POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Princípio

Esta Política aplica-se a todos os executivos, diretores, trabalhadores, agentes, afiliadas, contratados, consultores ou prestadores de serviços do controlador **TABELIONATO DE NOTAS E DE PROTESTO DE TITULOS E TABELIONATO E OFICIALATO DE REGISTRO DE CONTRATOS MARITIMOS** , inscrito no CNPJ sob o nº **55.807.183/0001-43,** doravante denominado "**CONTROLADOR**", que possam recolher, processar ou ter acesso a dados (incluindo dados pessoais e/ou dados pessoais sensíveis), sendo de responsabilidade de todos os acima familiarizarem-se com esta Política e garantir o cumprimento adequado.

A Política de Segurança da Informação tem como princípio estabelecer mecanismos de controles para garantir a efetiva proteção dos dados corporativos e pessoais dos colaboradores, sendo elas por aquisição no ato de sua coleta ou por resultado de processamento.

Contribuir para a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações da companhia.

Objetivo

- *Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico do* **CONTROLADOR***;*
- *Definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas, transmitidas ou impressas no* **CONTROLADOR**
- *Estabelecer as competências e atribuições dos atores envolvidos nesta política;*
- *Elencar os processos necessários para atingir um padrão aceitável de Segurança da Informação, conforme as legislações existentes e os padrões que o mercado estabelece;*

Abrangência

Esta política de segurança aplica-se a todos os funcionários, prestadores de serviços, incluindo trabalhos executados externamente ou por terceiros que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações do **CONTROLADOR***, na qual serão tratados como usuários. Todo e qualquer usuário que utilize recursos computadorizados da companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática pertencentes a organização.*

Conceitos, Termos e Abreviações

TERMOS/ABREVIAÇÕES	SIGNIFICADO

Ambiente de homologação	Ambiente tecnológico similar ao ambiente de produção, que possa simular situações muito próximas das que se encontra no dia a dia, composto por um conjunto de ferramentas necessárias para que usuários recebam e validem versões de sistemas de informação.
Ambiente de produção	Entende-se por ambiente de produção o conjunto composto de ferramentas necessárias para que usuários recebam versões finais de sistemas de informação que serão utilizadas no seu dia a dia;
Ameaça	Risco potencial de um incidente indesejado que pode resultar em dano para um sistema ou para a organização.
Aplicação	Programa de computador que auxilia o usuário a desempenhar uma atividade específica (ex.: AutoCAD, para a área de engenharia e arquitetura; Skype, para telefonemas e conferências).
Ativo	Qualquer coisa, material ou imaterial, que tenha valor para a organização.
Autenticação	Processo que verifica se o usuário identificado é realmente quem ele diz ser, através do uso de sua senha pessoal ou de outros mecanismos (ex.: tokens e smartcards).
Backup	Cópia de segurança de arquivos e sistemas
Biometria	Uso de mecanismos de identificação para restringir o acesso a determinados lugares ou serviços. Exemplos de identificação biométrica: através da íris (parte colorida do olho), da retina (membrana interna do globo ocular), da impressão digital, da voz, do formato do rosto e da geometria da mão;
Bloqueio de acesso	Processo que tem por finalidade suspender temporariamente o acesso
Colaborador	Funcionários de quaisquer cargos, estagiários, menores aprendizes e prestadores de serviços;
Confidencialidade	Termo utilizado em segurança da informação para garantir que as informações não sejam disponibilizadas ou divulgadas a pessoas ou processos não autorizados.
Disponibilidade	Termo utilizado em segurança da informação que garante que todas as informações e serviços importantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.
Evento de Segurança da Informação	Ocorrência identificada em um serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação anteriormente desconhecida, que possa ser relevante para a segurança da informação.
Integridade	Termo utilizado em segurança da informação que garante que as informações estejam protegidas de modificações, manipulações ou reproduções não autorizadas.
Informação Interna	É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
Informação Pública	É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
Informação Restrita	É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.
Login	Processo que permite a identificação, autenticação e autorização de acesso a um determinado sistema por um usuário. Também pode ser chamado de logon.
Normas de Segurança da Informação	Especificam os processos e controles que devem ser implementados para o alcance dos objetivos de segurança da informação definidos nesta política

