NORMAS DE SEGURANÇA

DA INFORMAÇÃO - NSI

DanPower

PROGRAMA DE SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

NORMAS DE SEGURANÇA DA INFORMAÇÃO – NSI

DanPower Caldeiras e Equipamentos Ltda, através da presente e como parte da formação e implementação de um Programa de Segurança da Informação e Governança em Privacidade e Proteção de Dados Pessoais, estabelece a presente **Normas de Segurança da Informação – NSI**, a qual é parte integrante da Política de Segurança da Informação e será regida pelas previsões a seguir elencadas:

1. OBJETIVO E ABRANGÊNCIA

O presente documento denominado **Normas de Segurança da Informação - NSI**, é parte integrante e complementar da Política de Segurança da Informação – PSI e é responsável por descrever e detalhar normas específicas de segurança da informação a serem seguidas por todos aqueles que mantém vínculo com a **DanPower**.

2. NORMAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

2.1 INTERNET

Todas as regras atuais da DanPower visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida no ambiente da internet está sujeita a divulgação e auditoria pela **DanPower**. Portanto, a **DanPower**, em total conformidade legal, reserva-se o direito de

monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A **DanPower**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor, sem prejuízo de eventuais medidas disciplinares.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A utilização desse serviço **para fins pessoais é vedado**, ressalvadas as exceções autorizadas pelo gestor da área, e desde que não prejudique a empresa e também não cause impacto no tráfego da rede.

Nos casos de uso da internet que cause impacto **no tráfego de dados (banda)** da rede no geral e que possam acarretar lentidão nos acessos à internet, o interessado **deverá pedir autorização e planejar junto a área de Tecnologia da Informação** o momento adequado para realizar a operação, a fim de não comprometer o uso da internet pelos demais setores.

Somente os colaboradores que estão devidamente autorizados a falar em nome da **DanPower** para os **meios de comunicação** poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela empresa poderão copiar, compartilhar, captar, fotografar, imprimir, enviar arquivos ou informação contendo, por exemplo, prints de tela, desenhos, projetos, imagens, documentos

etc, para si ou terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações de qualquer área/departamento da **DanPower** em listas de discussão, fóruns, sites, redes sociais, grupos, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir.

Os colaboradores com acesso à internet **não poderão fazer o download (baixa) de softwares/programas**, ressalvada autorização da área de Tecnologia da Informação.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da **DanPower** para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento ou músicas (em qualquer formato) não poderão ser utilizados, ressalvada autorização do gestor e da área de Tecnologia da Informação.

Materiais de cunho sexual não poderão ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (envio, subida) de qualquer software licenciado à **DanPower** ou de dados de sua propriedade aos seus parceiros e clientes sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da **DanPower** para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Os sistemas de administração/acesso remoto poderão ser utilizados, desde que sob autorização e supervisão da área de Tecnologia da Informação.

Serviços de comunicação instantânea/mensageria serão disponibilizados aos usuários que tenham atividades profissionais relacionadas a essas categorias e poderão ser bloqueados pela área da Tecnologia da Informação.

2.2 CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da **DanPower** quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da **DanPower** é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição.

A utilização desse serviço **para fins pessoais é vedado**, ressalvadas as exceções autorizadas pelo gestor da área, e desde que não prejudique a empresa e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do **DanPower** para as ações exemplificativas abaixo:

- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- ressalvada autorização do gestor da área, é proibido transmitir conteúdo corporativo (sigiloso, ou não) através do email profissional para o endereço de e-mail pessoal;
- enviar mensagem por correio eletrônico usando o nome ou o endereço de outra usuário/pessoa que não esteja autorizado a utilizar;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do **DanPower** estiver sujeita a algum tipo de

investigação;

