POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

1. OBJETIVO

A Política de Segurança da Informação e Comunicação é uma declaração formal da Leaf acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores.

2. ABRANGÊNCIA

Todos os colaboradores, gerentes, diretores, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e utilizam ativos informacionais corporativos da Leaf, suas unidades, subsidiárias e/ou coligadas.

3. MISSÃO

Garantir a confidencialidade, integridade, disponibilidade, autenticidade e a legalidade da informação necessária para a realização dos negócios, promovendo a melhoria contínua do Sistema de Segurança da Informação da Leaf.

4. DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- Lei 9.609/98 – Lei do Software
- Lei 12.965/2014 – MCI / Marco Civil da Internet
- Lei 13.709/2018 – LGPD / Lei Geral de Proteção de Dados Pessoais

5. TERMOS E DEFINIÇÕES

- ***TI*:** Tecnologia da Informação
- ***Software*:** É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares.

- ***Backup*:** É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- ***Mídias Removíveis*:** Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória entre outros.
- ***USB (Universal Serial Bus)*:** É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
- ***VPN (Virtual Private Network)*:** Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por colaboradores em trânsito.
- ***Softwares de Mensagens*:** São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou vídeo, em tempo real.
- ***Firewall*:** É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança à rede e ou a um determinado ponto da rede.
- ***Modem Wireless*:** É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets, notebooks, desktops, etc. objetivando conexão com a uma rede e acesso à internet.

6. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DA SEGURANÇA

A Segurança da Informação e Comunicação deve ser responsabilidade de todo, baseada em hábitos, posturas, responsabilidades e cuidados constantes no momento do uso dos ativos de informação, portanto, cabe a todos os colaboradores, estagiários e prestadores de serviços, cumprir fielmente a Política de Segurança da Informação e Comunicação da Leaf. Devendo sempre, buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação e comunicação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Leaf, cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual, e comunicar imediatamente a empresa quando do

descumprimento ou violação desta política, diretamente ao escritório do SGI ou através do canal de ética.

6.1. COMUNICAÇÃO EXTERNA

Somente os colaboradores que estão devidamente autorizados a falar em nome da empresa, podem escrever em nome da empresa em sites de Bate-papo (*Chat Room*), Grupos de Discussão (fóruns, *newsgroups*), e-mails, telefone ou qualquer outro meio de comunicação. Em caso de dúvidas, procurar o gestor da área ou o RH.

6.2. DIRETORIAS, GERÊNCIAS, SUPERVISÕES E COORDENAÇÕES

Cabe às Diretorias, Gerências, Supervisões e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento dessa Política de Segurança da Informação e Comunicação; e comunicar imediatamente eventuais casos de violação de segurança da informação e comunicação através do canal de ética.

6.3. GOVERNANÇA DE TI E GOVERNANÇA CORPORATIVA

Cabe as gerências propor ajustes, melhorias, aprimoramentos e modificações desta Política junto ao escritório do SGI (anexo a Gerência de TI). Ao escritório do SGI cabe: convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito dessa Política; prover todas as informações de gestão de segurança da informação e comunicação solicitadas por Gestores.

6.4. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

6.4.1. PÚBLICA

É uma informação da Leaf ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

6.4.2.RESERVADA

É uma informação trocada entre a Leaf e seus clientes, terceiros, prestadores e fornecedores, e que ela não tem interesse em divulgar. O acesso por parte de outros indivíduos além daqueles para os quais a mensagem é destinada poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação Interna, Confidencial ou Altamente Confidencial. Só deve ser acessada por aqueles colaboradores, clientes, terceiros, prestadores ou fornecedores da Leaf para quem foi destinada.

6.4.3.INTERNA

É uma informação da Leaf que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da Leaf.

6.4.4.CONFIDENCIAL

É toda informação que pode ser acessada somente por colaboradores da Leaf explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio, violar a privacidade de seus colaboradores ou de terceirizados e/ou comprometer a estratégia de negócio da organização.