Prestadores de serviços	Pessoa jurídica ou física que mantenha contrato de prestação de serviço no CONTROLADOR.
PSI	Política de Segurança da Informação
Restore	Recuperação de arquivos e sistemas.
Segurança da Informação	É o conjunto de controles que visam garantir a preservação dos aspectos de confidencialidade, integridade e disponibilidade das informações
Sistemas de Informação	Todo aplicativo, software e sistemas de informação que sejam adquiridos, desenvolvidos ou mantidos pela equipe técnica do **CONTROLADOR** ou por ela contratada.
Software	Um termo genérico para definir um programa de computador composto por uma sequência de instruções, que é interpretada e executada por um processador ou por uma máquina virtual. Essa sequência deve seguir padrões específicos que resultam em um comportamento desejado.
Usuário	servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;
Visitante	Todo indivíduo que não mantenha qualquer vínculo formal com o **CONTROLADOR**, ou seja, aqueles que não se enquadram na definição de Colaborador, conforme acima.
VPN (Rede Privada Virtual)	Conexão estabelecida sobre uma infraestrutura pública (internet), usando protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas.

Missão do departamento de tecnologia da informação

Manutenção de todo parque tecnológico da empresa, agregando valores na oferta de soluções em tecnologia da informação, alinhada aos objetivos e estratégia da empresa, atuando como guardião da segurança da informação e ativos de informática, promovendo segurança, disponibilidade e garantindo a integridade das informações.

Papéis e Responsabilidades

Compete ao Colaborador

- Cumprir as regras estabelecidas nesta política, normas e procedimentos de segurança da informação, bem como as demais leis, regulamentos e normas aplicáveis pelos órgãos reguladores;
- Proteger as informações contra acessos indevidos, divulgação não autorizados e descarte de forma segura;
- Zelar para que os recursos tecnológicos sejam utilizados de forma eficaz, dentro das finalidades corporativas e de conhecimento pelo **CONTROLADOR**;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (elevadores, escadas, taxi, Uber e quaisquer outros meios de transporte, restaurantes etc.) ou com terceiros não autorizados;
- Não compartilhar ou divulgar credenciais de acesso ou equipamentos sem a autorização explicita da área de Segurança da Informação. As senhas são de responsabilidade do usuário, sendo

individual e intransferível, sendo substituídas de forma periódica;

- Estar atualizado em relação a esta Política de Segurança e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de Segurança da Informação sempre que estiver com dúvidas;
- Solicitar quaisquer acessos ou perfis necessários as atividades profissionais por meio de ferramenta de chamados, contendo as aprovações do gestor imediato;
- Não criar, adquirir ou realizar uso de softwares não homologados e não instalados pela área de Tecnologia.
- Comunicar a área de Segurança da informação quaisquer riscos de segurança da informação existentes na área de atuação.

Compete ao Prestador de Serviços

- É de responsabilidade dos prestadores de serviços, observar e seguir as orientações estabelecidas para o cumprimento desta Política de Segurança da Informação.
- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo **CONTROLADOR**.
- Apresentar sempre que solicitado, o relatório de medição do serviço executado, na qual deverá conter a descrição de todas as atividades executadas, discriminando de forma detalhada o serviço executado;

Compete ao departamento de Tecnologia da Informação

- Determinar as diretrizes de Segurança da Informação, garantindo ações de prevenção contra incidentes de segurança;
- Aprovar e revisar periodicamente a Política de Segurança da Informação;
- Propor controles e melhorias relacionadas à segurança da informação e privacidade e proteção de dados pessoais;
- Definir e documentar as políticas e procedimentos relacionados a operacionalização da segurança da informação;
- Monitorar e analisar os alertas e informações relacionadas à segurança das informações;
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;
- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;
- Disseminar a cultura de Segurança junto as demais áreas da empresa;
- Participar dos projetos em que a área estiver envolvida acompanhando e sugerindo questões relacionadas ao tema da área.
- Realizar as cópias de segurança do ambiente tecnológico;
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os

controles necessários para cumprir os requerimentos de segurança estabelecidos nesta PSI e normas adicionais;

