1 OBJETIVO

Esta Política define as diretrizes e regras de Segurança da Informação em execução na SALTON, sendo aplicado para todos os empregados e empresas terceiras, como também para fornecedores que utilizam informações e ativos da SALTON, seja na forma física ou digital, visando atingir um alto padrão de segurança em diversos níveis e com o compromisso geral de todos os envolvidos que tenham acesso aos sistemas e ambientes da SALTON.

2 APLICABILIDADE

Aplicável a todas as unidades.

3 REFERÊNCIAS

ISO/IEC 27001

4 SIGLAS E DEFINIÇÕES

AD: (Active Directory) - Serviço de diretório da Microsoft que fornece autenticação e autorização centralizadas para recursos de rede;
FS: **(**File Server) - Servidor de arquivos que permite o armazenamento e compartilhamento de arquivos em uma rede;
FS: (File Sync) - Servidor de arquivos com sincronização automática em nuvem;
OU: **(**Organizational Unit) - Unidade organizacional usada para classificar objetos em diretórios, como o AD;
VS: (Vault Salton) - Cofre de senhas desenvolvido pela Salton para que você possa salvar suas senhas dentro do Protheus;
Endpoint: Máquina do usuário final.

5 DESCRIÇÃO

Com o intuito de instituir procedimentos que componham um sistema íntegro e consistente de segurança da informação, a SALTON busca:

- Cumprir as legislações em vigor, regulamentos e documentos normativos vinculados à segurança da informação, principalmente, mas não restringindo-se a Lei 13.709 de Proteção de Dados (LGPD), dentre outras boas práticas de mercado e frameworks de segurança da informação;
- Assegurar que a SALTON seja capaz de garantir a continuidade nos negócios, mesmo em decorrência de incidentes causados por falhas ou desastres, assegurando a disponibilidade e confiabilidade da infraestrutura de rede e serviços;
- Garantir que os recursos tecnológicos e a informação são utilizados de maneira adequada por todos os integrantes da empresa e parceiros de negócio;
- Implementar controles para preservar os interesses dos colaboradores, clientes e demais parceiros contra danos que possam acontecer devido a falha de segurança. Nesta política estarão descritas as normas de utilização e possíveis atividades que possam ser consideradas como violação ao uso dos serviços, e, portanto, considerados proibidos. Todos os itens, ações, atitudes que não constam como expressamente permitidos neste documento, são considerados proibidos;
- Informar sobre as diretrizes aplicadas na empresa para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a SALTON, seus colaboradores e parceiros;
- Mitigar riscos a fim de prevenir eventuais incidentes cibernéticos e de segurança da informação;
- Estabelecer padrões de comportamento relacionados à segurança da informação estando estes adequados as necessidades do negócio e proteção legal da empresa e dos indivíduos. O usuário deve conhecer as regras para

utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a SALTON, seus funcionários ou parceiros;

- Preservar as informações da SALTON quanto à:
  - Integridade: garantir que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
  - Confidencialidade: garantir que o acesso à informação seja obtido somente por pessoas autorizadas e não seja divulgado em qualquer meio fora da SALTON;
  - Disponibilidade: garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

5.1 BOAS PRÁTICAS E COMPORTAMENTO SEGURO

A Política de Segurança da Tecnologia da Informação SALTON estabelece diretrizes para o manuseio da informação, descrevendo a seguir a conduta que todos os usuários do ambiente da SALTON devem adotar como boas práticas e comportamento seguro:

- Colaboradores e parceiros de negócio devem assumir atitude proativa e engajada no que diz respeito à privacidade e proteção de dados;
- Todos os colaboradores que produzem informações, possuem o papel de "agente cumpridor da segurança da informação", sendo responsáveis pela manipulação segura do dado de acordo com o nível de confidencialidade necessário;
- A conduta ética também deve estar presente no acesso e manuseio das informações, conforme código de conduta da SALTON;
- A SALTON detém a propriedade intelectual de qualquer informação e/ou projeto elaborado pelos colaboradores. As informações não devem ser repassadas sem autorização;
- Apenas a Direção e pessoas previamente autorizadas podem falar em nome da empresa, inclusive para classificar ou divulgar informações como públicas;
- **O login e a senha do colaborador são pessoais e intransferíveis,** sendo expressamente proibido o seu compartilhamento com colegas, terceiros ou qualquer outra pessoa;
- Colaboradores e parceiros de negócio devem utilizar a internet de forma profissional e controlada, respeitando as regras determinadas pela SALTON;
- Informações estratégicas da SALTON, enquanto não divulgadas de forma oficial e pública, são consideradas confidenciais e reservadas;
- O colaborador deve bloquear sua estação de trabalho quando interromper o uso, mesmo que por breves momentos;
- O colaborador, ao final do seu expediente, deve guardar todos os documentos sensíveis e confidenciais em armários trancados com chave;
- Os gestores devem ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

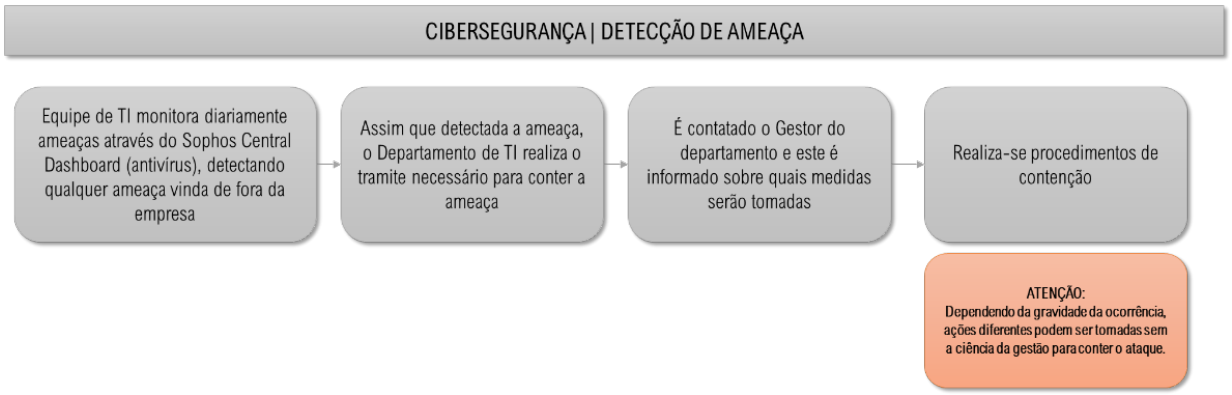
5.2 CIBERSEGURANÇA

A cibersegurança é um dos pilares fundamentais da Política de Segurança da Informação da Salton. Seu objetivo é proteger os ativos digitais da organização contra acessos não autorizados, vazamentos de dados, ataques cibernéticos e quaisquer riscos que possam comprometer a integridade, confidencialidade e disponibilidade das informações.

Todos os colaboradores que utilizam dispositivos eletrônicos corporativos (como computadores, notebooks, smartphones e tablets) devem adotar comportamentos seguros e responsáveis no ambiente digital. Entre os deveres dos usuários, destacam-se:

- Zelar pela segurança da informação no uso diário de sistemas, e-mails, redes e aplicações;
- Utilizar senhas fortes, pessoais e intransferíveis, mantendo-as em sigilo;
- Evitar o acesso a sites não confiáveis e não clicar em links ou anexos de origem duvidosa;
- Bloquear a estação de trabalho sempre que se ausentar;
- Atualizar dispositivos conforme orientações e políticas da empresa;
- Reportar imediatamente ao setor de TI qualquer comportamento anômalo, tentativa de fraude, infecção por malware ou suspeita de violação de segurança.

A SALTON determina que é responsabilidade do setor de TI, monitorar, eliminar e comunicar o se houver ameaças identificadas no ambiente virtual estando em conformidade com a Política de Segurança da Informação e LGPD.



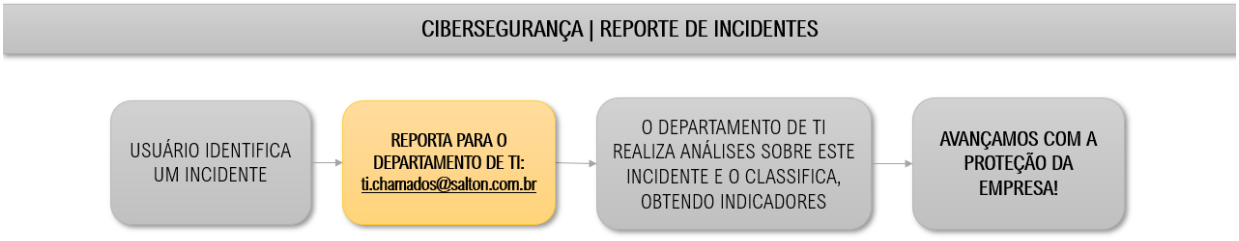
5.2.1 Reporte de incidentes

O que é um incidente de segurança da informação?

Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Tecnologia da Informação SALTON.

A SALTON estruturou um procedimento próprio denominado “PLANO DE RESPOSTA À INCIDENTES”, o qual descreverá o passo-a-passo e ações que deverão ser observadas pelos profissionais da área de TI, Encarregado de dados e outros integrantes do Comitê de Privacidade e Segurança da informação (“CPSI”).

O reporte de incidentes deve ser realizado diretamente à área de Tecnologia da Informação:



CATEGORIA	DEFINIÇÃO
CONTEÚDO ABUSIVO	Envio de e-mails não solicitados pelo destinatário. Incidentes relacionados à difamação, assédio, discriminação, entre outros.
CÓDIGO MALICIOSO	Códigos maliciosos infectando sistemas, disponíveis para download, anexos a e-mails ou recebendo comandos.
PROSPECÇÃO POR INFORMAÇÕES	Envio de solicitações a sistemas para descobrir vulnerabilidades, configurações ou serviços. Abrange processos de testes não solicitados. (Varredura) Monitorar ou

	gravar tráfego de rede sem autorização. (Escuta não autorizada) Obter informações sigilosas de pessoas se utilizando de manipulação, confiança, boa-fé. (Engenharia social).
TENTATIVA DE INTRUSÃO	Tentativas de comprometimento ou acesso a sistemas através de ataques que explorem vulnerabilidades (XSS, buffer overflow, outras). (Tentativa de exploração de vulnerabilidades) Tentativas de login, utilizando força bruta (dicionários) ou não. (SSH, webmail, ftp etc.).
INTRUSÃO	Comprometimento de sistema ou de aplicação (serviço).
INDISPONIBILIDADE DE SERVIÇO OU INFORMAÇÃO	Tentativas ou sucesso na indisponibilização de serviços ou informações, exaurindo recursos de hardware, software ou de conectividade.
SEGURANÇA DA INFORMAÇÃO	Ataques cuja finalidade é o acesso ou modificação de informação de forma não autorizada, sem envolver o comprometimento de sistemas (invasão, força bruta), e geralmente se aproveitando de oportunidades. Sequestro da informação através de criptografia do conteúdo e exigência de resgate para fornecer chave de criptografia.
FRAUDE	Cópia, venda, instalação, download ou distribuição de material protegido por direitos autorais (violação de direitos autorais). Ataque onde uma entidade assume ilegitimamente a identidade de outra para obter qualquer tipo de informação, recurso ou vantagem. (Fingir ou falsificar identidade ou instituição). Utilização de recursos de forma não autorizada (correntes de e-mail, servidores de jogos, entre outros). (Uso de recursos de forma não autorizada).
OUTROS	Incidentes não representados anteriormente.

