uso dos colaboradores, cabendo ao colaborador realizar solicitação através da ferramenta específica para os respectivos acessos.

8.3. E-mail

As mensagens do correio eletrônico disponibilizado aos colaboradores devem ser redigidas, obrigatoriamente, com observância de linguagem profissional e que não comprometa a imagem da organização, ou vá de encontro à legislação vigente ou aos princípios éticos da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A. Cada usuário é responsável pela conta que lhe foi disponibilizada para desempenho de suas funções.

O conteúdo do correio eletrônico poderá ser monitorado pela equipe de TI, quando ocorrerem situações que coloquem em risco a UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A ou a segurança de dados pessoais ou dados pessoais sensíveis de outros colaboradores, sócios ou parceiros. O usuário não deve ter expectativa de sigilo de sua correspondência em *e-mail* fornecido pela empresa.

As informações produzidas por funcionários, colaboradores e prestadores de serviço no exercício de suas funções, são propriedade intelectual da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A e não cabe a seus criadores qualquer forma de direito autoral.

A utilização de *e-mail* pessoal nas estações de trabalho observará o disposto na Norma de Acesso à Internet, disponível para consulta interna aos empregados da Unidasul.

O colaborador não deverá abrir anexos duvidosos, tampouco arquivos de extensões como.bat, .exe, srs,, *links* enviados por *e-mail*, bem como deve desconfiar de *e-mails* que contenham mensagens que não estejam relacionadas à atividade profissional ou em línguas estrangeiras, devendo comunicar imediatamente quaisquer suspeitas à equipe de TI.

Em caso de dúvidas, o colaborador deverá consultar a equipe técnica.

8.4. Ambiente de *internet*

O ambiente de *internet* deve ser utilizado para o desempenho de atividades profissionais do usuário, sendo vedada a utilização para fins pessoais

e recreativos. *Sites* que não agreguem conhecimento profissional ou para o negócio não devem ser acessados.

Os sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados se encontram na lista de sites proibidos e são bloqueados para acesso.

Os acessos realizados no ambiente de internet são monitorados pela organização com o objetivo de cumprimento desta política.

8.5. Envio de documentos e informações

É proibido enviar fotos de documentos ou informações da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A através de mídias de celular, ressalvadas hipóteses de extrema necessidade, devidamente fundamentadas.

Em caso de recebimento, o colaborador deverá transmiti-lo imediatamente para seu computador corporativo, excluindo a mídia terminantemente de seu dispositivo móvel.

Os documentos e informações deverão ser transmitidos exclusivamente através do *e-mail* corporativo e da ferramenta de comunicação interna *Microsoft Teams*.

8.6. Uso das estações de trabalho

As estações de trabalho são pessoais e, portanto, configuradas com as permissões necessárias para a prestação de serviços de cada colaborador.

É obrigatório o bloqueio das estações de trabalho durante a ausência do colaborador, bem como todos os computadores da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A serão configurados para bloqueio automático após 10 minutos em desuso.

É vedada a instalação de *softwares* e *hardwares* sem autorização/auxílio da equipe técnica, ainda que o perfil de usuário do colaborador permita esta ação.

É vedada a realização de *downloads* de filmes, músicas, fotos em *sites* de pirataria, os quais são monitorados pela equipe de TI.

Documentos imprescindíveis para as atividades dos colaboradores deverão ser salvos em drives de rede. Os arquivos gravados apenas localmente nos computadores (Ex. drive C:), não terão garantia de Backup e poderão ser perdidos caso ocorra uma falha no equipamento, furto ou qualquer sinistro e assim sendo, o usuário poderá ser responsável por sua negligência.

É vedada a utilização de aplicativos de mensagens instantâneas (*WhatsappWeb, Skype*), em contas pessoais, nas estações de trabalho, exceto exceções tratadas pontualmente pela equipe de TI.

As portas USB dos computadores se encontram bloqueadas. Em caso de necessidade de utilização, deverá haver autorização formal da chefia, com comunicação à equipe de TI para liberação. Os *smartphones* não devem ser carregados nas estações de trabalho. Em caso de necessidade, realize o carregamento na tomada elétrica.

Em caso de necessidade de utilização de *sites* de transferência de arquivos, em razão do tamanho do documento, deverá ser observado o teor da Norma de Acesso à Internet, disponível para consulta interna aos empregados da Unidasul.

8.7. Autenticação e senhas

A política de autenticação e de senhas visa a evitar o acesso não autorizado a dados pessoais e demais informações. Pessoas não autorizadas são aquelas que não detêm legitimidade legal, regulamentar ou estatutária para o tratamento de dados. Por isso, as seguintes medidas são necessárias:

- A autenticação nos sistemas é realizada através de senha pessoal e intransferível, ou seja, de responsabilidade exclusiva do usuário.

- O padrão de senha deve ser complexo, observados os critérios mínimos estipulados pela Segurança da Informação da Unidasul.

- A senha deverá ser trocada periodicamente, seguindo o padrão descrito no item anterior.

- As senhas são únicas, pessoais e intransferíveis e tornam o portador da senha responsável por todas as ações praticadas com o seu uso.