Compete ao departamento Recursos Humanos

- Disponibilizar a política e as normas de Segurança da Informação para todos os colaboradores e assegurar que ele esteja ciente das diretrizes, normas e procedimentos internos;
- Informar ao departamento de tecnologia e/ou Segurança da Informação todos os desligamentos, transferências, férias e modificações no quadro de funcional, para que seja realizado a revogação dos acessos;
- Garantir que os colaboradores tenham ciência a esta política de segurança da informação.

Compete ao departamento Jurídico

- Requerer a inserção de cláusulas que obriguem o cumprimento desta PSI, proteção e privacidade de dados pessoais, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade e preservando sua confidencialidade.
- Avaliar as ações de remediação previstas para os casos de não conformidade a PSI e demais normas e procedimentos;

Notificação de Incidentes de Segurança da Informação

Compete ao departamento de tecnologia e/ou segurança da informação, o reporte a qualquer evento que possa vir a comprometer a segurança das informações da empresa, zelando pelo parque tecnológico como também em especial aos dados pessoais dos titulares dos dados.

Compete também ao departamento de tecnologia e segurança da informação, reportar ao Encarregado de Proteção de Dados Pessoais da empresa, qualquer evento de segurança, para que sejam tomadas toda as medidas cabíveis sobre.

A notificação ao incidente de segurança, na qual envolva dados pessoais deverá se estender ao titular, à Autoridade Nacional de Proteção de Dados, ao Juiz Corregedor Permanente e à Corregedoria Geral da Justiça, **no prazo máximo de 48 horas úteis**, contados a partir do seu conhecimento, de incidente que possa acarretar risco ou dano relevante aos titulares, com esclarecimento da natureza do incidente e das medidas adotadas para a apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados.

Dados Pessoais de Funcionários

1. Cada usuário é responsável pela proteção dos dispositivos físicos contendo informações do **CONTROLADOR** que estão sob sua guarda;
2. Cada usuário deve estar ciente que o uso de qualquer recurso de TI no ambiente da empresa, utilizando recursos e equipamento corporativos, está sujeito a vistoria e auditorias, sempre que a

lei local permitir.

3. Cada usuário deve estar ciente que o uso de qualquer recurso de TI no ambiente do **CONTROLADOR**, ainda que de propriedade pessoal, está sujeito a vistoria, sempre que a lei local permitir.

Dados Pessoais de Funcionários

O **CONTROLADOR** se compromete a não acumular ou manter intencionalmente dados pessoais de funcionários com finalidades de processamento, além daqueles relevantes na condução do seu negócio, incluindo o cumprimento de obrigações legais, garantindo assim um dos princípios da minimização de dados atendendo as exigências da vigente Lei de Proteção de Dados 13.709/18 - LGPD.

Assim, todos os dados pessoais de funcionários serão considerados dados confidenciais e serão mantidos a fim de cumprimentos de obrigações legais. Quando não mais for, contudo, necessário seu registro, a exclusão desses dados poderá ser solicitada pelo usuário, atendendo-se, assim, o direito de esquecimento coberto pela Lei de Proteção de Dados 13.709/18 - LGPD.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando consentido pelo usuário e cumprimento de uma base legal seguido as exigências da vigente Lei de Proteção de Dados 13.709 – LGPD podendo ser revogado o consentimento a qualquer momento.

Programas Ilegais

É expressamente proibida a instalação ou uso de quaisquer programas não licenciados popularmente conhecidos como programas PIRATAS dentro da organização.

Periodicamente e sem aviso prévio, o departamento de tecnologia da informação realizará auditorias em servidores, computadores (desktop e ou laptops), dispositivos móveis ou qualquer outro dispositivo fornecido pela organização e disponibilizados ao usuário.