5.3 LGPD

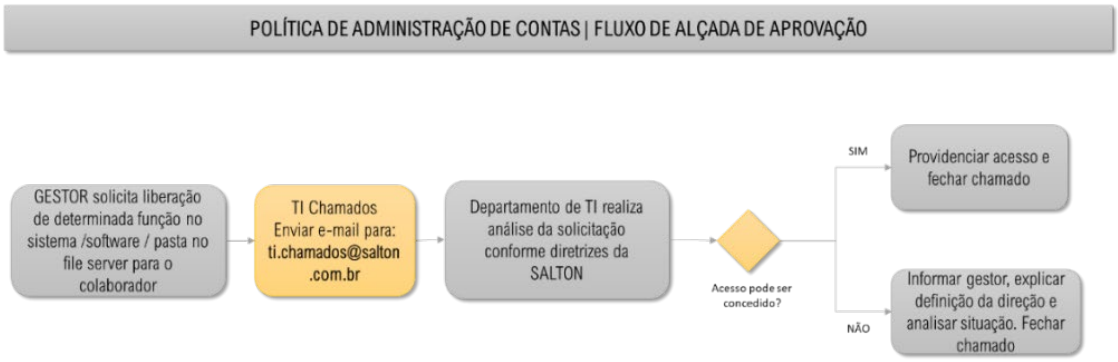
A Lei Geral de Proteção de Dados (LGPD) estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados de pessoas físicas, impondo proteção e penalidades para o não cumprimento. A SALTON a fim de cumprir com as determinações aplicadas à LGPD, estabelece uma POLÍTICA PRÓPRIA para tratar acerca das regras de Privacidade que deverão ser adotadas pela SALTON bem como papéis e responsabilidades pela Segurança da Informação.

5.3.1 Comitê de privacidade e segurança da informação (CPSI)

A SALTON estruturou um Comitê de Privacidade e Segurança da Informação (denominado CPSI), que atuará nas temáticas de “Privacidade” e de “Segurança da Informação”, exercendo um papel tático e estratégico na empresa, se reportando diretamente à Direção e auxiliando a SALTON no acompanhamento de assuntos estratégicos, no cumprimento da legislação aplicável, estabelecendo políticas, diretrizes, avaliação de riscos, avaliação de ações, avaliação de incidentes e problemas, definição de estratégia, disseminação da cultura e além de garantir recursos para a segurança e da privacidade de dados.
As definições específicas acerca das suas frentes de atuação, critérios para nomeação dos membros, mandato, competências, reuniões e suas deliberações, estão definidas em documento próprio denominado REGIMENTO INTERNO DO COMITÊ.

5.4 ADMINISTRAÇÃO DE CONTAS

A SALTON estabelece diretrizes gerais para acesso a ativos, softwares e sistemas informatizados da empresa. Toda permissão de acesso é de responsabilidade e deve ser solicitada ao departamento de TI, sendo este concedido conforme alçada de aprovação e necessidade do perfil para a execução de suas atividades profissionais. A alçada de aprovação e liberação de acesso seguem um fluxo pré-estabelecido conforme determina esta Política:



5.4.1 Gestão de identidades e controle de acessos

Este tópico visa estabelecer diretrizes e procedimentos para a criação, gerenciamento e controle de acessos às identidades digitais dos usuários da empresa SALTON. Esta diretriz busca garantir que o acesso a sistemas, dados e recursos seja concedido de forma segura e adequada, alinhando-se aos princípios de segurança da informação, especialmente à confidencialidade, integridade e disponibilidade.
E aplicável a todos os colaboradores, prestadores de serviço, fornecedores, consultores e terceiros que utilizam sistemas e recursos da empresa SALTON. Aplica-se também a todos os sistemas, aplicativos, redes e dispositivos que requerem autenticação e autorização de acesso.
A SALTON estabelece como forma de identificação de todo o usuário o login e senha no AD (Active Directory).
Os procedimentos de criação, manutenção, bloqueio e revogação estão descritos a seguir e devem ser seguidos por todos os usuários que se autentiquem no AD:

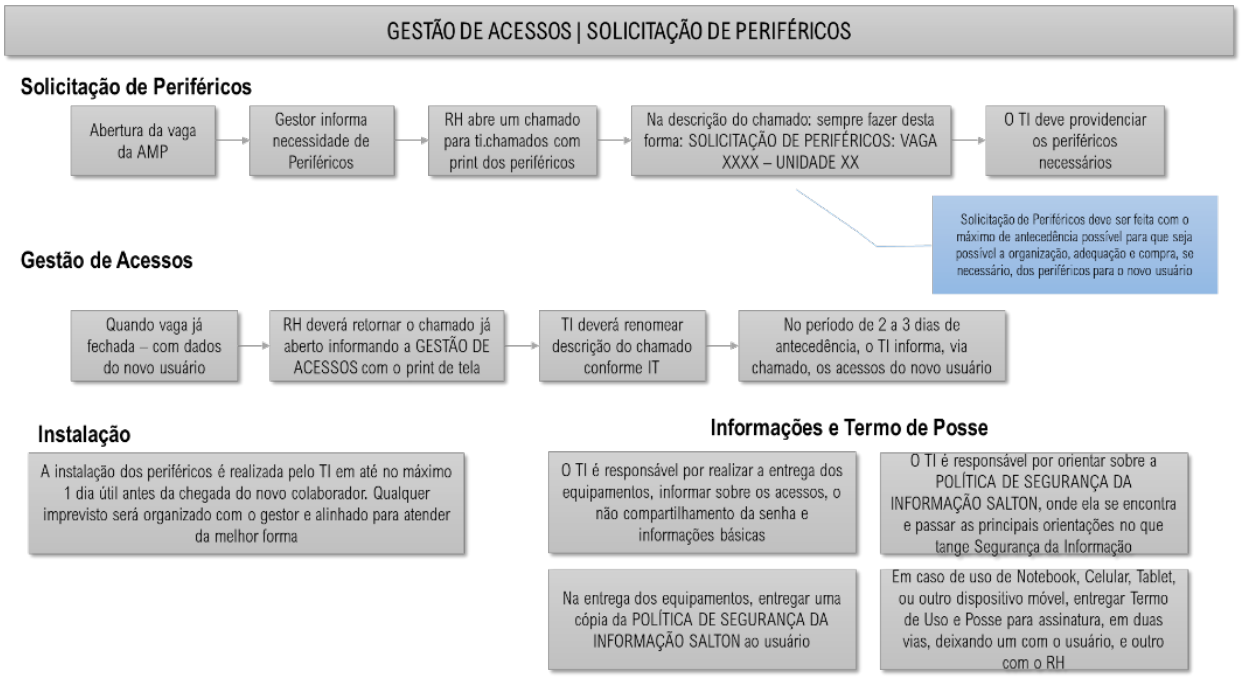
- A SALTON determina como padrão a criação de login de usuário como nome, sobrenome;
- O login e senha são pessoais e intransferíveis;
- Cada usuário do AD, pertencerá a um grupo específico, ou seja, ao seu setor;
- O usuário poderá ter acesso a outras pastas dentro do File Server mediante autorização da Gestão de Acessos e alçada de aprovação citada no fluxo acima;
- Aprovações especiais, que necessitem de alçada de aprovação superior ao do gestor podem ser solicitadas, e serão comunicadas as partes interessadas.

5.4.1.1 Criação de conta para novos usuários

Este tópico tem como objetivo normatizar o fluxo de criação de contas em tempo hábil, para a entrada de novos colaboradores na empresa. A seguir vê-se o fluxo e detalhamento, com as diretrizes a serem seguidas pelos gestores, RH, TI e demais partes envolvidas.

- O Gestor preencherá a AMP, informando primeiramente sobre a necessidade de periféricos, softwares e caso já tenha os dados do novo usuário;
- O RH por sua vez, enviará a parte onde consta os dados quanto as necessidades dos periféricos na AMP, via chamado (ti.chamados@salton.com.br) para o TI, sendo os tempos considerados:
    - Para Compra de Periféricos, solicita-se 30 dias de antecedência da abertura do chamado;
    - Para Gestão de Acessos, solicita-se uma semana de antecedência da entrada do novo colaborador;

- Caso tenha compra / configuração de softwares e licenças especiais, solicita-se duas semanas de antecedência a entrada do novo colaborador.

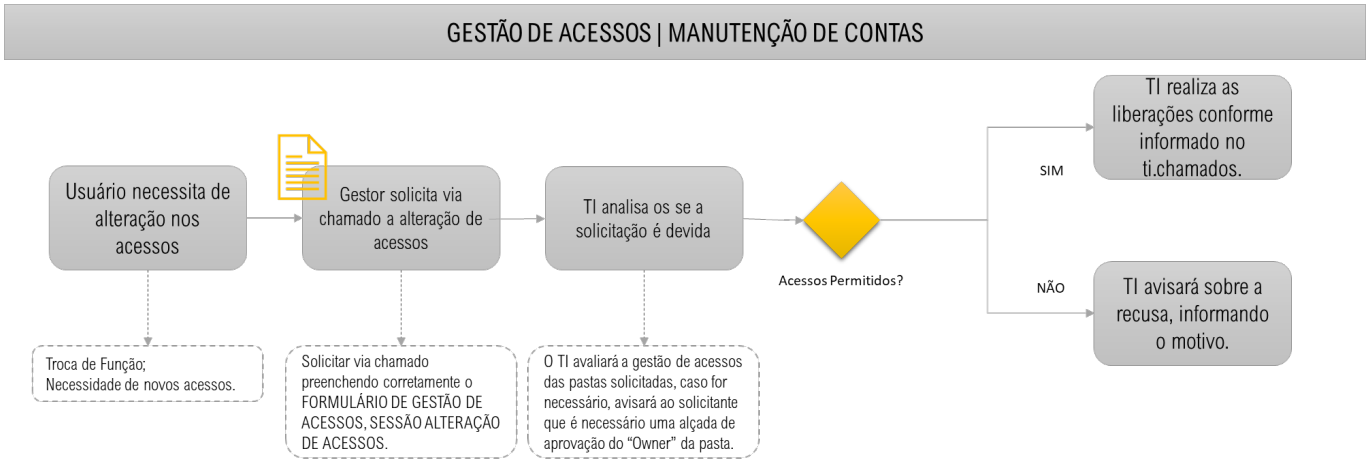


5.4.1.2 Princípio de menor privilégio

- Concessão de Acessos:
  - Os usuários terão acesso apenas aos recursos e sistemas que são essenciais para a execução de suas atividades diárias, evitando permissões desnecessárias ou excessivas;
  - O acesso a sistemas críticos ou dados sensíveis será restringido a usuários especificamente autorizados.
- Solicitação de Acesso Adicional:
  - Caso um usuário necessite de acesso a novos sistemas ou permissões adicionais, uma solicitação formal deverá ser feita e aprovada pelo gestor imediato e pela equipe de TI/Segurança da Informação;
  - Qualquer acesso adicional concedido será revisto regularmente para garantir que continue sendo necessário.

5.4.1.3 Manutenção de contas (alteração de acessos)

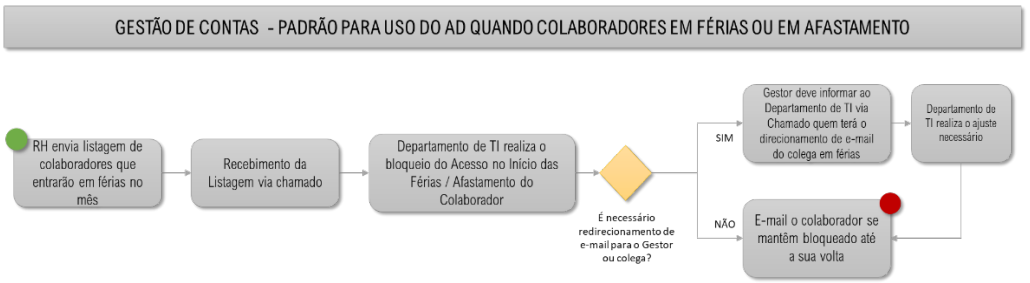
A manutenção na conta do usuário deve ser realizada sempre que houver troca de setor, alteração de função ou necessidade de acesso a pastas, sistemas ou informações diferentes daquelas já utilizadas. Nessas situações, o gestor da nova área deverá abrir chamado à TI, indicando os acessos necessários para a nova função e solicitando, no mesmo chamado, a revogação dos acessos antigos que não sejam mais necessários.



Qualquer necessidade diferente das situações descritas nesta política deve ser previamente acordada com a Diretoria e formalizada por meio de chamado.

