POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este documento consiste na Política de Segurança da Informação – PSI da **DANCAL**, que deverá ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. No entanto destaca-se ainda que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da organização.

GLOSSÁRIO:

- Ativo: Algo que tenha valor para a organização.
- Evento: Acontecimento que acarrete mudança do estado atual de um processo.
- Incidente: Evento que traz prejuízos à organização.
- Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos.
- Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização.
- Malwares: O nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador.
- SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.
- Phishing: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamento para sites ou números de telefone, a fim de roubar sua identidade.

Sumário

1. Introdução

A informação é um ativo estratégico da **DANCAL**. Em reconhecimento a esse fato, a **DANCAL** estabeleceu Políticas e Diretrizes para sua segurança.

Para ser efetiva, a segurança da informação deve ser um esforço corporativo envolvendo o comprometimento de todos os empregados, clientes, prestadores de serviços e outros fornecedores da **DANCAL** que lidam com informações e/ou sistemas de informação. Esta política e suas diretrizes estabelecem as responsabilidades de todos os agentes envolvidos, gestores, guardas e usuários.

Este documento descreve a visão da empresa **DANCAL** para prevenir e reagir às várias ameaças incluindo, mas não se limitando a, acessos não autorizados, divulgação, duplicação, modificação, destruição, perda, uso indevido, ou roubo de informações da **DANCAL**.

Esta Política da Segurança da Informação e suas diretrizes aplicam-se a todos os processos que tratam a Informação ou Sistemas de Informação da **DANCAL** e foi formulada com base no Código de Prática Para a Gestão da Segurança da Informação, NBR ISO/IEC 27002, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

2. Objetivo da Política de Segurança da Informação

“A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados” (ABNT NBR ISO/IEC 27002).

A Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam

e/ou dificultem o processo do negócio, mas que garantam:

2.1 A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;

2.2 O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;

2.3 A participação e cumprimento por todos os colaboradores, em todo o processo.

3. Política de Segurança da Informação

A **DANCAL** considera a Informação um ativo estratégico para os seus negócios, razão pela qual estabelece que:

3.1 A utilização da Informação da empresa é restrita aos objetivos de seu negócio;

3.2 A responsabilidade pela segurança da Informação é de todos os empregados, fornecedores, clientes, contratados, inclusive aqueles afiliados a outras empresas que por força do negócio tenham acesso à Informação;

3.3 A prática permanente da Segurança da Informação tem de assegurar:

3.4 A confiabilidade, a integridade, a disponibilidade, a confidencialidade e a legalidade das informações;

3.5 O uso adequado da informação e os recursos disponibilizados.

4. Diretrizes

4.1 É compromisso da direção da **DANCAL** alocar recursos e investimentos necessários, compatíveis com suas estratégias de negócio, de forma a suportar projetos de Segurança da Informação.

4.2 Medidas devem ser tomadas para proteger os recursos da Informação contra divulgação acidental ou sem autorização, modificação ou destruição, como também assegurar a confiabilidade, integridade, disponibilidade e legalidade da Informação.

4.3 A gestão dos acessos aos recursos de Informação da **DANCAL**, conforme esta Política de Segurança da Informação será feita pela divisão de Tecnologia da Informação.

4.4 Informações sensitivas ou confidenciais devem ser protegidas contra alterações de seu conteúdo e de acessos não autorizados. Dados identificados como críticos aos negócios da **DANCAL** devem ser protegidos contra perdas ou destruição.

4.5 Os riscos aos recursos de Informação devem ser identificados, isolados e monitorados regularmente. O custo das medidas de prevenção e/ou correção deve ser compatível com o valor do ativo em questão.

4.6 Procedimentos de segurança devem ser adotados e cumpridos durante as fases de desenvolvimento ou aquisição de novos sistemas de Informação.

4.7 A divulgação e treinamento desta Política de Segurança da Informação devem ser continuamente praticados em todos os níveis e para todos os envolvidos.

4.8 As diretrizes desta Política de Segurança da Informação devem ser adaptáveis às vulnerabilidades e variáveis tecnológicas que possam afetar os recursos de Informação.

4.9 Esta política deverá estar formalizada nos acordos / contratos pactuados com quaisquer instituições ou empresas que acessem ou utilizem ou usarem a INFORMAÇÃO da **DANCAL**.

4.10 As empresas prestadoras de serviços que acessem ou utilizem os recursos de TI da **DANCAL** deverão no que lhes couber, obrigar-se contratualmente ao cumprimento da Política e Diretrizes desta política.