Permissões e Senhas

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da Companhia, o setor de origem do novo usuário deverá comunicar esta necessidade ao departamento de tecnologia, por meio do sistema padrão de chamados de suporte, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos. A Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada 45 (quarenta e cinco) dias.

Sempre será recomendado senhas tenham sempre um mínimo de 8 (oito) caracteres alfanuméricos e com caractere especial tais como (% $ # @ ! * &).

Todo e qualquer tipo de transferência de acesso em caso de ausência do colaborador a plataformas eletrônicas e/ou permissão de aprovação quando este existir, deverá ser comunicado ao departamento de tecnologia pelo gestor imediato do colaborador, para que as permissões possam ser alteradas (delegação de poderes).

Coleta de Dados Pessoais

A coleta de dados pessoais fica restrito à apenas para finalidades definidas pela organização, obedecendo os princípios previsto no artigo 6º da Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

Compartilhamento de Pastas e Dados

É de obrigação dos usuários rever periodicamente todos os compartilhamentos existentes em suas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam disponíveis a acessos indevidos.

Sistemas de Câmeras

O acesso às imagens das câmeras internas deve ser, em regra, restrito às áreas de tecnologia e/ou segurança da informação. Já as câmeras vinculadas à prestação de serviços contratuais a clientes do Controlador devem ser acessadas apenas pelo departamento de monitoramento.

Quando houver necessidade específica de análise das imagens, o caso deverá ser tratado com o gestor responsável pela área envolvida, para avaliação da finalidade, necessidade e extensão da inspeção.

As imagens devem ser armazenadas, em regra, pelo prazo razoável de **30 dias**, mantidas sob sigilo e utilizadas apenas para finalidade definida. Após esse período, deverão ser eliminadas de forma segura da base de dados do Controlador.

Cópia de Segurança (backup) de Sistemas e Servidores

As cópias de segurança dos sistemas integrados e servidores de rede são responsabilidade do departamento de Tecnologia da Informação e devem ser realizadas diariamente, conforme boas práticas de segurança e recursos disponíveis do **CONTROLADOR**. O backup diário deve priorizar aplicações, sistemas e arquivos essenciais para a continuidade do negócio.

Admissão/Demissão de Funcionários/Temporários/Estagiários

Toda contratação que envolva a utilização de sistemas, dispositivos móveis ou quaisquer equipamentos fornecidos pelo **CONTROLADOR** deverá ser comunicada ao Departamento de Tecnologia da Informação, que registrará o respectivo ticket e providenciará, quando necessário, a criação de usuário, senha, e-mail e a formalização dos termos de responsabilidade.

Em caso de demissão ou desligamento, o Departamento de TI deverá ser previamente comunicado para realizar o inventário dos termos assinados, inativar os acessos do colaborador em todos os sistemas e avaliar os equipamentos devolvidos. Caso sejam identificadas avarias decorrentes de mau uso, os valores de reparo poderão ser apurados e tratados conforme contrato, políticas internas e limites legais aplicáveis.

O registro do usuário inativado será mantido pelo prazo de 3 meses, após o qual deverá ser eliminado definitivamente, observadas as regras internas de retenção e descarte.

Compete ao setor de Recursos Humanos ou Departamento Pessoal dar ciência ao colaborador sobre a Política de Segurança da Informação — PSI, coletando sua assinatura de concordância. Nenhum colaborador, empregado, estagiário, aprendiz ou temporário poderá iniciar suas atividades sem expressa ciência e concordância com a PSI do **CONTROLADOR**.

Base legal de apoio: LGPD, Lei nº 13.709/2018, art. 6º, especialmente os princípios da finalidade, necessidade, segurança e responsabilização; e art. 46, quanto à adoção de medidas técnicas e administrativas para proteção dos dados pessoais.

Transferência de Funcionários

Todo e qualquer movimento interno de transferência de cargo, atribuição ou departamento, deve ser comunicado ao departamento de tecnologia da informação e/ou segurança da informação, a fim de que este realize os ajustes de permissões em toda estrutura de sistemas e acessos compartilhados de informática.