6.4.5.ALTAMENTE CONFIDENCIAL

É uma informação crítica para os negócios da Leaf ou de seus clientes. A divulgação não autorizada dessa informação pode causar sérios impactos de ordem financeira, de imagem, de reputação, operacional ou, ainda, sanções administrativas, civis e criminais à Leaf ou aos seus clientes, comprometendo assim, sua credibilidade no mercado. É sempre restrita a um grupo específico de pessoas.

7. OBJETIVOS DA POLÍTICA DE SI

A Leaf estabeleceu objetivos do SGI como prática tangível e mensurável para monitorar e avaliar a eficácia do sistema de gestão Integrado (SGI), através dos OKRs (Objetivos-Chave) e desdobramento por meio dos KRs (Resultados-chave). Os objetivos do SGI são consistentes com a política do SGI e com a política da segurança da informação, compatíveis com o direcionamento estratégico da empresa e levam em consideração as normas, os requisitos legais aplicáveis a suas atividades-fim, a conformidade de produtos e serviços oferecidos aos clientes e a promoção do aumento da satisfação dos mesmos.

A Leaf assegura que os indicadores dos objetivos e suas metas deverão ser desdobrados pelos níveis pertinentes da organização de forma a propiciar o envolvimento e o comprometimento de todos com a qualidade e a segurança da informação.

POLÍTICA SGI	ESTRATÉGIA	OKR Objetivos-Chave	KRs Resultados-chave
PLT-001 Política da Segurança da Informação e Comunicação	PROCESSOS INTERNOS	Garantir a Infraestrutura, Segurança da Informação e Privacidade de Dados	Métricas, iniciativas e resultados monitorados na plataforma de gestão de OKRs da Leaf

Os objetivos e metas do SGI são continuamente monitorados e analisados criticamente pelos gestores e pela direção nas reuniões de Analise Critica e nas reuniões estratégicas.

Os gestores são responsáveis pelo monitoramento continuo dos seus indicadores e por promover ações para assegurar o atingimento das metas.

Os objetivos e metas do SGI estão suportados pelos sistemas Leaf: Produção, Desenvolvimento e Comercial através de Portal Sigel e relatórios internos.

8. PROPRIEDADE INTELECTUAL

É de propriedade da Leaf, todos os “designs”, criações, códigos e procedimentos, desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício com a Leaf.

9. DISPOSITIVOS MÓVEIS

Todos os dispositivos móveis adquiridos pela Leaf devem ser cadastrados para serem incluídos como parte integrante da rede corporativa e, devem ainda, ficar vinculados a um setor, onde ficarão sob a responsabilidade total do respectivo colaborador que assinou a concessão.

A concessão de uso deve ser feita através do formulário **FRM-027 TERMO DE RESPONSABILIDADE - PLANO CORPORATIVO**, e devem estar em conformidade com as necessidades funcionais do colaborador.

Os colaboradores da Leaf responsáveis por dispositivos móveis, devem fazer sua parte para proteger a rede da empresa e os dados confidenciais que estão armazenados, quando acessados através dos dispositivos móveis.

Com o objetivo e o compromisso de zelar pelo patrimônio da Empresa, deve-se sempre tomar as seguintes medidas:

- ✓ Observar os cuidados necessários no manuseio do dispositivo;
- ✓ Não expor dados da Empresa ou de Clientes enquanto utiliza dispositivos móveis;
- ✓ Utilizar o dispositivo somente para fins de desenvolvimento de atividades corporativas;
- ✓ Fazer o melhor para proteger o dispositivo contra perda ou roubo;
- ✓ Verificar com a TI da Leaf, regularmente, quanto a necessidade de atualizações;
- ✓ Usar apenas aplicativos homologados pela TI da Leaf;
- ✓ Informar imediatamente sobre um dispositivo perdido, roubado ou furtado, e comunicar o fato imediatamente a Gerência de Infraestrutura de TI, solicitando o bloqueio do serviço para os casos necessários, além de lavrar um boletim de ocorrência junto à autoridade policial, entregando-o, também, a Gerência de Infraestrutura de TI.