5.4.1.4 Colaborador em férias, afastamento

É determinado pela SALTON que o colaborador em férias ou afastamento deve ter seu perfil bloqueado no AD.
Isto implica que o colaborador, gestor e colegas não tem acesso ao seu computador, e-mail ou documentos salvos no U:\.
Todo e qualquer documento referente as atividades laborais, deve estar salvo no diretório do setor (S:\), evitando inconvenientes no período em que o colaborador não estiver na empresa.
Redirecionamento de e-mail, com informação de aviso de férias, é obrigatório, informando a quem deve-se redirecionar o e-mail.
Fica estabelecido o seguinte fluxo:



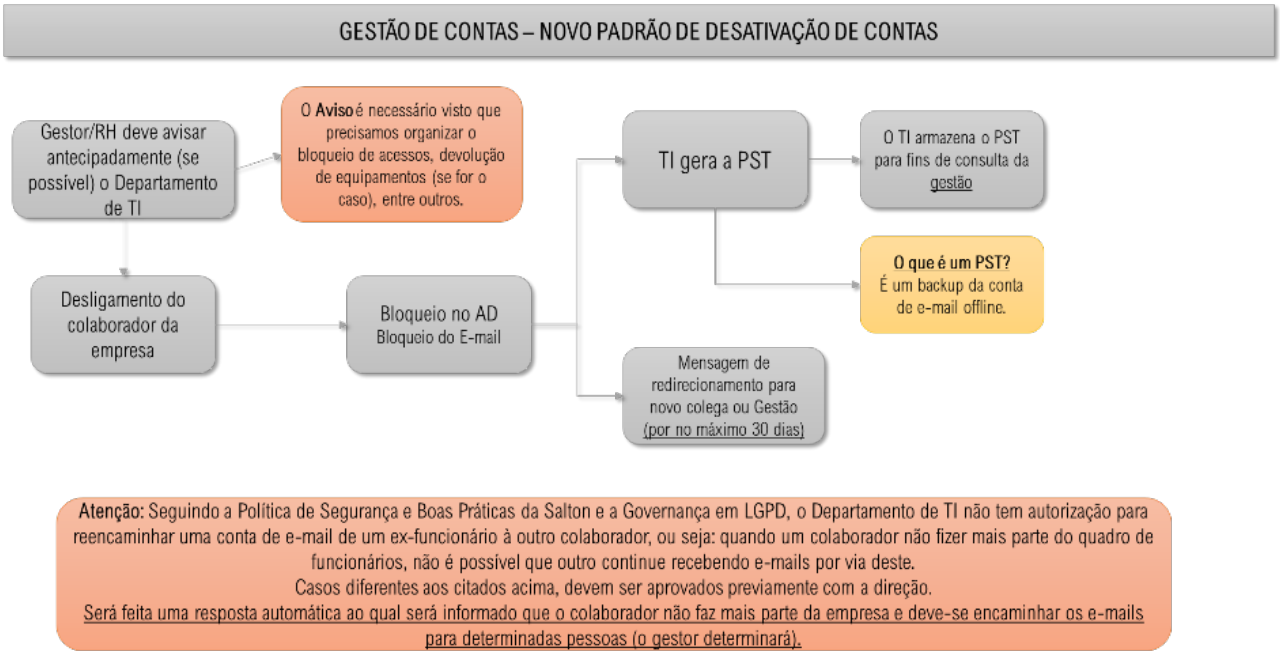
O **login e a senha do colaborador são pessoais e intransferíveis**, sendo expressamente proibido o seu compartilhamento com colegas, terceiros ou qualquer outra pessoa. O colaborador poderá ser responsabilizado por todas as ações realizadas com o uso de suas credenciais, inclusive em caso de uso indevido, irregular ou ilícito.
Todos da SALTON devem atender as diretrizes assim descritas nesta Política conforme abaixo:

- Os novos "e-mails recebidos" devem ser direcionados para o colega que o substituirá durante este período, **com um aviso informando** que os assuntos serão atendidos pelo colega em questão;
- O colega que assumirá as demandas, precisa ter (com o seu usuário e senha próprios), os mesmos acessos a sistemas, aplicativos, servidor de arquivos, nuvem e afins, para atender as demandas neste período. Ou seja, ao sair de férias, o departamento de TI deve ser acionado, caso seja necessário para realizar estes ajustes;

- Em nenhuma hipótese o colaborador deve ter acesso a conta de e-mail, usuário e senha e nem fazer login no computador do colega que se ausentou. Todas as ações devem ser feitas com seu usuário próprio, conforme regras de segurança expressamente descritas nesta Política.

5.4.1.5 Desligamento de colaborador (revogação de acesso)

A Política de Segurança da Informação prevê procedimento de Revogação de Acessos que deve ser seguido no momento de desligamento de colaboradores, ao qual garante a segurança das informações da empresa e está de acordo com os princípios da LGPD.
Fica estabelecido pela SALTON o procedimento citado a seguir como padrão para tramite de bloqueio do AD e da conta de E-mail no momento de desligamento do colaborador.
Qualquer necessidade diferente a descrita nesta política deve ser previamente acordada com a diretoria e solicitada via chamado.



A seguir detalhamento:
- O RH deve avisar o departamento de TI a respeito do desligamento via chamado;
- O RH deve informar ao departamento de TI se haverá substituição, realocação, ou se os equipamentos deverão ser recolhidos;
- O departamento de TI fará o bloqueio da conta deste usuário, o que implica o não acesso ao computador e ao e-mail;
- Neste computador e e-mail serão feitos backups para garantir que a informação contida e empresarial seja armazenada de forma segura;
- O gestor da área pode solicitar a qualquer momento o acesso ao conteúdo do computador e e-mail (histórico);
- Será feita uma mensagem de encaminhamento informando a saída do colaborador, direcionando os e-mails para os colaboradores que o gestor determinar;
- Casos diferentes dos citados acima, devem ser aprovados previamente com a direção e solicitado via chamado para o departamento de TI.

5.4.1.6 Casos específicos de revogação de acesso

Usuários pertencentes ao setor de TI: como medida de segurança, adota para SALTON, mediante o desligamento de um membro da equipe de TI da SALTON, o gestor de TI deverá imediatamente providenciar o "Reset" de todas as senhas gerenciais e administrativas ao qual este usuário tenha acesso.

5.4.1.7 Revisão de acessos

- O acesso de todos os usuários será revisado no mínimo uma vez ao ano, para garantir que permaneçam adequados e alinhados às funções do colaborador;
- Gestores de departamentos e a equipe de TI/Security serão responsáveis por verificar se os acessos continuam necessários ou precisam ser ajustados.

5.5 NORMATIZAÇÃO DO ACESSO REMOTO (VPN)

Este tópico tem como objetivo definir diretrizes claras para a utilização segura do acesso remoto à rede corporativa da SALTON.
O uso do acesso remoto (VPN) somente é concedido mediante prévia aprovação do gestor e da direção imediata, para casos de home office ao qual o colaborador tenha a autorização para este acesso.
- O acesso remoto às estações de trabalho, é restrito e seu funcionamento ocorre de segunda à sexta-feira, das 7h00 às 19h00;
- Atividades fora deste padrão devem ser notificadas previamente, pelo gestor do departamento, através de abertura de chamado, com autorização da direção;
- Todos os usuários são responsáveis pela proteção de suas credenciais de acesso e pela segurança de seus dispositivos de conexão;
- O acesso remoto à rede corporativa da empresa SALTON deve ser realizado exclusivamente através da VPN homologada pela empresa;
- A conexão VPN deve ser estabelecida obrigatoriamente antes de qualquer tentativa de acesso a sistemas, arquivos ou aplicativos corporativos;
- A VPN utilizará criptografia de alto nível (SSL/TLS) para proteger as comunicações entre o dispositivo remoto e a rede interna;
- Tentativas de conexão à rede corporativa sem a VPN serão automaticamente bloqueadas pelos sistemas de segurança;
- É proibido o uso de VPN de terceiros ou soluções alternativas para acessar a rede da empresa;
- O uso de equipamentos e periféricos da SALTON para uso em home office, deve ser concedido pelo gestor da área, informado via chamado para o setor de TI que analisará a viabilidade do uso em home office;
- Não é permitido o uso de computadores e notebooks pessoais para acesso remoto;
- Em caso de perda ou comprometimento de credenciais, o usuário deve notificar a equipe de TI imediatamente para realizar o bloqueio e redefinição das credenciais.

5.5.1 Princípio de menor privilégio

- Os usuários terão acesso remoto apenas aos sistemas e recursos estritamente necessários para a execução de suas funções;
- A atribuição de permissões será feita com base no princípio do menor privilégio, garantindo que os usuários não tenham mais acessos do que o necessário.

5.5.2 Monitoramento e registro de atividades

- Todo o tráfego e as atividades relacionadas ao acesso remoto serão monitorados e registrados pelos sistemas de monitoramento do Firewall da Salton;
- A equipe de Segurança da Informação realizará auditorias regulares nos logs de acesso remoto para identificar comportamentos anômalos ou não autorizados;
- Os softwares de monitoramento estão continuamente monitorando atividades e possíveis ameaças nos endpoints, reportando à equipe de segurança qualquer atividade suspeita;
- A solução de caça ameaças, através da integração de Firewall, estará continuamente monitorando atividades e possíveis ameaças nos firewalls, reportando à equipe de segurança qualquer atividade suspeita;
- As integrações dos diversos softwares de monitoramento e caça ameaças que a empresa possui estão continuamente monitorando atividades e possíveis ameaças de rede como shadow IT, tráfego de IOT, redes wifi e outros tráfegos de dispositivos que não possuem endpoint Sophos, reportando à equipe de segurança qualquer atividade suspeita;
- Qualquer atividade suspeita ou tentativa de violação será reportada imediatamente e investigada pela equipe de resposta a incidentes.

5.5.3 Acesso remoto por terceiros

Todo o acesso externo a sistemas, banco de dados e aplicações, por parte de terceiros, deve ser realizado exclusivamente via TeamViewer, mediante o conhecimento prévio e acompanhamento do TI.
O acesso a terceiros via VPN deve ser realizado com supervisão da equipe de TI e por um usuário responsável, sendo:

- Nenhum terceiro deve ter acesso a banco de dados ou informações sigilosas que não sejam pertinentes ao processo avaliado;
- Nenhum terceiro deve ter privilégios de administrador;
- O acesso remoto deve ser realizado exclusivamente pela ferramenta TeamViewer;
- É necessário agendamento prévio com a área de TI para acompanhamento do serviço terceirizado;

5.5.4 Desconexão segura

- Ao término do trabalho, o usuário deve se desconectar adequadamente da VPN e fechar todas as sessões de acesso remoto;
- Conexões inativas por mais de 30 minutos serão encerradas automaticamente como medida de segurança.

5.5.5 Restrições e limitações

- O acesso remoto deve ser utilizado exclusivamente para fins profissionais e em conformidade com as políticas internas de uso de TI;
- É estritamente proibido utilizar a conexão VPN para acessar redes ou recursos não relacionados ao trabalho.

5.5.6 Acesso a locais públicos

- É proibido acessar a rede corporativa por meio de redes públicas não seguras, como redes Wi-Fi de cafés, aeroportos, eventos ou outros ambientes de acesso compartilhado. Quando houver necessidade de acesso externo, inclusive por colaboradores em atividade comercial ou em deslocamento, o usuário deverá utilizar alternativas

seguras, como rede móvel própria, ponto de acesso pessoal protegido por senha ou outro meio previamente autorizado pela TI, observadas as orientações de segurança aplicáveis;

- Em caso de necessidade de acesso em locais públicos, o usuário deve garantir que o ambiente físico também é seguro, evitando o uso de computadores públicos ou o compartilhamento de tela com terceiros.

5.6 POLÍTICA DE ADMINISTRAÇÃO DE SENHAS

As senhas são consideradas o meio de autenticação necessário. Os usuários devem contribuir com a eficiência do sistema de gestão de senhas seguindo as boas práticas a seguir:

- O **login e a senha do colaborador são pessoais e intransferíveis**, sendo expressamente proibido o seu compartilhamento com colegas, terceiros ou qualquer outra pessoa. O colaborador poderá ser responsabilizado por todas as ações realizadas com o uso de suas credenciais, inclusive em caso de uso indevido, irregular ou ilícito;
- Ter no mínimo 12 caracteres;
- Conter pelo menos uma letra maiúscula (A-Z);
- Conter pelo menos uma letra minúscula (a-z);
- Conter pelo menos um número (0-9);
- Conter pelo menos um caractere especial (!@#$%^&*(),.?":{}|<>);
- Não pode conter sequências óbvias (exemplo: 123456, abcdef, qwerty);
- Não pode conter informações pessoais, como nome, sobrenome, data de nascimento ou CPF;
- Não é permitido repetir as últimas cinco (5) senhas;
- Utilizar um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local, em hipótese alguma;
- Não é permitido anotar a senha em papel ou em outros meios de registro de fácil acesso;
- Não é permitido salvar suas senhas em documentos de rede (Word / Excel);
- As senhas não podem ser expostas em meio físico ou virtual;
- Habilitar, sempre que disponível, o uso de duplo fator de autenticação;
- Caso haja suspeita de comprometimento da senha, deve ser alterada imediatamente.
- Sempre bloqueie a tela do dispositivo ao se afastar do computador;
- A Salton dispõe de um cofre de senhas dentro do Protheus chamado Vault, para o uso deste, consulte o TI que ensinará sobre seu uso.