Cópias de Segurança de Arquivos Individuais

O departamento de tecnologia da informação não se responsabiliza por qualquer arquivo pessoal utilizado em equipamentos da companhia, ficando de responsabilidade do próprio usuário a elaboração de cópias de segurança ("backups") arquivos textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos eletrônicos, de uso pessoal na organização residentes em suas estações de trabalho.

São disponibilizados locais de armazenamentos em rede para armazenamento de arquivos eletrônicos de finalidades diversas e estes repositórios fazem parte de jornadas de backups diários do departamento de tecnologia da informação.

Propriedade Intelectual

É de propriedade do **CONTROLADOR**, todos os “designs”, planilhas, documentos, criações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo empregatício ou contratual com o **CONTROLADOR**.

Uso do Ambiente Web (internet)

O acesso à internet será autorizado apenas aos usuários que necessitem desse recurso para o desempenho de suas funções, incluindo empregados, estagiários, aprendizes, profissionais terceiros e demais pessoas autorizadas, conforme contrato ou vínculo estabelecido com o CONTROLADOR.

O uso não profissional deverá ocorrer exclusivamente pela rede Wi-Fi de visitantes, mediante voucher. Todos os acessos poderão ser monitorados, sendo proibido o acesso a conteúdos impróprios, ilegais ou incompatíveis com as políticas internas da companhia.

A definição dos usuários autorizados a navegar na internet corporativa será de responsabilidade da direção da companhia. A instalação de aplicativos ou softwares nos equipamentos corporativos somente poderá ser realizada pelo Departamento de Tecnologia da Informação. Qualquer instalação feita por pessoa não autorizada será considerada violação de conduta.

Durante o uso da internet, é proibido acessar, visualizar, copiar, baixar ou transferir conteúdos relacionados a:

- estações de rádio ou conteúdos não relacionados às atividades profissionais;
- pornografia ou conteúdo sexual;
- atividades ilegais;
- preconceito, discriminação, depreciação ou incitação contra pessoas ou grupos;
- salas de discussão ou fóruns não relacionados aos negócios do CONTROLADOR;
- discussões públicas sobre os negócios da companhia, salvo autorização da Diretoria;
- divulgação ou distribuição de informações classificadas como confidenciais;
- download de arquivos, programas ou softwares ilegais.

O uso da internet corporativa deverá observar as finalidades profissionais, as regras da Política de Segurança da Informação e os princípios de segurança, necessidade, finalidade e transparência.

Uso do Correio Eletrônico - ("e-mail")

O correio eletrônico fornecido pelo CONTROLADOR é uma ferramenta corporativa destinada exclusivamente à comunicação interna e externa relacionada às atividades da companhia, sendo vedado seu uso para finalidades pessoais, salvo em situações excepcionais, previamente autorizadas pela Diretoria, por escrito ou por meio eletrônico.

As mensagens devem ser redigidas em linguagem profissional, respeitosa e compatível com os princípios, valores e imagem institucional do CONTROLADOR. É proibido o envio de mensagens com conteúdo ofensivo, discriminatório, racista, difamatório, pornográfico, relacionado a terrorismo, bullying, ameaças, correntes, linguagem de baixo calão ou qualquer comunicação que possa causar prejuízo a pessoas, empresas ou à reputação da organização.

O uso do e-mail corporativo é pessoal e vinculado ao usuário, que será responsável pelas mensagens enviadas por sua conta. O recurso deverá ser utilizado de forma criteriosa, necessária e adequada, evitando sobrecarga ou congestionamento dos serviços.

O uso do e-mail corporativo deverá ocorrer, em regra, durante o horário comercial ou dentro do horário previsto no contrato de trabalho, salvo necessidade profissional autorizada.

