EXPLORITAS

EXPLORITAS ADMINISTRAÇÃO FINANCEIRA LTDA

MANUAL DE SEGURANÇA DA INFORMAÇÃO

Dezembro 2025

O NÃO CUMPRIMENTO DESTE MANUAL PODERÁ RESULTAR EM AÇÕES DISCIPLINARES APROPRIADAS, INCLUINDO ADVERTÊNCIAS, QUE PODERÃO VIR A CULMINAR NO DESLIGAMENTO DA EMPRESA. ESTE MANUAL NÃO É DESTINADO A CRIAR QUALQUER CONTRATO DE TRABALHO ENTRE A EMPRESA E QUAISQUER DE SEUS MEMBROS.

Revisões

Revisão	**Data**	**Alteração**	**Responsáveis**
00	01/2016	Criação do Documento	Murad Antun
01	01/2017	Revisão do Documento	Murad Antun
02	12/2018	Revisão do Documento	Murad Antun
03	12/2019	Revisão do Documento	Murad Antun
04	12/2020	Revisão do Documento	Murad Antun
05	12/2021	Revisão do Documento	Rodrigo Hokamura
06	12/2022	Revisão do Documento	Rodrigo Hokamura
07	12/2023	Revisão do Documento	Rodrigo Hokamura
08	12/2024	Revisão do Documento	Ricardo Campos
09	12/2025	Revisão do Documento	Vitor Inaba

Objetivos

O objetivo deste Normativo é garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização dos negócios da Gestora de Investimentos. Definimos assim processos, ferramentas e diretrizes para assegurar que as informações obtidas e geradas sejam acessadas por quem de direito e manuseadas dentro dos padrões éticos e com a devida diligência.

Esta Política de segurança da informação, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da Companhia, ou acesso a informações pertencentes à Gestora de Investimentos.

Todo e qualquer usuário de recursos computadorizados da Companhia tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

- Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados/ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

É Dever de todos dentro da empresa considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização dos negócios, que possui grande valor para a organização e deve sempre ser tratada profissionalmente.

Classificação da Informação

É de responsabilidade do Gestor 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 abaixo:

Pública	Toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
Interna	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.
Confidencial	Toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
Restrita	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.

Todos na empresa não devem 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 ou mídia confidencial ou restrita sobre suas mesas.

Dados Pessoais De Funcionários

A Empresa se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio.

Todos os Dados Pessoais de Funcionários serão considerados dados confidenciais e não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da empresa.

Programas Ilegais

É terminantemente proibido o uso de programas ilegais (PIRATAS) na empresa. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da empresa.

Os computadores da empresa seguem uma restrita política para download ou instalação de aplicativos. Tal prática somente é permitida de posse das credenciais de administrador. O sócio com esta credencial fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

Permissões e Senhas

Serão criados dentro de nossa rede de computadores diretórios exclusivos para cada área, sendo esses diretórios bloqueados para as áreas que não sejam diretamente ligadas às informações contidas nos mesmos. Tais diretórios possuem direitos de acesso em sua raiz e respeitam a divisão de áreas estabelecida pela organização a saber:

Gestão
Comercial
Administrativo
Risco
Compliance

Cada usuário recebe direitos para acessar um ou alguns destes diretórios conforme as atividades que deverá realizar na empresa.

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 sócio responsável por TI, por e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada a cada ano.

Os computadores pessoais para cada funcionário têm senha individual de acesso. Caso o funcionário não esteja no ambiente de trabalho, é obrigatório bloquear o computador via senha pessoal para segurança e integridade dos dados.

Por segurança, TI recomenda que as senhas tenham sempre um mínimo de 8 (oito) caracteres alfanuméricos.

Todos os usuários responsáveis pela aprovação eletrônica de processos deverão comunicar ao Setor de TI qual será o seu substituto quando de sua ausência da empresa para que as permissões possam ser alteradas (delegação de poderes).

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.