A concessão de senhas deve ser controlada, considerando:

- Senhas temporárias devem ser alteradas imediatamente e não devem ser armazenadas de forma desprotegida;
- Todo o usuário terá aviso de redefinição de senha a cada 30 dias;
- A Salton e o TI reservam o direito de a qualquer momento solicitar a troca da senha fora do prazo estipulado, caso for necessário;
- São de responsabilidade do usuário os cuidados com a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida.

Tudo que for executado com o login e senha de usuário da rede ou de outro sistema será de inteira responsabilidade do usuário, sendo que o colaborador poderá ser responsabilizado por todas as ações (inclusive ilícitas), executadas por seu “usuário”.

Todo conteúdo corporativo produzido, armazenado, transmitido ou recebido por meio dos recursos, sistemas, contas, dispositivos e ambientes tecnológicos disponibilizados pela empresa poderá ser acessado, monitorado e analisado pela organização, sempre que necessário, para fins de compliance, auditorias, investigações internas, apuração de incidentes, atendimento a requisitos legais ou regulatórios e verificação do cumprimento das políticas internas. O uso dos recursos corporativos implica ciência e concordância do colaborador quanto à possibilidade dessas verificações.

5.6.1 Falhas de autenticação

Para proteger contra acessos não autorizados, serão aplicadas as seguintes medidas em caso de falha na autenticação:

- Se um usuário errar a senha 5 vezes consecutivas, a conta será bloqueada temporariamente por 3 minutos. Após o tempo de bloqueio, o usuário poderá tentar novamente;
- Se o erro persistir após mais 5 tentativas consecutivas, a conta poderá ser bloqueada permanentemente, exigindo a redefinição da senha pelo setor de TI;
- Caso ocorra um número elevado de falhas de autenticação em diversas contas, o setor de segurança da informação será acionado para investigar possíveis ataques.

5.6.2 Monitoramento e vazamento de credenciais

- A equipe de segurança da informação monitora constantemente possíveis vazamentos de credenciais associadas à organização;
- Caso uma credencial vazada seja identificada, o usuário afetado será notificado imediatamente para realizar a troca de senha com urgência;
- Dependendo do risco identificado, a conta poderá ser temporariamente bloqueada até que a senha seja alterada;
- O uso de senhas vazadas é estritamente proibido, e os sistemas corporativos podem impedir a reutilização dessas credenciais.

5.6.3 Responsabilidades dos usuários

- Criar senhas seguras conforme esta política;
- Alterar a senha dentro do prazo estabelecido;
- Notificar o setor de TI imediatamente em caso de suspeita de comprometimento;
- Nunca utilizar a mesma senha para contas pessoais e corporativas;
- Nunca compartilhar seu login e senha com colegas, terceiros ou qualquer outra pessoa.

5.7 REGRAS PARA UTILIZAÇÃO DE E-MAIL

Este tópico visa definir normas de utilização do e-mail corporativo, abrangendo o envio, o recebimento e o gerenciamento das contas de e-mail do domínio @salton.com.br. A utilização do e-mail corporativo deve ocorrer exclusivamente para fins profissionais, observadas as diretrizes desta política e as orientações de segurança da informação aplicáveis.

É expressamente proibido conectar, configurar, sincronizar ou acessar o e-mail corporativo em dispositivos pessoais, incluindo celulares, notebooks, tablets ou quaisquer outros equipamentos particulares, salvo autorização formal e prévia da empresa, com validação da área de TI e aplicação dos controles de segurança necessários. Todos os colaboradores devem observar as diretrizes abaixo:

- As diretrizes estipuladas a respeito à administração de senhas dizem respeito também ao acesso aos e-mails do usuário;
- **O login e a senha do colaborador são pessoais e intransferíveis**, sendo expressamente proibido o seu compartilhamento com colegas, terceiros ou qualquer outra pessoa. O colaborador poderá ser responsabilizado por todas as ações realizadas com o uso de suas credenciais, inclusive em caso de uso indevido, irregular ou ilícito;
- Todo tráfego de e-mail (entrada e saída) é passível de monitoramento e armazenamento em repositórios que permitam a auditoria interna e externa, estando sujeito à avaliação à critério da empresa (Direção, DPO, Jurídico, Compliance e Departamento de TI), quando necessário, a qualquer momento e sem necessidade de prévio aviso;

- Todo o conteúdo produzido no e-mail corporativo é de propriedade da SALTON, e desta forma, não é permitido utilizar o e-mail corporativo para fins pessoais em hipótese alguma;
- Não devem ser enviadas informações confidenciais ou restritas da empresa através de e-mail, cujo conteúdo não possa tornar-se público;
- Ao receber e-mails de origem externa da companhia, o usuário não deve clicar em links, abrir arquivos ou anexos, a menos que reconheça o remetente e confirme que o conteúdo é absolutamente seguro. E-mails contendo links ou arquivos suspeitos devem ser encarados como potenciais ameaças e encaminhados para o departamento de TI;
    - Não é permitida a abertura de anexos de e-mail com as seguintes extensões: .exe, .com, .bat, .src, .pif, .dat, .ini, .sys, .key e .scr, por se tratarem, em grande parte dos casos, de vírus ou programas maliciosos. Caso a empresa julgue necessário, poderá haver bloqueios de outras extensões que comprometam o desempenho da rede ou perturbem o bom andamento dos trabalhos, sem prévio aviso;
- Caso a SALTON julgue necessário, haverá bloqueios de e-mail com arquivos anexos que comprometam o uso de banda ou prejudiquem o bom andamento dos trabalhos;
- É obrigatória a manutenção da caixa de e-mail por parte do usuário (caixa de entrada, itens enviados, itens excluídos) evitando acúmulo de e-mails e arquivos desnecessários. O departamento de TI poderá realizar intervenção, caso julgue necessário;
- É proibido o cadastramento do e-mail de domínio corporativo fornecido pela empresa (@salton.com.br) em sites que não tenham a finalidade de trabalho ou relacionados às atividades da empresa. Todo o cadastramento deverá ser aprovado previamente pelo gestor e acompanhado pelo departamento de TI;
- É proibido o envio igual ou superior à 50 destinatários de e-mail numa mesma mensagem. Isto será caracterizado como prática de "spam". Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, exceto autorizadas pela diretoria ou gestão da área;
- É proibido enviar, reenviar, encaminhar ou, de qualquer forma, propagar mensagens em “cadeia”, ou "pirâmides", ou “correntes”, independentemente da vontade do destinatário de receber tais mensagens, assim como e-mails com conteúdo pornográfico, racista, discriminatório, religioso ou que não tenham relação com o conteúdo de trabalho, ou não sejam relacionados ao interesse da empresa. São proibidas mensagens profanas, obscenas, indecentes, lascivas, materiais que explícita ou implicitamente se refiram à conduta sexual, incitações raciais, que constituam apologia ao fanatismo, demais conteúdos ilegais ou que possam de alguma forma ofender demais pessoas. Também é proibida a utilização do correio eletrônico para exercer o direito de liberdade de expressão;
- É proibido se utilizar de práticas que visem ocultar sua verdadeira identidade no envio de e-mails;

A SALTON reserva-se ao direito de suspender ou revogar o acesso e utilização de qualquer e-mail sob seu domínio, a qualquer tempo e sob seu critério, sem a necessidade de aviso prévio.

5.8 DIRETRIZES DE UTILIZAÇÃO DE REDE

Esse tópico define as normas de utilização da rede SALTON que abrange login, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso. Estes itens são tempestivos a todos os usuários de sistemas, ambientes e redes de computadores da SALTON.

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- Não utilize login e senha que não sejam suas para acesso a computadores ou sistemas;
    - **O login e a senha do colaborador são pessoais e intransferíveis**, sendo expressamente proibido o seu compartilhamento com colegas, terceiros ou qualquer outra pessoa. O colaborador poderá ser responsabilizado por todas as ações realizadas com o uso de suas credenciais, inclusive em caso de uso indevido, irregular ou ilícito;

- Casos excepcionais de acesso ao sistema com login compartilhado somente serão permitidos mediante aprovação formal da Direção, do DPO, quando aplicável, observados os controles de segurança, rastreabilidade e finalidade do acesso. As informações relacionadas a esses acessos poderão ser analisadas para fins de auditoria, investigação interna, apuração de incidentes e verificação de conformidade com as políticas internas;

- Todo o tráfego de informações realizado por meio dos recursos, sistemas, contas, dispositivos e ambientes tecnológicos disponibilizados pela empresa poderá ser monitorado e deverá ser armazenado em repositórios que permitam rastreabilidade, auditoria interna e auditoria externa, conforme avaliação e critério da empresa, incluindo Direção, Jurídico, Compliance, Departamento de TI e RH, quando aplicável;
- As pastas dos setores e usuários são monitoradas pelo Departamento de TI com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos em todos os diretórios da SALTON;
- Não é permitido criar ou remover arquivos fora da área alocada ao usuário que possam comprometer o desempenho e funcionamento dos sistemas;
- Não é permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam interferir no funcionamento do servidor;
- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor ou tentativas de "invadir" um servidor;
- É estritamente proibida a utilização de técnicas que comprometam o desempenho e funcionamento da rede – práticas hackers/crackers;
- É responsabilidade do usuário manter as informações da SALTON armazenadas nos locais de compartilhamento, onde é efetuado o backup diário.

5.9 DIRETRIZES DE ARMAZENAMENTO E COMPARTILHAMENTO DE DADOS

A empresa institui como Política de Armazenamento e Compartilhamento de Dados o uso do File Server e File Sync como forma de armazenar e compartilhar documentos internos corporativos.
A estrutura de pastas do File Server e do File Sync obedecem às diretrizes estabelecidas pela SALTON, sendo elas apresentadas a seguir:
G:\ Salton (File Server) ou F:\ Salton (File Sync): Os documentos devem ser salvos nas pastas específicas e corretas, evitando a duplicidade no armazenamento de informações e garantindo assertividade quanto as versões dos documentos;
No File Server: Deve-se armazenar arquivos referentes ao setor, que são para histórico ou com pouco uso;
No File Sync: Deve-se armazenar arquivos referente ao setor, de uso diário e relevantes para o andamento dos trabalhos;
Pastas Segregadas: São pastas que contêm assuntos específicos que estão atrelados a mais de um setor, ao qual pessoas específicas tem acesso;
A solicitação e por consequência a criação de novas pastas segregadas é avaliada pelo departamento de TI e direção, com o intuito de averiguar o correto posicionamento dentro da Matriz de Acessos.
Pastas Setoriais: Toda documentação inerente ao setor deve ser armazenada de forma organizada dentro da pasta Setorial. É expressamente proibido manter documentos do setor nas áreas de trabalho.
Pasta do Usuário: Nesta pasta, o colaborador deve salvar documentos de uso diário e transitório, relativos à empresa, que não estejam vinculados diretamente as atividades do setor.
Público: Nesta pasta não é permitido salvar documentos confidenciais, com informações pessoais ou sensíveis em hipótese alguma.
Toda sexta-feira os documentos nesta pasta são excluídos e por isto, não se deve manter documentos importantes.
Esta pasta tem como finalidade apenas o trânsito provisório de documentos e deve ser utilizado com cautela seguindo as definições desta Política e da LGPD.

Scanner: O setor é responsável pela limpeza desta pasta e do cuidado na armazenagem dos arquivos que se encontram nele.