Quando houver tratamento de assuntos relacionados a clientes, colaboradores, fornecedores, terceiros, estagiários, aprendizes ou representantes, é proibida a exposição desnecessária de dados pessoais. O compartilhamento dessas informações somente poderá ocorrer por pessoa autorizada, para finalidade legítima e estritamente necessária. Quando necessário, deverá ser criado e-mail interno específico para tratamento do caso, sendo a resposta final ao cliente realizada pelo departamento responsável pelo atendimento.

É vedado o envio de mensagens que contenham dados pessoais ou informações confidenciais sem autorização, necessidade ou finalidade compatível com as atividades do CONTROLADOR.

Auditorias nos servidores de e-mail poderão ser realizadas para garantir a segurança, a disponibilidade, a performance dos serviços e o cumprimento da Política de Segurança da Informação — PSI, observados os princípios da transparência, necessidade, proporcionalidade e segurança.

E-mails suspeitos ou com anexos duvidosos não devem ser abertos. O usuário deverá comunicar

imediatamente o Departamento de Tecnologia da Informação para análise e tratamento, a fim de prevenir vírus, malwares, vazamento de dados ou comprometimento da infraestrutura tecnológica da organização.

Uso do Celular

Os dispositivos móveis e linhas corporativas disponibilizados pelo CONTROLADOR deverão ser utilizados exclusivamente para fins profissionais e em benefício das atividades da organização.

A utilização de dispositivos pessoais para atividades corporativas observará as regras previstas na Política de BYOD (Bring Your Own Device) da organização, incluindo critérios de autorização, segurança da informação, controle de acesso e proteção de dados pessoais. O uso de equipamento pessoal dependerá de aprovação do Comitê de Segurança e do Departamento de Tecnologia da Informação.

Independentemente do dispositivo utilizado — corporativo ou pessoal — o colaborador deverá cumprir integralmente as políticas internas de segurança, confidencialidade e proteção de dados, conforme ciência e concordância formal previamente realizada.

Todos os dados corporativos ou dados de contato de clientes coletados durante as atividades profissionais deverão ser registrados no sistema oficial de CRM da empresa. Quando armazenados temporariamente em dispositivo pessoal autorizado, deverão ser posteriormente eliminados do aparelho após sua devida replicação ao ambiente corporativo.

É proibida a coleta, armazenamento ou tratamento de dados pessoais sem autorização da organização, finalidade legítima e necessidade relacionada às atividades profissionais, sujeitando o colaborador às medidas disciplinares cabíveis, inclusive aquelas previstas no art. 482, alíneas “e” e “h”, da CLT.

Necessidade de Novos Sistemas, Aplicativos e ou Equipamentos

A definição de compra (marca, modelo) fica de inteira responsabilidade do departamento de tecnologia da informação.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware), deverá primeiramente ser discutida com o departamento de tecnologia da informação na qual irá avaliar, aconselhar e emitir o seu aceite.

O departamento de tecnologia da informação fica **ISENTO** por qualquer decisão tomada sobre compra, troca ou manutenção de equipamentos (hardware) e ou software sem a sua consulta prévia.

Responsabilidades por Equipamento Corporativos

Os usuários que tiverem direito ao uso de computadores pessoais (laptop), ou qualquer outro equipamento computacional dentro do ambiente tecnológico do **CONTROLADOR**, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;

- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc;
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto:

- Registre a ocorrência em uma delegacia de polícia **PRESENCIAL** (Não pode ser via WEB);
- Comunique ao seu superior imediato e ao Setor de Informática no mesmo instante através de e-mail;
- Envie uma cópia da ocorrência para o Setor de Informática.

Responsabilidades dos Gerentes/Supervisores

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso dos colaboradores, pertencentes às suas equipes, aos sistemas e informações da companhia, cabendo a eles verificar se os colaboradores estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O departamento de tecnologia da informação fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;
- Que informação ou rotina determinadas usuário acessou;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

Uso de Antivírus

A atualização do antivírus será automática, agendada pelo departamento de tecnologia da informação. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

- Todo arquivo em mídia, proveniente de entidade externa ao **CONTROLADOR**, deve ser verificado por programa antivírus.

- Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.
- Todas as estações de trabalho devem ter um antivírus instalado.