10. PONTO DE ATENÇÃO: ENGENHARIA SOCIAL

Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas. Ela manifesta-se de diversas formas, e podemos dividi-la em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do colaborador com relação à Segurança da Informação e Comunicação, na exploração da confiança das pessoas para a obtenção de informações

sigilosas e importantes e na não compreensão de como uma simples informação poderia trazer prejuízos à empresa. Essa ameaça deve ser evitada a todo custo, pois trabalhamos com informações sensíveis e sigilosas, por isso temos o **Termo de Confidencialidade** para colaboradores e terceiros.

10.1. ENGENHARIA DIRETA

É aquela caracterizada pelo contato direto entre o engenheiro social e a vítima através de telefonemas, aplicativos de mensagens, mídias sociais, e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

10.2. ENGENHARIA INDIRETA

Caracterizam-se pela utilização de softwares ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e e-mails falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a ofertas tentadoras e apagar o e-mail imediatamente.

11. BOAS PRÁTICAS, DENTRO E FORA DA EMPRESA

11.1. COMUNICAÇÃO VERBAL

- ✓ Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.
- ✓ Evite nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.
- ✓ Caso seja extremamente necessária a comunicação de assuntos sigilosos em ambientes públicos, ficar atento as pessoas à sua volta que poderão usar as informações com o intuito de prejudicar a imagem da empresa.

11.2. SEGURANÇA PARA NOTEBOOKS

- ✓ Quando em deslocamentos de carro, coloque o mesmo no porta-malas ou em local não visível.

- ✓ Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.
- ✓ Não coloque o notebook em carrinhos de aeroportos ou despache junto à bagagem.
- ✓ Em locais públicos (recepção de hotéis, restaurantes e aeroportos dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.
- ✓ Evite utilizar o notebook em locais públicos e, se for realmente necessário, ao fazê-lo, empregue grande discrição e esteja sempre atento a observadores indevidos.
- ✓ Nos hotéis, preferencialmente, guarde o notebook no cofre do seu apartamento.

12. DIRETRIZES DE SEGURANÇA

Conforme definição da norma NBR ISO/IEC 17799:2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação e Comunicação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação e comunicação é aqui caracterizada pela preservação da:

a) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

c) Disponibilidade, que é a garantia de que o acesso a informação estará disponível sempre que for necessário;

d) Autenticidade, que é a garantia de que a informação será registrada ou modificada apenas por pessoas que estejam autorizadas para tal.

e) Legalidade, que é a garantia de que todos os procedimentos relacionados à informação dentro da empresa, sejam feitos de acordo com as leis vigentes.

12.1. USO ACEITÁVEL DE ATIVOS

Para garantir o uso adequado da informação e de todos os outros ativos informacionais devemos seguir todas as instruções e diretrizes dispostas nessa política e em todas as outras que compõem o SGI, dessa forma, podemos manter uma gestão adequada e prover proteção contra roubo, fraude, espionagem, destruição não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os colaboradores adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas nesse sentido.

Campanhas contínuas de conscientização de Segurança da Informação e Comunicação serão utilizadas para incentivar a manutenção dos objetivos e o engajamento.

A Política de Segurança da Informação e Comunicação da Leaf é revisada e aprovada semestralmente pela Diretoria.

12.2. AMBIENTE FÍSICO

O ambiente físico deve ser protegido, a segurança é indispensável para garantir o bom desempenho dos colaboradores enquanto exercem suas atividades nas dependências da Empresa, além da salvaguarda das informações inerentes a essas atividades.

12.2.1. ACESSO FÍSICO

Clientes, Visitantes, Terceiros, Prestadores de Serviço e Fornecedores, precisam preencher formulário especifico – **FRM-055 SOLICITAÇÃO DE ACESSO PARA NÃO COLABORADORES** – para obter autorização e receber o crachá apropriado.

Os colaboradores Leaf devem ser cadastrados no sistema de controle, por biometria e crachá, no ato da admissão, onde as políticas de acesso estão devidamente aplicadas.

12.2.2. NÍVEIS DE ACESSO

As áreas, a rede e os equipamentos na Leaf, são controlados quanto ao acesso e utilização. Estando as permissões de acesso e utilização, diretamente ligadas as necessidades funcionais e ao nível hierárquico dos colaboradores. Os níveis de permissão devem ser observados, respeitados e não deve haver, em hipótese nenhuma, tentativas de acesso não autorizado.