- produzir, transmitir, retransmitir ou divulgar mensagem que:
  - ✓ contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da **DanPower**;
  - ✓ contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
  - ✓ contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - ✓ vise obter acesso não autorizado a outro computador, servidor ou rede;
  - ✓ vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  - ✓ vise burlar qualquer sistema de segurança;
  - ✓ vise vigiar secretamente ou assediar outro usuário;
  - ✓ vise acessar informações confidenciais sem explícita autorização do proprietário;
  - ✓ vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  - ✓ inclua imagens criptografadas ou de qualquer forma mascaradas;
  - ✓ tenha conteúdo considerado impróprio, obsceno ou ilegal;
  - ✓ seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico (em especial pornografia infantil) entre outros;
  - ✓ contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  - ✓ tenha fins políticos locais ou do país (propaganda política);
  - ✓ inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura padronizada divulgada pela empresa ou que tenha no mínimo o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico.

2.3 APLICATIVOS DE COMUNICAÇÃO/MENSAGERIA E APLICAÇÕES DE ÁUDIO/VIDEOCONFERÊNCIA

Atualmente, determinadas atividades corporativas utilizam aplicações de áudio/videoconferência e/ou aplicações mensageria para comunicação interna e externa.

O uso de tais aplicações, quando autorizada pelo gestor ou pela área de Segurança da Informação, deve ocorrer para fins exclusivamente corporativos e relacionados às atividades do colaborador/usuário dentro da empresa.

A utilização desse serviço **para fins pessoais é vedado**, ressalvadas eventuais exceções autorizadas pelo gestor da área, e desde que não prejudique a empresa e também não cause impacto no tráfego da rede.

Ao fazer uso de aplicativos de mensageria e/ou de áudio/videoconferência o colaborador deve sempre preservar o sigilo e a confidencialidade das informações, atendendo aos requisitos desta Política e respeitando a legislação vigente.

Aplicativos de mensageria devem contar, no mínimo, **com criptografia ponta a ponta (end-to-end encryption ou E2EE).**

Aplica-se ao uso uso de aplicativos de mensageria e/ou áudio/videoconferência as mesmas regras previstas para o uso de internet e de correio eletrônico naquilo que não for conflitante com o presente tópico.

2.4 APLICAÇÕES DE INTELIGÊNCIA ARTIFICIAL - AI

É proibido o uso pelos colaboradores da DanPower de tecnologias de Inteligência Artificial, AI Generativa e aplciações semelhantes, tais como, mas não exclusivamente, CHAT GPT, DALL-E e/ou outras, para uso profissional e/ou dentro das instalações da DanPower.

O uso de tais ferramentas no ambiente corporativo pode representar riscos, em especial, divulgação de informaçãoes sigilosas, quebra de segredo comercial e industrial entre outros. Informações e dados imputados em tais sistemas se tornam de domínio público e o processo é irreversível.

Portanto, fica proibido o uso das referidas tecnologias nos equipamentos e sistemas da DanPower, ressalvada autorização expressa em sentido contrário proveniente da área de Tecnologia da Informação ou da Direção da empresa.

2.5 IDENTIFICAÇÃO

Os sistemas que usam mecanismos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a DanPower e/ou terceiros.

O uso das da identificação e/ou senhas de outra pessoa pode, em tese, constituir crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos mecanismos de identificação e deverá ser aplicada a todos os colaboradores.

Salvo as exceções expressamente autorizadas, se existir login que esteja sendo compartilhado por mais de um colaborador, a responsabilidade perante a **DanPower** e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

A área de Tecnologia da informação é responsável pela criação da identidade lógica dos colaboradores na instituição.

2.6 SENHA

Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), em celulares ou outras aplicações eletrônicas que sejam compreensíveis por linguagem humana (não criptografados); Também não devem ser anotadas em cadernos, blocos de notas, rascunhos etc.

As senhas devem respeitar um padrão mínimo de segurança, sendo sugerido evitar senhas baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após tentativas sequenciais de acesso sem sucesso a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a área de Tecnologia da Informação da **DanPower**.

Os usuários tem o dever de vigilância com a própria senha e podem alterá-la a qualquer momento e sempre que entenderem necessário a fim de preservar a segurança da informação.

