# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Objetivo**

Esta política representa as estratégias e abordagens que a Criasett utiliza para promover o adequado manuseio da informação, de forma clara e concisa as regras, recomendações e ações para o tratamento das questões de segurança da informação obtidas de seus clientes, colaboradores, fornecedores e o público em geral.

**Introdução**

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.
Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos e prejudicar nosso crescimento e vantagem competitiva. Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação da Criasett.

Para tanto, visa atingir os seguintes objetivos:

• Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;
• Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas, acidentais ou propositais;
• Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Proteção da Informação**

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos da Criasett, a informação deve ser adequadamente manuseada e protegida.
A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.
Toda informação relacionada às operações da Criasett, gerada ou desenvolvida nas dependências da Criasett, pelos colaboradores (setorial) durante a execução das atividades ou de prestadores de serviços, constitui ativo desta instituição, essencial à condução de negócios, e em última análise, à sua existência.
Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.
A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da Criasett.
É diretriz que toda informação de propriedade da Criasett seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

**Descarte de informações**

O descarte da informação é realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital. A informação é descartada considerando prazos mínimos legais ou regulatórios, bem como sua necessidade para o negócio ou a área, o que for maior.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Responsabilidades**

É missão e responsabilidade de cada correspondente, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.
Todas as atividades executadas pelo Correspondente, por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.
Para auxiliar a todos os colaboradores nessa missão, a direção e o RH da Criasett , que administra as disciplinas de conhecimento darão suporte a essa ciência.
A direção e o RH são os responsáveis por editar as políticas e padrões que apóiam a todos na proteção dos ativos de informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema.

**Informações Confidenciais**

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Criasett.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

São responsáveis pela observância desta Política os diretores, acionistas, sócios, colaboradores, estagiários, prestadores de serviços, consultores diversos (incluindo advogados, auditores e consultores financeiros) fornecedores, concorrentes. O responsável que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem consentimento por escrito da Criasett. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidas pela Criasett.

O responsável deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.
O responsável deverá informar prontamente a Criasett sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

**Violação da Política, Normas e Procedimentos de Segurança da Informação**

As violações de segurança devem ser informadas á direção e ou RH. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas;

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração da Criasett e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os responsáveis às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

## PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEG. INFORMAÇÃO

### Classificação da Informação

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.
As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.
As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas pelos responsáveis de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário. Cabem ao responsável todos os esforços necessários de segurança para protegê-las.
Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem da Criasett, ou prejuízos graves ao crescimento.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**São exemplos de informações confidenciais:**

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;
- Informações sobre produtos e serviços que revelem vantagens competitivas da Criasett frente ao mercado;
- Todo o material estratégico da Criasett (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Quaisquer informações da Criasett, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.
- Informações pessoais dos colaboradores: salários, endereços; entre outros.

**Acesso a Sistemas e Recursos de Rede**

Os responsáveis são totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.
O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Correio Eletrônico**

O sistema de correio eletrônico deverá ser utilizado somente para atividades relacionadas à Criasett e que contribuam positivamente.

**É proibido:**

- Enviar ou ser conivente com conteúdo não-aderente a esta política de segurança;
- Enviar mensagens para listas de clientes, fornecedores e parceiros que não sejam de interesse da Criasett, sem a devida autorização da área responsável;
- Enviar mensagens que configurem spam para usuários internos e externos;
- Enviar mensagens com a identificação do remetente alterada ou falsificada;
- Enviar mensagens com o conteúdo alterado ou falsificado;
- Invadir a privacidade de usuários pelo acesso não-autorizado à sua caixa postal;
- Enviar informações confidenciais da Criasett para redes públicas (Internet), sem autorização.

**Utilização dos Recursos de Informação**

Apenas os equipamentos e software disponibilizados e/ou homologados pela Criasett podem ser instalados e conectados à rede da Criasett
Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Autenticação e Senha**

Os responsáveis são responsáveis por todos os atos executados com seu identificador (login / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

**Os responsáveis devem:**

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não contá-la a ninguém e não anotá-la em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Selecionar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar

**Direitos de Propriedade**

Todo produto resultante do trabalho realizado na Criasett (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da Criasett. Em caso de extinção ou rescisão de contrato ou de prestação de serviços, por qualquer motivo, implicarão na extinção imediata de todos os direitos de uso e acesso a direitos ativos da informação que possuíam o indivíduo ou empresa.

**Equipamentos particulares/privados**

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da organização.

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

criasett
indústria gráfica

**Mesa Limpa**

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.
Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

**Conversas em Locais Públicos e registro de informações**

Não discutir ou comentar assuntos confidenciais em locais públicos ou em áreas expostas (transportes, restaurantes, encontros sociais, etc.) incluindo comentários e opiniões em blogs e redes sociais.

Código do documento: P-DIR-06
Revisão: 00
Data de emissão: 20/20/2026
Área responsável: Diretoria
Aprovação: Diretoria
Classificação: Documento público