12.2.3. DATA CENTERS

As máquinas (servidores) que armazenam dados e sistemas da Leaf estão em área protegida, Data Centers Próprios, localizadas na cidade de Vitória – ES e Serra – ES. A entrada é devidamente controlada, monitorada e restritas. Pessoas sem o nível de acesso necessário (clientes, visitantes, terceiros, prestadores de serviço, fornecedores e até mesmo colaboradores sem acesso liberado) que necessitarem ter acesso físico aos locais, sempre o farão acompanhados de pessoas autorizadas.

12.2.4. EQUIPAMENTOS

Notebooks, equipamentos de gravação, fotografia, vídeo, som ou qualquer outro tipo de equipamento similar a estes, que não sejam patrimônio da Leaf, devem obter autorização especifica – **FRM-025 SOLICITAÇÃO DE UTILIZAÇÃO E CIRCULAÇÃO DE EQUIPAMENTOS** – para serem utilizados nas dependências da Empresa, além de ter constante supervisão. A autorização deve ser concedida pelo gestor da área e ou gestor de segurança.

É responsabilidade da área envolvida com qualquer possível atividade de terceiros encaminhar os equipamentos para a devida avaliação e autorização, assim como a de qualquer colaborador em relação ao uso de equipamentos particulares nas dependências da Leaf.

Deve-se ainda, utilizar o formulário – **FRM-025 SOLICITAÇÃO DE UTILIZAÇÃO E CIRCULAÇÃO DE EQUIPAMENTOS** – para qualquer tipo de movimentação de equipamentos, seja uma movimentação interna ou externa.

12.2.5. MESA E TELA LIMPAS

Afim de evitar exposição desnecessária de informações sensíveis e evitar o comprometimento da segurança da informação e comunicação, devemos observar os seguintes princípios:

- ✓ Informações sensíveis ou críticas para o negócio da Empresa não devem estar disponíveis em papeis ou mídias removíveis e de fácil acesso, onde possam facilmente ser copiadas.

- ✓ Os documentos em papeis e as mídias removíveis não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas, quando não estiverem em uso, especialmente fora do horário do expediente.
- ✓ Fazer logoff antes de se afastar de um computador que esteja sendo usado por você, de forma que fique bloqueado, até que volte a usá-lo reinformando usuário e senha.
- ✓ Manter os pertences pessoais em gavetas ou armários trancados.
- ✓ Nunca deixar crachá de identificação ou chaves em qualquer lugar, mantenha-os junto a você.
- ✓ Notificar o RH imediatamente, no caso de perda do crachá ou chave.
- ✓ Nunca escrever senhas em lembretes que possam acabar sendo expostos.

12.3. AMBIENTE LÓGICO

Todo acesso ao ambiente lógico e às informações ai contidas, deve ser controlado. A autorização de acesso ao ambiente lógico se dá através do preenchimento de documento específico – **FRM-050 SOLICITAÇÃO PARA CONCESSÃO, ATUALIZAÇÃO OU REVOGAÇÃO DE ACESSO LÓGICO**, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente. O responsável pela autorização ou confirmação da autorização deve ser explicito e registrado. Os dados, as informações e os sistemas de informação da Leaf, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a segurança desses bens.

12.3.1. ACESSO LÓGICO

No ambiente Leaf, existem dois níveis de proteção para utilização dos recursos na rede corporativa, sendo: um usuário e senha para acesso ao sistema operacional nas estações de trabalho, que estão em uma rede com domínio, e outro usuário e senha para acessar os sistemas Leaf, onde são rodados os serviços para os clientes. Dessa forma, todo usuário deve ter identificações únicas, pessoais e intransferíveis, para acesso ao ambiente lógico e seus recursos, qualificando-o como responsável por qualquer atividade desenvolvida sob estas identificações. O titular deve, também, assumir a responsabilidade quanto ao sigilo das suas senhas pessoais.