Cópia De Segurança (Backup) do Sistema Integrado e Servidores de Rede

Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade de TI e serão ser feitas diariamente. Mais informações sobre horários e locais dos backups estão disponíveis no normativo de Plano de Continuidade de Negócios.

Segurança e Integridade do Banco de Dados

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva da área de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

Admissão/Demissão de Funcionários, Temporários e Estagiários

O setor responsável pela contratação ou demissão deverá informar ao gestor de TI, para que os funcionários possam ser cadastrados ou excluídos nos sistemas da empresa. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id).

Cabe ao setor solicitante da contratação a comunicação sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à empresa, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.

No caso de demissão, o fato deve ser informado o mais rapidamente possível ao gestor de TI, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor da contratação obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação.

Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política via Manual de Compliance.

Cópias de Segurança de Arquivos Individuais

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da empresa.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da empresa, T.I. disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

Propriedade Intelectual

É de propriedade da Exploritas Ltda, todos os arquivos ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a empresa.

Uso do Ambiente Web

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na empresa. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso da Internet será monitorado pelo Gestor de T.I., inclusive através de "logs" no servidor que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou. A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição dos Sócios da empresa, com base em recomendação do Gestor de T.I.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da empresa sem expressa anuência do gestor de T.I.

Nosso Wi-Fi não disponibilizará acesso à Web para computadores de clientes e demais prestadores de serviços uma vez que os mesmos não estão sob a política de segurança da informação da Exploritas Ltda.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da empresa;
- Que promovam discussão pública sobre os negócios da Exploritas Ltda, a menos que autorizado pelos sócios responsáveis;
- Que possibilitem a distribuição de informações de nível "Confidencial".
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

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

O correio eletrônico fornecido pela Exploritas Ltda é um instrumento de comunicação interna e externa para a realização do negócio da empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da empresa, não podem ser contrárias à legislação vigente e nem aos princípios éticos da empresa. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da Exploritas Ltda.

Para incluir um novo usuário no correio eletrônico, o respectivo gestor deverá fazer um pedido formal ao Gestor de T.I., para que este providencie a inclusão do mesmo.

A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da empresa.

O Setor de T.I. poderá, visando evitar a entrada de vírus na empresa, bloquear o recebimento de e-mails provenientes de sites gratuitos.

Uso de Telefones, Celulares e Smartphones

Visando a segurança da informação, adotamos os seguintes critérios em relação ao uso de telefones:

- As ligações da mesa de operação e da mesa de clientes são gravadas por segurança e armazenadas em local seguro. As diretrizes sobre estas gravações estão na norma de Gravações Telefônicas.
- Celulares são de uso restrito dentro do ambiente de trading. Neste ambiente, todo e qualquer contato com entidades de relacionamento da Exploritas Ltda deve ser realizado via telefone gravado.
- Celulares de clientes não poderão usar o Wi-Fi da empresa para acesso à web, mas deverão sim utilizar a rede Exploritas-Guest.

Necessidades De Novos Sistemas, Aplicativos ou Equipamentos

O Setor de T.I. é responsável pela aplicação da Política da empresa em relação à definição de compra e substituição de “software” e “hardware”.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de T.I.

Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

Uso de Notebooks de Propriedade da Empresa

Os usuários que tiverem direito ao uso de notebooks de propriedade da Exploritas Ltda, 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.

Em caso de furto:

Registre a ocorrência em uma delegacia de polícia;

Comunique ao seu gestor e ao Setor de T.I;

Envie uma cópia da ocorrência para o Setor de T.I.

Responsabilidades dos Gestores

Os gestores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da empresa, cabendo a eles verificarem se os mesmos 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.

De tempos em tempos o Setor de T.I. fará levantamentos de acessos dos usuários às informações, verificando se as ações estão em concordância com as autorizações.

Uso De Anti-Vírus

Todo o ambiente de tecnología da Exploritas Ltda é protegido por sistema anti-vírus administrado pelo Setor de T.I.

Todo arquivo em mídia proveniente de entidade externa à empresa deve ser verificado por programa antivírus.

Todo arquivo recebido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de T.I., via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Penalidades

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.