5.9.1 Manutenção de conteúdos nas pastas

- A manutenção de documentos e conteúdos é de responsabilidade de cada setor e de seus usuários;
- Nas pastas do setor deve-se armazenar toda documentação referente ao setor e zelar pela manutenção dos conteúdos, organizando subpastas em assuntos específicos. Deve-se também evitar a duplicidade de documentos, e avaliar periodicamente se todo conteúdo armazenado é necessário, evitando o acúmulo de documentos;
- O compartilhamento Público não deve ser utilizado para armazenamento de arquivos que contenham assuntos ou dados sigilosos, de natureza pessoal ou sensível;
    - Somente usar o compartimento do Público para trânsito de arquivos temporários.

5.9.2 Compartilhamento de documentos e informações

- O trânsito de documentos e informações, devem inicialmente ser feitos através de e-mail corporativo, respeitando o grau de sigilo e confidencialidade destacado nesta política;
- Nos casos em que os arquivos são maiores que a capacidade de envio via e-mail, a SALTON estabelece como ferramenta homologada para compartilhamento de documentos o OneDrive;
- É proibido o compartilhamento de documentos da SALTON em e-mails, contas ou equipamentos pessoais. Todas as informações da SALTON estão regulamentadas pelo termo de confidencialidade e seu tráfego fora dos canais indicados é proibido;
- É proibido o compartilhamento de documentos da empresa por meio de ferramentas não autorizadas ou gratuitas (exemplo WeTransfer);
- Nenhuma informação pessoal poderá ser utilizada, salva, gravada ou mantida nos servidores da SALTON. Toda a informação disponibilizada no ambiente SALTON é considerada de uso corporativo. A SALTON reserva-se o direito de excluir qualquer informação de seu ambiente, a seu critério e sem necessidade de aviso prévio;
- É expressamente proibido criar, armazenar e manipular arquivos com senhas dentro da rede (pastas) da Salton, sejam elas no File Server ou principalmente em armazenamento local;
    - A aplicação homologada e única para salvar senhas na SALTON é o VAULT SALTON;
    - Caso o setor precise cadastrar senhas, entrar em contato com o TI solicitando acesso a este módulo e explicação de como ele funciona.

5.9.3 Uso do OneDrive

- No OneDrive o colaborador deve salvar documentos de uso diário e transitório, relativos à empresa, que não estejam vinculados diretamente as atividades do setor;
- É permitido o compartilhamento de documentos referentes a assuntos empresariais que necessitem de compartilhamento e edição simultâneas por mais de uma pessoa;
- Documentos internos e corporativos somente podem ser compartilhados com usuários internos da SALTON, com fim específico;
- Arquivos maiores que a capacidade de envio através de e-mail, cujo conteúdo possa ser compartilhado com terceiros;
- É proibido o compartilhamento de documentos de natureza sigilosa, pessoal ou sensível, salvo com autorização da direção ou DPO da empresa;
- Documentos, procedimentos, instruções de trabalho devem ser armazenados em mantidas no servidor de arquivos;

- O uso do OneDrive deve ser realizado de maneira segura, sendo permitido compartilhamento de informações a usuários específicos;
- Não é aconselhado compartilhar de forma pública, sendo mais seguro especificar as pessoas que podem receber a informação;
- Caso seja necessário o compartilhamento de um link para diversos usuários, certifique-se que está enviando para as pessoas certas.

5.10 BACKUP

O Backup diário é realizado nos seguintes ambientes:
P:\ - SALTON
P:\ - Pastas Segregadas e Setoriais
U:\ - Pasta do Usuário
Z:\ - Scanner

- É de responsabilidade de cada usuário o armazenamento dos arquivos inerentes à empresa no servidor de arquivos para garantir seu backup;
- Os arquivos salvos na Área de Trabalho (Desktop) não possuem backup. Documentos que estiverem na área de trabalho não são passíveis de restauração em caso de perdas;
    - Tendo em vista que os arquivos/documentos referentes ao trabalho devem estar armazenados nos diretórios (Setor/Usuário), é excluída toda e qualquer responsabilidade do setor de TI em perdas de arquivos/documentos existentes na área de trabalho. A mesma regra é aplicada quando há necessidade de formatação do computador;
- Todos os arquivos inerentes a empresa devem ser salvos dentro do servidor de arquivos, onde possuem backup diário e elevados controles de segurança e restauração.

5.11 USO DAS ESTAÇÕES DE TRABALHO

Denomina-se estação de trabalho todo o equipamento de TI utilizado pelo colaborador, bem como todos os seus acessórios, tais como: computador, notebook, monitor, teclado, mouse, tablet, telefone, smartphones, leitores ópticos, HD externo, headphone, headset, entre outros. Esta lista é extensiva a outros itens que possam compor a infraestrutura de trabalho pertencente a empresa e oferecida ao colaborador para o desempenho das suas respectivas funções, portanto:

- Todo equipamento recebido é para uso profissional, sendo assim, é responsabilidade do usuário manter a integridade, limpeza e cuidados gerais com os dispositivos;
- Tenha o cuidado de bloquear o computador ao se afastar de sua mesa;
- Grave os arquivos na pasta do setor (servidor de arquivos), evite área de trabalho, já que não são feitos backups desta área;
- Tenha cuidado ao ingerir alimentos e bebidas próximo de seus equipamentos. Caso ocorra um acidente, é possível que o equipamento seja danificado e necessite de conserto. Caso tenha alguma ocorrência neste sentido, informe o departamento de TI imediatamente;
- Manter a tela inicial dos dispositivos eletrônicos limpa, sem nenhum documento solto sobre a tela inicial, apenas com os atalhos à internet e aplicativos utilizados diariamente;
- Tenha cuidado ao manusear os equipamentos. Cabos, por exemplo, são sensíveis e podem ser danificados aos serem torcidos;
- Não instale, manipule ou movimente computadores (desktops), equipamentos ou periféricos. Estes processos são de responsabilidade da área de TI e devem ser solicitados via abertura de chamados;

- Programas e softwares não homologados pela SALTON também não devem ser instalados pois não foram avaliados e podem não conter o nível de segurança estipulado pela empresa;
- Faça a troca de senhas e atualizações solicitadas pelo dispositivo no mínimo uma vez ao mês;
- Sendo patrimônios da empresa, fica vedada qualquer interferência, alteração e/ou objeção do usuário, em relação a possíveis remanejamentos ou substituições que possam vir a acontecer com sua estação;
- O remanejamento das estações deve ser solicitado via chamado ao departamento de TI;
- Quando há movimentação ou término de contrato de trabalho, o departamento de TI deve ser comunicado pelo gestor para que este recolha os equipamentos e periféricos, com o intuito de realizar as devidas manutenções e atualizações necessárias;
- A utilização das estações se resume aos trabalhos advindos para única e exclusivamente, a atenderem as necessidades da empresa, salvo em períodos fora do expediente (horários de almoço), onde o usuário poderá beneficiar-se da infraestrutura para navegação na internet, desde que esse feito particular não comprometa a integridade de dados entre outros documentos de manipulação interna da empresa, e que possam vir a prejudicar a mesma de alguma forma;
- É dever do usuário zelar pelo bom funcionamento dos equipamentos entregues, garantindo sua vida útil. Mediante qualquer avaria, deve-se comunicar imediatamente o TI, informando o ocorrido.

5.12 MESA LIMPA TELA LIMPA

Para garantir a confidencialidade dos dados tratados e evitar incidentes envolvendo os dados, tanto pessoais, quanto corporativos, a SALTON espera de seus colaboradores as seguintes medidas preventivas:

- Ao sair do posto de trabalho, deve-se guardar todos os documentos e/ou mídias físicas que estão sobre a mesa;
- Os documentos devem ser guardados de acordo com o nível de confidencialidade da informação;
- Documentos ou mídias físicas com dados corporativos confidenciais ou quaisquer tipos de dados pessoais contidos neles devem ser armazenados em gavetas, ou armários com chaves, em que apenas o responsável pela utilização do documento tenha a chave;
- Documentos ou mídias físicas com dados pessoais sensíveis ou informações críticas à organização devem ser armazenados em cofres;
- Durante o desenvolvimento do trabalho, o colaborador deve certificar-se de que a mesa esteja limpa, de forma que a acessibilidade aos documentos não tome tempo, cumprindo com o princípio da disponibilidade da informação. Além disso, é de responsabilidade do colaborador: Destruir, picotar ou, de qualquer forma, tornar ilegível qualquer documento antes de descartá-lo ou colocá-lo fora.
- Não imprimir documentos apenas com o intuito de ler. Se o objetivo for apenas a leitura, esta deve ser realizada na tela do computador;
- Qualquer impressão deve ser retirada da impressora imediatamente após a impressão ser efetuada;
- Agendas e cadernos com anotações devem ser armazenados em gavetas ou armários com chaves, em que apenas o responsável pela agenda/caderno tenha a chave;
- Limpar a mesa, trancar as gavetas e armários e trancar os cofres ao deixar o posto de trabalho, mesmo que seja para intervalo intrajornada;
- Não deixe senhas a amostra, salvas em arquivos na rede, ou escritas em cadernos ou agendas – para isto utilize o Vault (Cofre de senhas) da Salton – solicite apoio da equipe de TI para a utilização do Vault.

5.13 UTILIZAÇÃO DE COMPUTADORES, NOTEBOOKS E DISPOSITIVOS MÓVEIS CORPORATIVOS

Esse tópico visa definir as normas de utilização de computadores e notebooks corporativos.

- O login e senha do colaborador são pessoais e intransferíveis, sendo que o colaborador poderá ser responsabilizado por todas as ações (inclusive ilícitas), executadas por seu “usuário”;

- Computadores, notebooks e periféricos devem permanecer na SALTON, salvo atividades destinadas a este fim, como home office, viagens, comercial e com autorização da direção;
    - Colaboradores em férias, ausentes ou de licença/afastados devem devolver seus equipamentos que ficarão em posse da SALTON até seu retorno.
- O uso, manuseio ou custódia de equipamentos portáteis da SALTON somente é permitido após aprovação da área de Tecnologia da Informação através do <<"Termo de posse, uso e responsabilidade de bem móvel de propriedade da Vinícola Salton S/A">> e do cumprimento dos requisitos de segurança solicitados. Exemplos de equipamentos portáteis são: notebooks, celulares, entre outros;
- Os dados da SALTON são de propriedade da empresa e, portanto, devem ser mantidos em ativos da empresa. Visando manter a segurança da informação e evitar qualquer tipo de extração ou violação desta Política, resguardando as informações da SALTON, é vedado o uso de qualquer dispositivo externo para cópia ou transferência de informações tais como: CD's, DVD's, mídias regraváveis, pen-drives, entre outros;
- Todas as portas USB's são bloqueadas pelo setor de TI e somente deverão estar acessíveis mediante autorização da direção;
- Não é permitido o uso de computadores, notebooks e dispositivos eletrônicos particulares para fins laborais.

5.14 UTILIZAÇÃO DE IMPRESSORAS

Esse tópico visa definir as normas de utilização de impressoras disponíveis na rede SALTON.

- A responsabilidade pelo zelo e correta utilização dos equipamentos de impressão do complexo é de cada usuário;
- É vedada toda e qualquer possibilidade de alteração do layout da sala onde se encontram os equipamentos de impressão por intermédio do usuário. Quando se fizer necessária alguma alteração, deverá ser enviada uma solicitação via chamado ao setor de TI;
- Além das responsabilidades do usuário citados nos itens formadores desse parágrafo, é ainda seu dever:
    - Não é permitido deixar exposto material impresso que contenha informação sigilosa, pessoal ou de natureza sensível;
    - Ao enviar qualquer arquivo para impressão, verificar na impressora se o que foi solicitado já foi impresso anteriormente;
    - Em caso de erro na impressão, reaproveitar o papel na próxima tentativa. Em caso de impossibilidade de reaproveitamento na impressora, reutilizá-lo então como rascunho;
    - Não deixar impressões erradas na mesa de impressão;
    - Reabastecer as bandejas, caso se faça necessário, independendo de seu trabalho estar na fila de impressão.

5.15 INSTALAÇÃO DE EQUIPAMENTOS E SOFTWARES

A instalação de equipamentos, periféricos e softwares deve ser realizada somente pelo Departamento de TI ficando vedado a qualquer setor realizar estes procedimentos sem o acompanhamento e manutenção da TI.
Abaixo seguem diretrizes estabelecidas nesta Política.