Portas USB

A porta USB do computador é um importante ponto de vulnerabilidade de segurança, especificamente com o uso de pendrives ou discos externos, pois pode ser usada para fuga de informação e o seu uso não está em conformidade com a LGPD.

Por esse motivo, o uso de mídias removíveis e portas USB dos computadores é bloqueado por padrão (privacy by default), para todos os computadores do **CONTROLADOR**.

As portas USB dos computadores são liberadas somente para o uso de dispositivos de entrada de dados, como teclados, mouses e headsets, bem como também para os assinadores digitais.

Violação de Conduta

Se caracteriza violação PSI e Violação de Conduta qualquer ato que venha a:

- Expor a empresa a riscos elevados em possíveis perdas de receitas efetiva, seja ela por comprometer o nível de segurança dos dados ou em potencial perda de ativo;
- Envolva, exponha ou revele informações confidenciais;
- Viole os direitos autorais, negociações ou uso não autorizado de dados corporativos da empresa;
- Utilizar dos recursos corporativos para propósitos pessoais, ilícitos ou que venham a violar qualquer regulamento, lei ou qualquer outro dispositivo governamental;
- A não comunicação imediata de quaisquer descumprimentos da Política;
- Uso da imagem do **CONTROLADOR** de forma não autorizada.

Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas e/ou pastas públicas na rede como local de digitalização.

Descumprimento da Política de Segurança da Informação

Na hipótese de violação desta **PSI** ou das normas de segurança da informação, a Diretoria, com o apoio das áreas de Tecnologia e Segurança da Informação, Compliance, e Recursos Humanos, determinarão as sanções administrativas que serão aplicadas ao infrator, sendo que:

1. Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Matriz de Penalidades;
2. Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo

contrato estabelecido violado.

Como assegura o art. 482 do decreto lei 5.452/43 da CLT: “Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

...

g) violação de segredo da empresa”.

E, ainda, a Lei nº 9.279/96, no seu art. 195: “Comete crime de concorrência desleal quem:

...

xi - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

xii - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude”.

Regulamentos Aplicável

- Lei 12.527, de 18 de novembro de 2011 – Lei de acesso à informação;
- Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;
- NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;
- NBR/ISO/IEC 27001/2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;
- ISO/IEC Guide 73:2002 - Gestão de Riscos / Vocabulário - Recomendações para uso em normas;
- Norma NBR/ISO/IEC 27005:2008 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);
- Art. 9º, Parágrafo Único da Lei do Software 9.609/98;
- Art. 932, Inc. III da Lei de Responsabilidade Civil 10.406/02.
- Artigo 482 do Decreto-Lei 5.452/43 (CLT): "Violação de segredo da empresa" constitui justa causa;
- Lei nº 9.279/96: Divulgação de informações confidenciais constitui crime de concorrência desleal;

Data:	/ /

Assinado digitalmente por:

Por: INOVALGPD CONSULTORIA E TREINAMENTOS LTDA
Encarregado de Proteção de Dados: Wellington Rodrigues da Silva
CNPJ: 20.705.613/0001-31
Em: Terça-feira, 25 de Agosto de 2026, 13:05
Doc: ADM-20260512-001 v6 | SHA256: a87fd57dc9707767637db6707945c196de43808b17bf01b7ee57ace27d20a594

ELABORADO POR:

Encarregado de Proteção de Dados Pessoais (DPO)

InovaLGPD Consultoria e Treinamentos LTDA

20.705.613/0001-31

Representada por: Wellington Rodrigues da Silva

Data: / /

APROVADO POR:

CONTROLADOR

CNPJ: 55.807.183/0001-43

MARILIA DE ABREU OLIVEIRA:70112865194

Assinado de forma digital por MARILIA DE ABREU OLIVEIRA:70112865194
Dados: 2026.08.25 13:13:23 -03'00'

Oficial Titular

TABELIONATO DE NOTAS E DE PROTESTO DE TITULOS E TABELIONATO E OFICIALATO DE REGISTRO DE CONTRATOS MARITIMOS