As senhas devem obedecer a um padrão com pelo menos oito caracteres, contendo pelo menos um caractere numérico (0 a 9), pelo menos uma letra maiúscula (A a Z), pelo menos uma letra minúscula (a a z) e pelo menos um caractere especial (símbolos), não deve ser utilizado informações pessoais fáceis de serem obtidas como: nome, número de telefone ou data de nascimento como senha. Em hipótese alguma, anotar senhas em papeis como forma de lembrete ou armazenamento.

Não incluir senhas em processos automáticos de acesso aos sistemas, por exemplo, armazenadas em macros ou teclas de função.

A distribuição de senhas aos usuários (inicial ou não) deve ser feita de forma segura. Quando gerada pelo sistema, a senha inicial deve ser trocada pelo usuário no primeiro acesso.

A troca de uma senha bloqueada só deve ser providenciada por solicitação do próprio usuário, e verificando-se a continuidade na legitimidade de acesso do mesmo, junto ao seu gerente ou substituto.

As senhas possuem prazo de validade, o sistema irá, automaticamente, solicitar que o usuário renove sua senha, oferecendo uma interface para que esse processo de renovação aconteça.

A Leaf dispõe também de um servidor de VPN, para que os colaboradores possam, eventualmente, exercer suas atividades à distância. Para utilização desse serviço, existe um usuário e senha próprio, seguindo os mesmos padrões das senhas anteriores. O acesso garantido pela VPN, não isenta o usuário de utilizar as outras senhas de rede e sistemas, na verdade, tem a função de ser mais uma camada de segurança.

12.3.2. SISTEMAS

Os sistemas devem possuir controle de acesso por usuário e senha, pessoal e intrasferível, de modo a assegurar o uso apenas por usuários autorizados. O responsável pela autorização deve ser explicito, e deve existir um registro da aprovação concedida.

12.3.3. ESTAÇÕES DE TRABALHO

As estações de trabalho, incluindo equipamentos portáteis, e as informações aí contidas, devem ser protegidas contra danos ou perdas, bem como o acesso, uso ou exposição indevidos. Cada estação possui seu código de identificação único na rede, permitindo o acompanhamento e a rastreabilidade das atividades executadas.

O acesso as estações de trabalho se dão a partir de usuário e senha pessoais e intrasferíveis, ao termino das atividades o usuário deve encerrar o acesso desligando o equipamento, quando se ausentar temporariamente deve bloquear a utilização com senha.

Processamento de informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à Leaf, deve ser feito em equipamentos que estejam devidamente cadastrados no domínio Leaf, para garantir que as restrições de segurança tenham sido aplicadas.

Somente softwares licenciados pela área de TI devem ser executados em qualquer equipamento da Empresa.

12.3.4. IMPRESSÕES

É vedado o direito de impressão de material que contenha informações relativas aos serviços Leaf, exceto para Diretores, Gerentes e ou colaboradores diretamente autorizados por eles.

Quando autorizada, a impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado, qualquer documento enviado para impressão deverá ser retirado imediatamente pelo responsável.

As impressoras deverão ser utilizadas somente no âmbito profissional e para atividades inerentes a Leaf.

12.3.5. INSTALAÇÃO DE SOFTWARES

A Leaf respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da empresa. É terminantemente proibido o uso de softwares ilegais (sem licenciamento) na Empresa, sendo assim, a Gerência de TI

poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

Qualquer software que, para atender a necessidade de um serviço ou sistema Leaf, necessite ser instalado ou desinstalado, deverá ser comunicado a área de Infraestrutura de TI, para que, nos casos de instalações, o mesmo possa ser homologado e instalado pela TI, nos casos de desinstalação, para que possa ser confirmada a necessidade e realizada a tarefa.

12.3.6. REDE CORPORATIVA

O acesso à rede corporativa Leaf, é feito através de usuário e senha pessoal e intrasferível, inclusive no caso de acesso remoto. Os colaboradores estão separados em grupos de usuários com diferentes níveis de acesso, portanto, ao fazer login, é atribuído ao colaborador as permissões relativas ao grupo de rede a que pertence. Utilizamos rede baseada em Windows, com um servidor de domínio (AD), as configurações de usuário e as regras de segurança são parametrizadas no AD.