- É vedada a instalação, manipulação, movimentação de computadores, equipamentos e periféricos pelo usuário. Estes processos devem ser realizados pelo Departamento de TI e solicitados via abertura de chamados;
- Não é permitido a modificação de computadores, notebooks e equipamentos, tais como adesivagem, ou customização;
- A manutenção de computadores e demais equipamentos de TI somente podem ser realizadas pelo Departamento de TI visando garantir a integridade do equipamento;

- É vedada toda e qualquer possibilidade de remanejamento por intermédio do usuário, sendo que quando se fizer necessário, deverá ser enviada uma solicitação através do ti.chamados@salton.com.br ao departamento de TI com antecedência, ficando a cargo deste último ou de hierarquia superior à autorização;
- Não é permitido baixar programas e softwares pelo usuário. Para tal, solicita-se que o usuário abra um chamado para ti.chamados@salton.com.br;
- Programas e softwares não homologados pela SALTON também não são permitidos, pois estes não foram avaliados e podem não conter o nível de segurança estipulado pela empresa;
    - Caso haja a necessidade de um software não homologado pela Salton, o departamento que necessita da aplicação deve entrar em contato com o departamento de TI para avaliação da aplicação, levando em consideração um ambiente seguro para empresa e conformidade com a LGPD;
- É dever do usuário zelar bom funcionamento dos equipamentos entregues para fins laborais, garantindo sua vida útil;
    - Mediante de qualquer avaria, deve-se comunicar imediatamente o TI, informando o ocorrido.
- Certificados digitais, somente podem ser instalados mediante aprovação da direção.

5.16 AVALIAÇÃO DE NOVOS SOFTWARES

Determina-se como procedimento padrão para avaliação de novos softwares o fluxo a seguir. Todo setor que necessite utilizar um novo software, deve atentar ao processo citado a seguir a fim de garantir a correta avaliação no que tange os três tópicos: LGPD, Cibersegurança e Privacy by Design.

5.17 DIRETRIZ DE ACESSO À INTERNET

Esse tópico visa definir as normas de utilização da Internet, englobando a navegação em sites, downloads e uploads de arquivos.

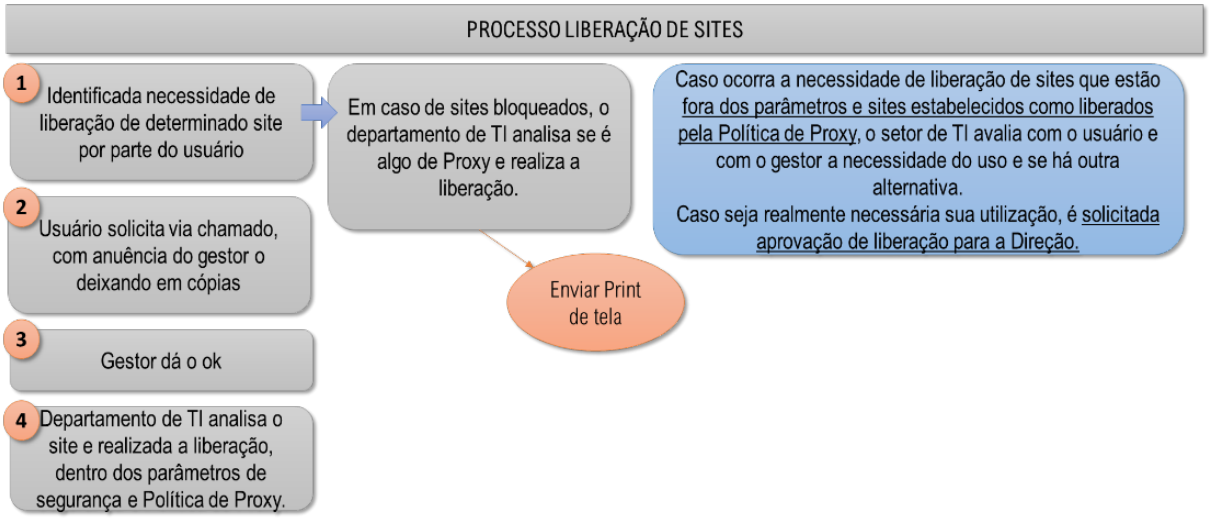
- É proibido o uso de atividades ilegais na Internet por meio da rede da SALTON por qualquer usuário (autorizado ou não);
- O acesso dos usuários a rede de internet se dá através dos Perfis de Proxy, descrito no tópico Política de Proxy – Perfis de acesso à Internet, deste capítulo;
- Somente as páginas/websites inerentes às atividades de trabalho e necessárias ao setor ou função do colaborador em questão serão liberadas para acesso;
    - Estas liberações são realizadas de acordo o perfil do Proxy e devem ser respeitadas as alçadas já aprovadas pela direção;
    - Caso o acesso para algum site eventualmente bloqueado se faça necessário para fins de trabalho relacionado à função desempenhada, o gestor deverá solicitar formalmente a liberação junto ao departamento de TI, via chamado pela ferramenta GLPI, que validará junto a direção a possível liberação;
    - Este acesso será analisado pelo departamento de TI que enquadrará ao Perfil de Proxy condizente;
- Não é permitida a utilização de qualquer software de transferência e compartilhamento não homologado pela empresa tais como, Google Drive, WeTransfer, Torrent, E-mule e/ou similares;
- É vetado baixar programas / softwares Free não homologados pelo departamento de TI da SALTON;
- Caso haja a necessidade de um software não homologado pela Salton, o departamento que necessita da aplicação deverá entrar em contato com o setor de TI para melhor avaliação da aplicação, entendimento das necessidades e para oferecer melhor solução levando em consideração um ambiente seguro para empresa e conformidade com a LGPD;

- O navegador de internet padrão a ser utilizado é o Google Chrome;
- É proibida a divulgação de informações confidenciais da SALTON em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
- É proibido o uso dos recursos de rede, internet, telefonia e sistemas da SALTON para fins pessoais;
- É proibido o acesso às redes e mídias sociais de qualquer natureza durante o expediente, salvo o uso profissional delineado pela direção;
- Caso a SALTON julgue necessário haverá bloqueios de acesso à arquivos e domínios que comprometam o uso de banda ou perturbem o andamento das atividades;
- Demais utilizações da Internet não listadas neste documento, que existam ou venham a ser criadas, devem ser solicitadas à gerência responsável. Se essa utilização for considerada pelo gerente como adequada e de interesse da organização, deve ser encaminhada à área de Tecnologia da Informação, para análise, aprovação e disponibilização.

5.18 DIRETRIZES PARA LIBERAÇÕES DE SITES

A SALTON estabelece quatro perfis de navegação de internet, onde o enquadramento de cada usuário/setor é determinado pela direção e setor de TI.
O acesso à internet se dá conforme o perfil de cada departamento. Cada site é analisado pelo Sophos que é integrado aos firewalls, e com base no seu conteúdo, é classificado. Essa classificação é utilizada para a construção dos perfis de navegação na internet. Foram definidos os seguintes perfis de navegação:

- Restrito;
- Intermediário;
- Avançado;
- Master.



Caso seja necessária alteração de perfis está se dará através de avaliação do departamento de TI que solicitará aprovação da Direção. Para liberação de sites, o processo a ser seguido é determinado conforme abaixo:
Em caso de dúvidas, de qual perfil é atribuído ao seu setor/ usuário, e as liberações dentro de cada perfil, entre em contato com o setor de TI.

5.19 UTILIZAÇÃO DA REDE WIFI

- A utilização da rede Wifi é uma concessão da SALTON aos usuários que necessitam deste recurso para desempenhar suas funções e poderá ser suspensa, caso sejam identificadas situações que possam comprometer a rede de dados da empresa, que constituam em desvio de finalidade de função do colaborador, ou ainda, que constituam em desvio moral ou ético com relação ao código de conduta da empresa;
- O acesso à rede corporativa e mobile se dá pelo login e senha do AD;
- É concedida a utilização de Wifi corporativo em equipamentos corporativos como notebooks e celulares;
- Para obter acesso a rede, é necessário que o usuário e seus aparelhos, notebooks e outros equipamentos sejam aprovados pelo gestor da área;
- O departamento de TI administrará os acessos à rede Wifi, tendo o direito de revogar a concessão de acesso, caso identificado uso indevido ou ameaça ao ambiente;
- Caso identifique o uso indevido dos recursos disponíveis, o gestor deverá comunicar a situação ao departamento de TI;
- A SALTON disponibiliza rede Wifi para visitantes para o exclusivo acesso à internet. Este ambiente é segregado do ambiente corporativo, e seus usuários têm acesso temporário;
- Qualquer necessidade que represente uma exceção às regras de acesso as redes mencionadas acima, deverão ser comunicadas formalmente pelo gestor, via chamado, que validará a solicitação junto a direção.

5.19.1 WIFI - uso em celulares particulares

A SALTON determina o processo abaixo para liberação do WiFi nos celulares particulares:

- Necessária aprovação da direção.
- O uso deste recurso deve ser realizado de forma moderada, respeitando a Política de Segurança e as normas de utilização de recursos da empresa;
- A direção realizará análise de liberação de Wifi e poderá solicitar inclusão ou exclusão de usuários, sem aviso prévio, ao qual o departamento de TI providenciará, informando o gestor de tal modificação;
- Toda e qualquer informação da SALTON não deve ser compartilhada, transmitida ou divulgada através de celulares particulares;
- O gestor se responsabiliza pela liberação e por monitorar o uso ordenado durante o horário de expediente;
- Salientamos que o Departamento de TI não tem acesso, monitora ou controle sobre dispositivos não empresariais;
- O uso do celular particular não deve estar vinculado às atividades laborais, para tal, equipamentos empresariais são disponibilizados: Computadores, notebooks, celulares corporativos e outros dispositivos (Teams);
- Em ambiente produtivo não é permitido o uso de celular particular no horário de expediente conforme regra da empresa, de acordo com a definição da Direção.

5.19.2 WiFi – visitantes

Todo o visitante que necessitar de acesso ao Wifi terá acesso a uma rede segregada, onde deve retirar um Voucher na recepção das unidades e tem duração de 1 dia para visitantes internos e 3 horas para visitantes das lojas.

Os gestores e colaboradores que recepcionam estes visitantes, técnicos e outros suportes, devem atentar à esta condição e providenciar a conexão necessária aos externos.

5.19.3 Rede WiFi ao meio-dia

É disponibilizada uma rede Wifi segregada para que os colaboradores possam utilizar em seus celulares particulares durante o período do meio-dia.
Este horário compreende das 11:00 às 14:00 horas, sendo que após este horário a rede é encerrada.

5.20 SOFTWARES DE COMUNICAÇÃO

Este tópico visa definir as normas e diretrizes para utilização das ferramentas homologadas pela empresa para comunicação instantânea e outros aplicativos de comunicação utilizados em atividades corporativas, tanto no ambiente interno quanto externo.
Fica definido como principal software de comunicação instantânea da empresa o Microsoft Teams. As ferramentas homologadas devem ser utilizadas exclusivamente para fins profissionais, observadas as diretrizes desta política e as orientações da área de Tecnologia da Informação:

- A instalação de ferramentas ou aplicativos de comunicação somente poderá ser realizada pela equipe técnica do Departamento de Tecnologia da Informação (TI), em computadores, notebooks, equipamentos e periféricos de propriedade da Salton, sendo vedada a instalação, configuração, sincronização ou utilização em equipamentos de uso particular ou pessoal;
- É expressamente proibido realizar login, instalar, configurar, sincronizar ou utilizar o Microsoft Teams, WhatsApp Web, e-mail corporativo ou qualquer outro comunicador corporativo em celulares, notebooks, tablets ou demais dispositivos pessoais, salvo autorização formal e prévia da empresa, mediante avaliação do gestor direto e da TI, com aplicação dos controles de segurança necessários;
- A utilização das ferramentas disponibilizadas pela empresa deverá ocorrer obrigatoriamente com contas, números, domínios ou credenciais corporativas autorizadas, sendo proibido o uso de número pessoal no WhatsApp Web, bem como de contas pessoais para tratar de assuntos corporativos. Todas as conversas, interações e registros realizados nessas ferramentas poderão ficar armazenados em repositórios que permitam auditorias internas e externas, sendo passíveis de avaliação pela empresa, incluindo TI, Jurídico, Compliance, RH e Direção, a qualquer momento e sem aviso prévio;
- A utilização de comunicadores corporativos vinculados ao domínio da Salton deve ser restrita à comunicação profissional e aos assuntos relacionados às atividades da empresa, observadas as regras de segurança da informação, confidencialidade e proteção de dados;
- Toda a utilização deverá estar relacionada com a atividade da empresa e estará sujeita às mesmas normas do Código de Conduta e da Política de Segurança da Tecnologia da Informação, cabendo as mesmas sansões e punições informadas em caso de infração;
- Todas as conversas realizadas por meio de comunicador no ambiente interno, com domínio @salton.com.br, são passíveis monitoramento e armazenadas em repositórios que permitam a auditoria interna e externa, estando sujeitas à avaliação a critério da empresa (setor de TI, jurídico, RH, Compliance e direção), quando necessário, a qualquer momento e sem necessidade de prévio aviso;
- A Salton reserva-se o direito de suspender, bloquear ou revogar o acesso e a utilização de qualquer conta, ferramenta ou recurso de comunicação sob seu domínio, a qualquer momento e a seu critério, sem necessidade de aviso prévio, especialmente em caso de risco à segurança da informação, descumprimento desta política ou necessidade de investigação, auditoria ou preservação de evidências.