- O compartilhamento de senhas, em quaisquer hipóteses, é expressamente proibido.

- Todos os recursos tecnológicos adquiridos pela UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A devem ter imediatamente suas senhas padrão (default) alteradas.

8.8. Controle de acesso de usuários

Todas as pessoas devem ser distintamente identificadas, sejam visitantes, estagiários, funcionários temporários, funcionários regulares, prestadores de serviços pessoa física e prestadores de serviços pessoa jurídica.

As estações de trabalho são pessoais e configuradas conforme as necessidades do usuário. As permissões de acesso são designadas através de diretórios de grupos de usuários de acordo com as funções desempenhadas.

Por isso, como já destacado anteriormente, as senhas de acesso são pessoais e intransferíveis, o que garante a segurança dos dados pessoais tratados por cada colaborador.

É necessário que o controle seja efetivo. Para tanto, haverá revisão periódica dos acessos dos colaboradores, visando a minimização da probabilidade de riscos de uma ameaça prejudicial à empresa.

9. SEGURANÇA NAS COMUNICAÇÕES

A comunicação do acesso de usuários autenticados e autorizados aos respectivos sistemas a que tem permissões, devem ser controlados seguindo a matriz de Controle de Acesso Unidasul. A disponibilidade dos segmentos e dispositivos de redes, assim como dos *links*, serviços e servidores devem seguir às premissas do Plano de Continuidade de Negócios da UNIDASUL

DISTRIBUIDORA ALIMENTÍCIA S/A, priorizando o acesso aos serviços mais críticos para o negócio.

A transferências de informações confidenciais ou internas para fora da organização deve ocorrer respeitando critérios de controle de acesso conforme a Matriz de Controle de Acesso, respeitando requisitos de sigilo e integridade.

Toda troca ou transferência de informações entre organizações que exijam confidencialidade e acordo de não divulgação deve ser monitorada e configurada de forma que atenda às restrições acordadas.

10. CONTINUIDADE DO USO DA INFORMAÇÃO

Todas as informações relevantes utilizadas para funcionamento da UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A devem possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção equivalente ao local principal, questões a serem delineadas na Política de *Backup*.

Outrossim, a área de Segurança da Informação deverá ser considerada no gerenciamento de projetos, independentemente do tipo de projeto; bem como deverá manter contato apropriado com grupos especiais, associações profissionais ou outros fóruns especializados em Segurança da Informação com o objetivo de se manter atualizada em relação às melhores práticas, novas tecnologias e ameaças recém-descobertas pela comunidade internacional.

11. CONTROLE DE ACESSOS

- Os colaboradores receberão acesso ao conjunto de sistemas corporativos inerentes à sua função na empresa, mediante uso de usuário e senha pessoal.

- Cadastro do ponto eletrônico

- Em atenção à Portaria 1510/2009 do Ministério do Trabalho e Emprego, é necessária a utilização de registro de ponto eletrônico.
- Na contratação do funcionário em regime de CLT, será realizado o cadastramento biométrico no sistema coorporativo respectivo.

12. SEGURANÇA FÍSICA DO DATACENTER

Somente podem acessar o datacenter coorporativo, instalado nas dependências da matriz da empresa, em Esteio/RS, os colaboradores autorizados pela gerência de TI. Terceiros podem acessar somente acompanhados por colaboradores autorizados.

13. DISPOSIÇÕES FINAIS

- Todos os incidentes que afetam a Segurança da Informação devem ser reportados ao Departamento de SI.
- Para qualquer implementação de sistemas e aplicações, é mandatória a utilização de ambientes de produção e homologação segregados.
- Devem ser estabelecidas e comunicadas as normas e responsabilidades específicas pela gestão e custódia dos ativos de informação conforme os assuntos específicos contidos nesta Política.
- Todas as mudanças em processos, procedimentos e tecnologias devem ser formalmente avaliadas considerando o atendimento aos requisitos desta PSI.

14. DAS RESPONSABILIDADES

A UNIDASUL DISTRIBUIDORA ALIMENTÍCIA S/A exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, estagiários, parceiros, fornecedores, prestadores de serviço, reservando-se o

direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, adotar as medidas legais cabíveis e punir os infratores.

15. DO PRAZO DE REVISÃO

A presente política deverá ser submetida à análise crítica e sofrer revisão constante, especialmente nas hipóteses de mudanças de processo, alteração de tecnologia (sistemas ou aplicativos), alteração de legislação ou por determinação da área responsável resultando em um processo abrangente de melhoria contínua das implementações de boas práticas em Segurança da Informação.

16. INFORMAÇÕES ADICIONAIS

Documentos Relacionados

- ABNT NBR ISO/IEC.27001:2013
- ABNT NBR ISO/IEC.27002:2005
- ABNT NBR ISO/IEC.27005:2011
- ABNT NBR ISO/IEC.16167:2013
- ABNT NBR ISO/IEC.27701:2019
- Lei 13.709, Lei Geral de Proteção de Dados
- Norma de Gestão de Acessos
- Norma M365
- Norma de acesso à Internet
- Política de Privacidade
- Política de Backup Corporativo