Não é permitido gravar, armazenar, expor, distribuir ou editar material com conteúdo sexual, preconceituoso ou ofensivo, através do uso dos recursos computacionais da rede corporativa. Assim como não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) em pastas da rede.

Todos os arquivos relativos as atividades da Empresa, devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos.

O espaço em disco é segmentado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo arquivos desnecessários. Arquivos que estão na rede com mais de 02 (dois) meses sem acesso, serão excluídos. No prazo de até 15 dias após a exclusão, é possível ter acesso aos arquivos excluídos, para isso, é necessário solicitar a TI. Após o prazo de 15 dias, não é mais possível recuperá-los.

Importante citar que: não é responsabilidade da área de TI a recuperação de arquivos que não respeitem as regras descritas.

12.3.7. MÍDIAS REMOVÍVEIS E DA PORTA USB

Não é permitido o uso de mídias removíveis na Empresa. Os casos excepcionais deveram ser, necessariamente, autorizados pela gerencia ou diretoria da Empresa.

Para liberação do uso de mídias removíveis e das portas USB é necessário justificar o uso e a aprovação da gerencia do solicitante ou da diretoria. Nos casos devidamente autorizados, o usuário de mídia removível e ou porta USB e o autorizador, serão diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos informacionais da Leaf.

Mesmo em casos autorizados, é vedado aos usuários utilizarem as mídias removíveis como meio de armazenamento perene das informações.

12.3.8. INTERNET

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual e ou como ferramenta de busca de informações pertinentes, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

É vedado qualquer tipo de download, como também, o upload de qualquer software licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados.

O acesso às páginas e web sites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdo impróprio e portais de relacionamentos. Os acessos à internet são monitorados através da autenticação do usuário na rede corporativa.

O uso da internet para assuntos pessoais deve ser restrito ao intervalo do colaborador e ao uso da rede disponível na área de convivência, sem comprometer as atividades na sub-rede corporativa

12.3.9. CORREIO ELETRÔNICO (E-MAIL)

É terminantemente proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral, e que possam causar prejuízos morais e ou financeiros. Também é vedado o uso do e-mail corporativo para assuntos pessoais.

Não se pode executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões de arquivos que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI. Também não se pode, utilizar o e-mail para enviar grande quantidade de mensagens (spam), reenviar e-mails do tipo corrente, aviso de vírus, avisos da Microsoft, criança desaparecida, criança doente, materiais preconceituosos ou discriminatórios, boatos virtuais e etc.

A utilização do e-mail/webmail da empresa fora do horário de trabalho, para posições que possuam controle/reporte de jornada, deve ser aprovado pela diretoria da Empresa.

Deve-se utilizar o e-mail para comunicações internas oficiais, as quais não necessitem obrigatoriamente do meio físico, essa prática diminui custo com impressão e aumenta a agilidade na divulgação do documento.

12.3.10. SOFTWARES DE MENSAGENS

Deve-se utilizar, preferencialmente, WhatsApp para contatos externos e o Lan Messenger para contatos internos, como ferramentas de comunicação e aumento de produtividade. Devendo ser usados, exclusivamente, para atividades relativas aos negócios e aos trabalhos desenvolvidos pela Leaf. Podendo ser monitorados e até mesmo vistoriados para efeito de auditoria, uma vez que são ferramentas para o desenvolvimento das atividades corporativas.

Enquanto o uso responsável dos sistemas de mensagens é estimulado, o seu abuso deve ser evitado.

Está terminantemente vedado o uso de sistemas de mensagens em redes de relacionamento pessoais enquanto no ambiente corporativo, devido a assincronia natural das mensagens instantâneas oriundas de terceiros sem finalidades laborais, o que, usualmente, torna-se contraproducente.

12.3.11. ACESSO REMOTO

Os usuários devem restringir o uso do acesso via VPN, acesso remoto, às finalidades relacionadas aos negócios da empresa, devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

É vedado aos usuários compartilhar credenciais de acesso por VPN com quem quer que seja, ou de acessar ele próprio o recurso de VPN e conceder o uso da sessão a qualquer outro colaborador.