5.21 USO DE APARELHOS PARTICULARES E CORPORATIVOS

No âmbito desta Política de Segurança da Informação, fica estabelecido que o uso de dispositivos pessoais para acesso, armazenamento, processamento ou compartilhamento de informações corporativas é, como regra geral, proibido.

A vedação se aplica a quaisquer equipamentos particulares, incluindo, mas não se limitando a celulares, notebooks, tablets e outros dispositivos eletrônicos. Também se inclui nessa orientação o download e o uso de aplicativos utilizados na atividade profissional, como Teams, e-mail corporativo e outros sistemas ou aplicativos que realizem comunicação, acesso ou transação de dados corporativos e profissionais.

Tal restrição visa preservar a confidencialidade, integridade e disponibilidade das informações da organização, reduzindo a exposição a riscos relacionados à perda de controle sobre dados corporativos e ambientes não gerenciados.

Em caráter excepcional, caso haja necessidade devidamente justificada de utilização de dispositivo pessoal para fins corporativos, essa utilização deverá ser previamente autorizada por gestão direta e direção e estará sujeita à aplicação de controles de segurança e monitoramento. Nessas situações, o colaborador declara ciência de que a empresa poderá acessar, a qualquer tempo, conteúdos e registros relacionados ao uso corporativo do dispositivo, incluindo dados, comunicações e backups, sempre que necessário para fins de auditoria, investigação ou atendimento a requisitos legais e regulatórios.

Já os dispositivos corporativos disponibilizados pela organização têm como finalidade exclusiva o desempenho de atividades profissionais e devem ser utilizados de forma responsável, ética e em conformidade com as diretrizes internas.

É expressamente proibida a utilização desses equipamentos para fins particulares, salvo em situações pontuais e controladas que não comprometam a segurança da informação, o desempenho dos ativos tecnológicos ou a imagem da organização. Ainda assim, permanece vedado o acesso a conteúdo ilícitos, impróprios ou potencialmente prejudiciais, bem como a realização de downloads de softwares, aplicativos ou quaisquer recursos não autorizados, especialmente aqueles que possam representar risco à segurança das informações.

A organização não assegura a privacidade dos dados pessoais eventualmente armazenados ou trafegados em dispositivos corporativos, uma vez que tais ativos constituem propriedade organizacional e estão sujeitos a monitoramento. Esse monitoramento poderá abranger acessos, comunicações, arquivos e utilização de recursos tecnológicos, sendo realizado com a finalidade de proteger os ativos de informação, assegurar o cumprimento das políticas internas e gerar evidências em caso de apuração de desvios de conduta ou incidentes de segurança.

5.22 DO USO DO WHATSAPP E O WHATSAPP WEB

No que se refere ao uso de aplicativos de mensageria, incluindo o WhatsApp Business e o WhatsApp Web, fica definido que sua utilização para fins corporativos deve ocorrer exclusivamente por meio de números e contas institucionais fornecidos pela organização. É expressamente vedado o uso de números pessoais para a condução de assuntos corporativos, bem como o vínculo entre contas corporativas e dispositivos pessoais sem autorização formal. Essa restrição tem como objetivo garantir rastreabilidade, governança da comunicação e proteção das informações trafegadas.

Adicionalmente, o uso do WhatsApp Web deve ser restrito a ambientes controlados e dispositivos previamente autorizados pela organização, sendo expressamente proibida a sua utilização em equipamentos públicos, compartilhados ou não seguros. O login deve ser realizado exclusivamente com contas corporativas, não sendo permitido o uso ou associação com contas pessoais. É obrigatório o encerramento da sessão ao término da utilização, como medida de proteção contra acessos indevidos.

O uso do WhatsApp corporativo em dispositivos pessoais não é recomendado e, quando excepcionalmente permitido, implica ciência e concordância do colaborador de que a organização poderá acessar as informações corporativas armazenadas ou trafegadas por meio desse recurso, inclusive para fins de investigação, auditoria ou verificação de conformidade, incluindo o acesso a backups, quando aplicável e necessário.

A organização poderá realizar auditorias periódicas e monitoramentos sobre o uso dos dispositivos, acessos à internet, sistemas corporativos e ferramentas de comunicação, com o objetivo de proteger seus ativos, assegurar a conformidade com esta política e com a legislação vigente, bem como identificar eventuais violações.
O uso dos recursos tecnológicos corporativos implica ciência e concordância do colaborador quanto à possibilidade de tais verificações, que poderão resultar na geração de evidências para fins disciplinares, legais ou regulatórios.
O descumprimento das diretrizes estabelecidas nesta política poderá acarretar a aplicação de medidas disciplinares, conforme previsto nas normas internas da organização e na legislação aplicável, sem prejuízo de outras sanções administrativas, civis ou penais cabíveis.

5.23 CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

A SALTON estabelece que todos os colaboradores devem receber treinamento sobre conscientização a respeito de segurança da informação segundo os aspectos a seguir:
- Na integração;
- No mínimo uma vez ao ano;
- Na semana de conscientização sobre cibersegurança;
- Sempre que for identificada a necessidade por parte do gestor;
- Sempre que for identificada um evento de ataque, phishing ou fraude ao qual o usuário não tenha sido capaz de identificar;
- É dever de todos identificar e solicitar gaps no dia a dia e solicitar reciclagem e treinamentos ao departamento de TI.

5.24 ABERTURA DE CHAMADOS

A SALTON estabelece que toda solicitação ao setor de TI deve ser realizada através do envio de e-mail com abertura de chamado para o e-mail: ti.chamados@salton.com.br
- Chamados envolvendo a solicitação de periféricos devem ser realizadas pelo gestor em nome do colaborador estando sujeito a avaliação do Departamento de TI e da aprovação da Direção;
- Chamados referentes a liberação de sites, são avaliados segundo sua categoria de liberação de Proxy e submetidos a aprovação da Direção, avaliando os riscos apresentados;
- Chamados referentes a concessão de acesso a pastas e aplicações devem ser solicitadas pelos gestores em nome do colaborador, sendo que estes acessos serão liberados mediante aprovação do gestor da pasta, passando por avaliação prévia do Departamento de TI.

5.24.1 Como realizar a abertura de um chamado

Enviar um e-mail para ti.chamados@salton.com.br, com o título e descrição da necessidade;
- Caso o chamado seja referente ao ERP Protheus, inserir no cabeçalho do e-mail as palavras “Sistema” ou “Protheus”;
- Automaticamente será gerado um chamado onde o título do e-mail é o título do chamado;
- No cabeçalho do e-mail (título do e-mail), insira o assunto;
- No corpo do e-mail insira a descrição do chamado
    - Detalhar o máximo de informações quanto for possível acerca da necessidade ou em que ponto do processo ocorre o erro;
- O detalhamento permite ao TI garantir o melhor diagnóstico;
- Informar se é uma demanda individual ou uma necessidade de todo um departamento;

- Informações com print de tela com o erro ajudam muito para encontrar a causa raiz do problema e acelerar a resolução.

ATENÇÃO: A equipe de TI está orientada a trabalhar apenas nas demandas que sejam formalmente recebidas via chamado.

5.25 CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação e gestão da informação, visa prover diretrizes para a segurança da informação, relacionadas ao manuseio, controle, proteção (contra indisponibilidade, divulgação imprópria, acesso indevido e modificação não autorizada de informações e de dados) e descarte, promovendo a melhoria contínua dos processos relacionados à segurança da informação, mantendo a confidencialidade, integridade e disponibilidade das informações.

PRIORIZAÇÃO DE CHAMADOS | SLA's		
URGÊNCIA	IMPACTO	PRIORIDADE
Alta: Caracterizamos como urgência alta, quando ocorrem incidentes com paradas de sistemas, que afetem o funcionamento do ambiente, ou os processos da empresa, sem solução paliativa. **Média**: Caracterizamos como urgência média, quando ocorrem incidentes com parada parcial de sistema, que afetem o funcionamento do ambiente, ou os processos da empresa, com solução paliativa. Solicitações e melhorias entram neste quesito **Baixa**: Chamados que não afetam o funcionamento das atividades e que possuem uma solução paliativa.	**Alto:** Parada total das atividades, causando danos gravíssimos que podem até se tornar irreversíveis. **Médio:** Parada parcial, com danos regulares e reversíveis. Solicitações cotidianas e melhorias entram neste quesito. **Baixo:** Incidentes que causam danos leves, os quais podem ser desconsiderados.	**Alta:** Incidente que se não foi trabalhado, acarretará em piora no quadro geral, deve ser tratado com prioridade. **Média:** Incidente relatado que deve ser trabalhado para que não se torne grave. **Baixa:** Requisições / solicitações que não afetam o ambiente e andamento das atividades cotidianas. Solicitações e melhorias entram neste quesito.
TIPOS	**Incidentes:** Acontecimentos inesperados que impossibilitam o andamento das atividades ou funcionamento de sistemas. **Requisições:** Solicitações e melhorias	

Atestar a correta classificação das informações em termos valor, requisitos legais, sensibilidade e criticidade, a fim de evitar qualquer modificação ou divulgação não autorizada, causando perdas e prejuízos à instituição, colaboradores, fornecedores, parceiros de negócio e clientes.

Todas as classificações de documentos aferidas deverão considerar o seu conteúdo com relação à disponibilização de dados pessoais de pessoas naturais identificadas ou identificáveis, de acordo com a Lei Geral de Proteção de Dados (LGPD) número 13.709/2018, para que dessa forma tenham a sua proteção e uso dentro da finalidade garantidas.

Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação quando a informação é gerada ou coletada, para que possa garantir a devida confidencialidade, especialmente no caso de conteúdo, dados pessoais, dados pessoais sensíveis e dados de cartões de crédito (quando aplicáveis) e imagens.

Os documentos internos são classificados quanto à sua confidencialidade em:

- CONFIDENCIAL: documentos que apresentam informações pessoais ou sensíveis aos olhos da alta direção, com um alto nível de confidencialidade, sendo seu acesso restrito à alta direção da corporação;
- USO INTERNO: documentos que apresentam informações necessárias à execução dos processos da corporação, com médio ou baixo nível de confidencialidade, sendo seu acesso restrito aos empregados da corporação;
- PÚBLICO: documentos que apresentam qualquer tipo de informações da corporação, desde que sem restrições quanto à confidencialidade, sendo seu acesso irrestrito a todas as partes interessadas relacionadas com a corporação.

5.26 TERMO DE COMPROMISSO

O Termo de Compromisso (ANEXO I – TERMO DE ADESÃO ÀS POLÍTICAS DA SALTON DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE) é utilizado para que colaboradores e estagiários se comprometam formalmente em seguir a Política de Segurança da Tecnologia de Informação SALTON, tomando ciência das punições impostas ao seu não cumprimento.
No termo de compromisso são reforçados os principais pontos da Política de Segurança da Tecnologia de Informação SALTON e, deve ser assinado por todos os colaboradores da instituição. Sua renovação deve ser feita sempre que necessário.