A periodicidade máxima para troca das senhas é 90 (noventa) dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato a área de Tecnologia da Informação, a fim de que essa providência seja tomada.

A mesma conduta se aplica aos usuários cujo contrato ou prestação de

serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar a troca à area de Tecnologia da Informação.

2.7 COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da **DanPower**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações provenientes da área de Tecnologia da Informação.

É **proibido** todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Tecnologia da Informação da **DanPower**, ou de quem este determinar.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá **imediatamente** acionar a área de Tecnologia da Informação.

Arquivos pessoais e/ou não pertinentes ao negócio do **DanPower** (fotos, músicas, vídeos etc) não deverão ser copiados, movidos, armazenados etc na rede corporativa, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem prévio aviso.

Documentos necessários para as atividades dos colaboradores da **DanPower** deverão ser salvos na rede da empresa, nas pastas correspondentes ao tipo de informação. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), **não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo,**

portanto, de responsabilidade do próprio usuário.

Os colaboradores da **DanPower** e/ou detentores de contas privilegiadas **não devem sem a prévia solicitação e a autorização da área de Tecnologia da Informação**:

- Instalar qualquer programa ou aplicação, seja no computador local, seja na rede;
- executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes no computador local ou na rede;
- executar nenhum tipo de comando ou programa que coloque em risco a segurança do computador e da própria rede;
- executar nenhum tipo de comando ou programa que venha a alterar qualquer tipo de configuração do computador e da própria rede.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os colaboradores devem informar imediatamente a área de Tecnologia da Informação a identificação de qualquer dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da área de Tecnologia da Informação ou por terceiros devidamente contratados para o serviço.
- O colaborador deve evitar o consumo de alimentos ou bebidas na mesa de trabalho próximo aos equipamentos.
- Deverão ser protegidos e bloqueados (senha) todos computadores quando não estiverem sendo utilizados (exemplo, bloquear a tela com senha ao se ausentar da mesa de trabalho).
- O colaborador deve fazer uso cuidadoso e zelar pelo bom estado geral dos equipamentos a que tiver acesso, a fim de evitar danos e contribuir com o

bom desempenho e vida útil.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da **DanPower**:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

2.8 DISPOSITIVOS MÓVEIS

O **DanPower** permite em determinadas circunstâncias e para facilitar a mobilidade e o fluxo de informação entre seus colaboradores o uso de dispositivos móveis, desde que seja para fins corporativos.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A **DanPower**, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador assume o compromisso de não utilizar, revelar ou divulgar

a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no **DanPower**, mesmo depois de terminado o vínculo contratual mantido com a instituição.

A **DanPower** poderá, quando julgar necessário, realizar cópia de segurança (backup) dos dados dos dispositivos movéis de uso corporativo.

Quando a aplicação do dispositivo móvel diponibilizar realização de backups automáticos, a mesma deve permanecer ativada a fim de resguardar as informações corporativas. Caso o colaborador tenha dúvida a respeito da ativação desta fucionalidade, deverá diligenciar junto a área de Tecnologia da Informação a fim de regularizar o equipamento.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da área de Tecnologia da Informação da **DanPower**.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela **DanPower**, notificar imediatamente seu gestor direto e a área de Tecnologia da Informação. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que no caso de uso indevido e/ou contrário à Política de Segurança da Informação e das presentes Normas de Segurança da Informação do dispositivo móvel, assumirá os riscos da sua má

utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **DanPower** e/ou a terceiros.

3. DISPOSIÇÕES FINAIS

Esta Política poderá ser revisada e modificada sempre que houver necessidade, devendo ser revisada ao menos a cada período de 2 (dois) anos contados da última atualização.

4. HISTÓRICO DE VERSÕES

Versão	Elaborado:	Revisão:	Aprovação:	Data Aprovação:	Histórico versão:
1	Daniel S. Salvador (jurídico)	Daniel S. Salvador (jurídico) Eduardo Oliveira (TI)	Aprovado	02/10/2023	

DanPower

Escaneie e
acesse o site:
www.danpower.com.br