Nunca deixar sessões de VPN abertas. Cada vez que o usuário se afastar do seu equipamento conectado via VPN, deve ser executado o *logoff* ou bloqueio do seu equipamento, além de manter-se conectado via VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

12.4. TRANSFERÊNCIA DE INFORMAÇÕES

Todas as transferências de informações entre a Leaf e seus clientes, são realizadas por meio seguro, cito E-mail seguro, FTPS, SFTP, Portal Leaf com HTTPS e selo de Segurança, APIs com login utilizando senhas criptografadas.

O acordo sobre o nível de segurança e, consequentemente, os meios que serão utilizados, estão explicitados nos contratos com cada um dos clientes e são dependentes do tipo de serviço a ser contratado.

Para os casos de desenvolvimento de novas soluções, as definições do acordo para as transferências de informações, também estarão explicitadas na documentação do projeto.

13. SANÇÕES ÀS VIOLAÇÕES DESSA POLÍTICA

Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos legais, se aplicáveis. O colaborador infrator deverá ser notificado, e a ocorrência da transgressão prontamente comunicada ao seu gestor imediato e à Diretoria.

A não observância pelo funcionário das normas desta Política, seja isolada ou cumulativamente, implicará ao infrator as seguintes punições: Aviso de Descumprimento, Advertência ou Suspensão, Demissão por Justa Causa e Abertura de Processo Civil ou Criminal, se for o caso.

O Aviso de Descumprimento será encaminhado por e-mail ao funcionário infrator e ao chefe imediato na primeira violação cometida, indicando qual a norma que foi violada.

Tanto o Aviso de Descumprimento quanto a Advertência ou Suspensão Disciplinar será aplicada seguindo as ações disciplinares (Advertência Verbal, Advertência Escrita, Suspensão, Desligamento sem Justa Causa, Desligamento com Justa Causa ou Abertura

de Processo Civil ou Criminal), de acordo com o grau de severidade dos casos de infrações ou na hipótese de reincidência e será registrada na ficha pessoal do funcionário.

A Demissão por justa causa será aplicada nos casos legais e de natureza grave ou nas hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, resumidas a seguir:

I. Ato de Improbidade – todo ato no qual o funcionário descumpre um dever legal, cuja conduta pode ser considerada abusiva e desonesta, causando prejuízos ao patrimônio do empregador.
II. Incontinência de conduta ou mau procedimento – A incontinência de conduta refere-se a quaisquer atos imorais praticados no ambiente de trabalho, tais como: exibir fotos pornográficas, desrespeitando os colegas e a Instituição. O mau procedimento ocorre toda vez que o funcionário age de forma incompatível com as regras da empresa.
III. Ato de Indisciplina ou de Insubordinação – O ato de indisciplina é caracterizado por descumprimento de ordens gerais do empregador a todos os empregados. Ato de insubordinação é o descumprimento de ordens pessoais do chefe imediato a determinado empregado.
IV. Violação de segredo da empresa – Consiste no ato do empregado, passar a outrem informações sigilosas, ou tão sem autorização do empregador.

Referência: Lei 13709/2018 – Lei Geral de Proteção de Dados Pessoais

14. CANAL DE ÉTICA

E-mail: canaldeetica@leaf.com.br

15. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.

16. HISTÓRICO DE ALTERAÇÕES

Data	Nº Revisão	Item	Descrição
20/11/2020	00	Todos	Emissão do documento
31/03/2021	01	Todos	Revisão para implantação do SGI
10/12/2021	02	Todos	Revisão de acordo com os apontamentos da auditoria
18/05/2022	03	Classificação	Alteração classificação do SGI
31/10/2023	04	Todos	Atualização do layout padrão da SGI
26/02/2024	05	Todos	Atualização da estrutura do documento
27/02/2024	06	Objetivos do SI e Missão	Inclusão dos objetivos do Sistema de Informação no item 7 e inclusão do comprometimento com a melhoria contínua no item 3 Missão
27/03/2024	07	Item 13	Inclusão de sanções e punições para violações da Política

17. HISTÓRICO DE VERIFICAÇÕES

Data	Nº Revisão	Item	Descrição
19/04/2024	07	Todos	Incluído Histórico de Verificações