5.26.1 Verificação da utilização da política

Para garantir que as regras mencionadas acima estão sendo cumpridas, a SALTON se reserva no direito de:
- Implantar softwares e sistemas que monitorem e gravem todos os usos de Internet através da rede e das estações de trabalho da SALTON;
- Inspecionar qualquer arquivo armazenado na rede, estejam eles no disco local da estação ou nas áreas privadas da rede;
- Revogar, suspender, excluir qualquer informação ou conta dentro de seus ambientes sob seu critério, a qualquer tempo e sem necessidade de aviso prévio.

5.26.2 Violação da política, advertência e punições

Ao detectar uma violação da política, o setor de TI procurará determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.
Nos termos da Política de Segurança da Tecnologia de Informação SALTON, a empresa procederá ao bloqueio de acessos, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou de pôr em risco a imagem da instituição.
Haverá o treinamento dos usuários em segurança da informação, com o intuito de divulgar e conscientizar os colaboradores sobre a Política de Segurança da Tecnologia de Informação SALTON, a ser seguida por todos. O programa de treinamento em segurança fará parte do programa de integração de novos colaboradores. Os treinamentos de reciclagem devem ser previstos quando necessários.
Em caso de violação da presente Política aplicar-se-ão as penalidades abaixo a todos os funcionários, acionistas, estagiários, aprendizes e terceiros da SALTON, sendo que todos possuem o compromisso de informar qualquer irregularidade ou descumprimento da presente norma:
- Treinamento adicional (Medida Educativa);
- Advertência verbal;
- Advertência Formal (notificação);
- Suspensão;
- Demissão sem justa causa;
- Demissão por justa causa;
- Outras medidas jurídicas.

Em caso de terceiros, as penalidades deverão estar previstas nos contratos firmados com tais fornecedores.
Os critérios para análise a aplicação das medidas disciplinares estarão previstos no REGIMENTO INTERNO DO COMITÊ DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO.

5.27 CANAL DE DENÚNCIAS

Para denúncias em caso de descumprimento desta "Política", você poderá utilizar o canal de contato: https://www.contatoseguro.com.br/familiasalton.
O procedimento para recebimento das denúncias e investigação está detalhado no REGIMENTO INTERNO DO "CPSI".

5.28 REVISÃO DA POLÍTICA

Esta política entra em vigor a partir da data de sua aprovação, possuindo validade por tempo indeterminado e ainda sendo sujeita a revisões anuais ou conforme mudanças significativas nos processos que tenham relação com a política.

6 ANEXOS

6.1 ANEXO I – TERMO DE ADESÃO ÀS POLÍTICAS DA SALTON DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

TERMO DE ADESÃO ÀS POLÍTICAS DA SALTON DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Pelo presente instrumento e na melhor forma de direito, de um lado VINÍCOLA SALTON S/A, empresa de direito privado, registrada no CNPJ sob número 87.547.428/0001-37, situada a Rua Mario Salton, 300, Tuiuty, na cidade de Bento Gonçalves/RS, denominada a partir de agora SALTON e, de outro, _____, brasileiro (a), _____, residente e domiciliado em _____, registrado no CPF sob número _____, denominado a partir deste, COLABORADOR.

DECLARAÇÕES INICIAIS

Declaro que recebi, li, compreendi e me comprometo a cumprir com os seguintes documentos:

- POLÍTICA DE SEGURANÇA DA INFORMAÇÃO;
- POLÍTICA DE GOVERNANÇA E PRIVACIDADE DE DADOS;
- POLÍTICA DE USO DE INTELIGÊNCIA ARTIFICIAL;
- COMPROMISSO DE CONFIDENCIALIDADE CONTIDO NESTE TERMO;

O Termo de Adesão não se limita à Política de Segurança da Informação, Política de Governança e Privacidade de dados ou eventuais procedimentos relativos à privacidade e segurança da informação, mas refere-se ao sigilo de todas as informações da importantes à proteção do negócio da SALTON. Desta forma, não se limita aos processos de TI, mas engloba todos os processos da empresa.
As Políticas acima identificadas, ficarão disponíveis nos canais de comunicação internos da SALTON, podendo ser modificadas a qualquer momento visando o cumprimento às normas aplicáveis, sendo que neste caso o COLABORADOR receberá uma comunicação das alterações realizadas.
Após receber TREINAMENTO ESPECÍFICO, ler e entender seu conteúdo das POLÍTICAS, concordo e assumo o compromisso com as referidas regras, em especial, com os termos abaixo:

DO OBJETO

O objeto do presente termo de compromisso visa assegurar o cumprimento das POLÍTICAS INTERNAS da SALTON no que tange às temáticas de Privacidade e Segurança da Informação, bem como a proteção das INFORMAÇÕES CONFIDENCIAIS E/OU SIGILOSAS disponibilizadas pela SALTON, em razão da relação de emprego desenvolvida pelas partes.

Com a finalidade de proporcionar o bom e fiel desempenho das atividades faz-se necessária a disponibilização de informações técnicas e confidenciais, conforme explicado no item "DAS DEFINIÇÕES", neste documento.
Todas as informações produzidas ou acessadas em razão da relação empregatícia são de propriedade da SALTON, sendo proibida a divulgação e utilização não autorizada das referidas informações.

DAS DEFINIÇÕES
Todas as informações obtidas através da relação de emprego com a SALTON, incluindo, mas não se limitando a relacionadas ao negócio, informações estratégicas, comerciais, dados pessoais, dados de projeto, informações técnicas de produtos, especificação, funcionamento, sistemas, organização ou desempenho da referida empresa serão tidas como CONFIDENCIAIS E SIGILOSAS.
Parágrafo único: Serão consideradas para efeito deste termo toda e qualquer informação, patenteada ou não, de natureza técnica, operacional, comercial, jurídica, Know-how, invenções, processos, fórmulas e designs, patenteáveis ou não, sistemas de produção, logística e layouts, planos de negócios (*business plans*), métodos de contabilidade, técnicas e experiências acumuladas, senhas, documentos, contratos, papéis, estudos, dados pessoais, pareceres e pesquisas a que o colaborador tenha acesso:
a) por qualquer meio físico, sejam eles documentos expressos, manuscritos, fac-símile, mensagens eletrônicas (e-mail), fotografias etc.;
b) por qualquer forma registrada em mídia eletrônica (sistemas, fitas, CD's, DVD´s, disquetes, pen drives, clouds, discos rígidos ou quaisquer outros similares);
c) oralmente.

DA RESPONSABILIDADE
O colaborador compromete-se a manter sigilo não utilizando tais informações confidenciais em proveito próprio ou de terceiros.

As informações confidenciais confiadas aos colaboradores somente poderão ser abertas a terceiros mediante consentimento prévio e por escrito da SALTON, ou em caso de determinação judicial, hipótese em que o colaborador deverá informar de imediato, por escrito, à empresa a fim de que esta tome as medidas cabíveis.

DAS INFORMAÇÕES NÃO CONFIDENCIAIS
Não configuram informações confidenciais aquelas:
a) já disponíveis ao público em geral sem culpa do colaborador;
b) que já eram do conhecimento do colaborador antes de sua do ingresso na SALTON e que não foram adquiridas direta ou indiretamente da SALTON;
c) que não são mais tratadas como confidenciais pela SALTON.

DA GUARDA DAS INFORMAÇÕES
Todas as informações de confidencialidade e sigilo previstas neste termo terão validade durante toda a vigência deste instrumento, enquanto perdurar a relação de trabalho e, ainda, por um período indeterminado, do rompimento do vínculo do colaborador com a SALTON.

DAS OBRIGAÇÕES
Deverá o colaborador:
I) usar tais informações apenas com o propósito de bem e fiel cumprir os fins da SALTON;
II) manter o sigilo relativo às informações confidenciais e revelá-las apenas aos colaboradores que tiverem necessidade de ter conhecimento sobre elas;
III) proteger as informações confidenciais que lhe foram divulgadas, usando o mesmo grau de cuidado utilizado para proteger suas próprias informações confidenciais;

IV) manter procedimentos administrativos adequados à prevenção de extravio, perda ou acesso indevido de quaisquer documentos ou informações confidenciais, devendo comunicar à SALTON, imediatamente, a ocorrência de incidentes desta natureza pelo canal: https://www.contatoseguro.com.br/familiasalton.
V) utilizar adequadamente os equipamentos da empresa, conforme regras e boas práticas indicadas na Política de Segurança da SALTON, evitando acessos indevidos aos ambientes computacionais aos quais estarei habilitado, que possam comprometer a segurança das informações, incluindo, mas não se limitando a proibição de compartilhamento de senhas entre outras regras estabelecidas na Política.
VI) As senhas disponibilizadas ao colaborador não podem ser utilizadas para fins que não sejam aqueles definidos pelo Gestor ou Diretor de área.

PARÁGRAFO PRIMEIRO: O colaborador fica desde já proibido de produzir cópias ou backup, por qualquer meio ou forma, de qualquer dos documentos a ele fornecidos ou documentos que tenham chegado ao seu conhecimento em virtude da relação de emprego.

PARÁGRAFO SEGUNDO: O colaborador deverá devolver, íntegros e integralmente, todos os documentos a ele fornecidos, inclusive as cópias porventura necessárias, na data estipulada pela SALTON para entrega, ou quando não for mais necessária a manutenção das informações confidenciais, comprometendo-se a não reter quaisquer reproduções, cópias ou segundas vias, sob pena de incorrer nas responsabilidades previstas neste instrumento.

PARÁGRAFO TERCEIRO: O colaborador deverá destruir todo e qualquer documento por ele produzido que contenha informações confidenciais da SALTON, quando não mais for necessária a manutenção dessas informações confidenciais, comprometendo-se a não reter quaisquer reproduções, sob pena de incorrer nas responsabilidades previstas neste instrumento.

DAS DISPOSIÇÕES ESPECIAIS

Ao assinar o presente instrumento, o colaborador manifesta sua concordância no seguinte sentido:
I) todas as condições, termos e obrigações ora constituídas serão regidas pelo presente Termo, bem como pela legislação e regulamentação brasileiras pertinentes;
II) o presente termo só poderá ser alterado mediante a celebração de um novo termo, posterior e aditivo;
III) as alterações do número, natureza e quantidade das informações confidenciais disponibilizadas pela SALTON não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Confidencialidade e Sigilo, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste instrumento;
IV) o acréscimo, complementação, substituição ou esclarecimento de qualquer das informações confidenciais disponibilizadas para o colaborador, em razão do presente objetivo, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, não sendo necessário, nessas hipóteses, a assinatura ou formalização de Termo aditivo.

DA VALIDADE

Este termo tornar-se-á válido a partir da data de sua efetiva assinatura pelas partes, sem data de expiração após o desligamento do colaborador da SALTON.
Parágrafo Único: As disposições deste instrumento devem, contudo, ser aplicadas retroativamente a qualquer informação confidencial que possa já ter sido divulgada, antes da data de sua assinatura.

DAS PENALIDADES

A não-observância de quaisquer das disposições de confidencialidade estabelecidas neste instrumento, sujeitará ao colaborador infrator, como também ao agente causador ou facilitador, por ação ou omissão de qualquer daqueles

relacionados neste Termo, ao pagamento, ou recomposição, de todas as perdas e danos comprovadas pela SALTON, bem como as de responsabilidade civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, também ensejando a possibilidade de aplicação das medidas disciplinares permitidas pela CLT.S

CANAL DE DENÚNCIA

Assumo o compromisso de reportar à SALTON por meio do CANAL: https://www.contatoseguro.com.br/familiasalton, qualquer comportamento ou situação que esteja em desacordo com as regras estabelecidas nas POLÍTICAS acima identificadas.

DO FORO

O foro competente para dirimir quaisquer dúvidas ou controvérsias resultantes da execução deste Instrumento é o da cidade de Bento Gonçalves/RS, caso não sejam solucionadas administrativamente.
Por esta ser a expressão da minha vontade, assino o presente Termo.

Cidade, data.

_____
Colaborador

7 HISTÓRICO DE REVISÕES

REVISÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO	TREINAMENTO
00	27/05/2025	Emissão inicial do documento em substituição a PLI-TI 001-R04	Sim
01	22/06/2026	Revisão geral da Política e inclusão dos capítulos 5.22 e 5.23	Sim