4.11 Todos os ativos de Tecnologia da Informação e Telecomunicações deverão estar identificados.

5. Orientações Complementares

5.1 Agentes e Responsabilidades

A responsabilidade pela Segurança da Informação da **DANCAL** é atribuída aos seguintes agentes e responsáveis:

Usuário

Será de inteira responsabilidade funcionários, terceirizados, prestadores de serviços e demais colaboradores da **DANCAL**:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da **DANCAL**;

- Buscar a área de Segurança da Informação ou Suporte Técnico da TI para esclarecimentos de dúvidas referentes à PSI;
- Proteger as informações contra acesso, divulgação, modificação ou destruição não autorizados pela **DANCAL**;
- Garantir que equipamentos e recursos tecnológicos à sua disposição, de propriedade da **DANCAL**, sejam utilizados apenas para as finalidades aprovadas pela empresa;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Comunicar prontamente ao gestor imediato qualquer violação a esta política, suas normas e procedimentos.

Gestores ou usuário aprovador

Em relação à segurança da Informação, cabe aos gestores e responsáveis das respectivas áreas:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho e prestação de serviços, à responsabilidade do cumprimento da PSI da **DANCAL**;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Elaborar, com o apoio do Setor de Gestão de Processos e Tecnologia da Informação, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários e colaboradores para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;
- Tomar as decisões administrativas referentes aos descumprimentos da PSI da **DANCAL**.

DPO (Encarregado de Dados)

Em relação à segurança da Informação e LGPD, cabe ao DPO:

- Aceitar reclamações e comunicações dos titulares dos dados pessoais, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;
- Informar e aconselhar o responsável pelo tratamento e os demais profissionais sobre suas obrigações nos termos da LGPD;
- Controlar a conformidade com a LGPD e com as políticas do responsável pelo tratamento, incluindo a atribuição de responsabilidades, a sensibilização e a formação do pessoal envolvido no tratamento;
- Prestar aconselhamento, se tal for solicitado, no que se refere à avaliação do impacto da proteção de dados pessoais e acompanhar o seu desempenho;
- Cooperar com as autoridades;
- Servir de ponte para a autoridade de supervisão em questões relacionadas

com o tratamento.

Gestor da Segurança da Informação

Cabe ao Gestor de Segurança da Informação:

- Criar e atualizar a PSI da organização;
- Propor melhorias, alterações e ajustes da PSI;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;
- Pesquisar e propor novas tecnologias na área de segurança da informação sempre que julgar necessário.

O gestor da Segurança da Informação poderá ainda ser auxiliado e amparado pelas seguintes áreas e departamentos da empresa:

- Representante da Governança;
- Setor de Gestão de Processos e Tecnologia da Informação;
- DPO (Encarregado de Dados);
- Unidade de Suporte de TI;
- Divisão de Gestão de Pessoas;
- Assessoria Jurídica;
- Suporte técnico em Tecnologia da Informação Cabe ao Setor de Suporte Técnico e infraestrutura:
    - Definir e aplicar as regras referente a instalação de software e hardware nos equipamentos utilizados para acessos a dados da

DANCAL;

- Homologar os equipamentos pessoais (smartphones, desktops e Notebook) para uso na rede da **DANCAL**;

- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;
- Mediante informações da área de RH, manter registro e controle atualizado de todas as liberações de acesso concedidas, providenciando sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações e acessos;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.;
- Analisar criticamente incidentes de segurança em conjunto com o Gestor de Segurança da Informação;
- Manter comunicação efetiva com o Gestor de Segurança da Informação sobre possíveis ameaças e novas medidas de segurança;
- Buscar alinhamento com as diretrizes da organização.

5.2 Classificação da Informação

As informações relativas ao escopo da Política e das Diretrizes de Segurança da Informação são classificadas e devem preferencialmente identificadas por rótulos, conforme as naturezas abaixo:

- Pública
- Interna

- Dados pessoais
- Confidencial
- Confidencial restrita Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.
São exemplos de informação pública:

- Informações sobre eventos não restritos ou externos;
- Informações disponibilizadas pela área de Marketing, em redes sociais e aquelas informadas de forma pública no site institucional da empresa.

Interna

São informações disponíveis aos colaboradores da **DANCAL** para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.
São exemplos de informações internas:

- Memorandos, Padrões, Políticas e Procedimentos internos;
- Avisos e campanhas internas;

Dados pessoais

São informação permitem identificar, direta ou indiretamente, um indivíduo, então ela é considerada um dado pessoal:
São exemplos de dados pessoais:

- Nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço

residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.

Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.
São exemplos de informações confidenciais:

- Informações técnicas ou contratos de clientes, prestadores de serviços e fornecedores;
- Informações de acesso e senhas de ambientes e sistemas de clientes;
- Informações sensíveis da área interna da TI da **DANCAL** ou de outros departamentos;
- Processos judiciais;
- Dados cadastrais de funcionários.

Confidencial restrita

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas ao presidente, gerentes e funcionários cujas funções requeiram conhecê-las.
São exemplos de informações confidenciais restritas:

- Atas de reunião da governança com a presidência da **DANCAL**;

- Indicadores e estatísticas dos processos de negócio considerados restritos;
- Resultado de auditorias internas considerados restritos.

5.3 Princípios de Segurança da Informação:

Confiabilidade: A Informação retrata a realidade dos fatos a que se refere.

Confidencialidade: A classificação dada à Informação de acordo com a estratégia e criticidade para os negócios da empresa.

Disponibilidade: É a garantia de que a Informação poderá ser acessada quando necessário. Integridade: A Informação é a mesma em qualquer meio ou instante para todos os usuários.

Legalidade: Obediência às leis de Propriedade Intelectual e Autoral e às condutas éticas em vigor no país.

5.4 Acessos

5.4.1 O login e a senha de cada usuário da **DANCAL** são únicos, individuais e intransferíveis, sendo reconhecidas pela **DANCAL** como assinatura digital do usuário e representando o nível de delegação concedida para o desempenho de suas funções.

5.4.2 Os acessos externos aos recursos da **DANCAL** (acesso remoto de funcionários, prestadores de serviço, fornecedores, clientes ou outros agentes) somente serão concedidos mediante autorização prévia realizados por intermédio de soluções técnicas corporativas ou formalizadas por alguma outra forma que seja previamente homologada pelo Gestor de Segurança ou área equivalente.

5.4.3 O acesso à Internet é permitido somente por intermédio do Sistema de Segurança corporativo da **DANCAL**. É proibido o acesso direto à Internet por intermédio de provedores que geram acessos anônimos, como a rede Tor.

5.4.4 O acesso físico a qualquer área de trabalho deve ser protegido, de acordo com o valor da Informação ali residente. Um sistema apropriado de controle de acesso quando necessário deverá ser estabelecido pela **DANCAL** e homologado pela divisão de Tecnologia da Informação. Todos os acessos às áreas restritas devem ser registrados.

5.5 Utilização

5.5.1 A utilização das informações e dos recursos computacionais deve ser sempre compatível com a confidencialidade e a finalidade das atividades desempenhadas pelo usuário na **DANCAL**.

5.5.2 A utilização dos recursos (sistemas, correio eletrônico, armazenamento em disco, etc.) disponibilizados pela **DANCAL** deve ser feita segundo os padrões e procedimentos definidos

5.5.3 pela divisão de Tecnologia da Informação, visando manter a disponibilidade, compliance e desempenho das aplicações.

5.6 Direito e Propriedade

5.6.1 Todos os programas e documentações geradas por, ou providenciadas por empregados, consultores ou contratados para o benefício da **DANCAL** são propriedades da **DANCAL**.

5.6.2 Todos os usuários devem utilizar somente softwares homologados e devidamente legalizados pela divisão de Tecnologia da Informação da **DANCAL**, visando atender a Lei nº 9609 de 19/02/98, que trata dos direitos autorais e comercialização de softwares.

5.6.3 Todos os contratos com terceiros devem conter cláusulas de sigilo e proteção à propriedade intelectual;

5.7 Contingência

5.7.1 Para enfrentar situações de interrupção dos sistemas de informação, com consequente paralisação das atividades de negócio da **DANCAL**, a divisão de Tecnologia da Informação deverá manter um plano de contingência para os sistemas e recursos críticos que seja de sua responsabilidade, que garanta um nível mínimo de operação.

5.8 Legalidade

5.8.1 O uso de software não autorizado é crime previsto na Lei 9.609, de 19 de fevereiro de 1998. A não observância desta lei será considerada pela **DANCAL** como sendo falta grave, passível de sanções cabíveis.

5.9 Proteção

5.9.1 A **DANCAL** deverá manter dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais etc.) e lógica (vírus, acesso não autorizado etc.), compatíveis com os requisitos definidos nesta política.

5.9.2 Competirá à divisão de Tecnologia da Informação a definição de tais dispositivos de proteção, considerando as características regionais, a criticidade das informações e os recursos tecnológicos envolvidos.

5.10 Gerenciamento

5.10.1 As instruções específicas para a operacionalização desta Política de Segurança e utilização da Tecnologia da Informação da **DANCAL**, serão emitidas pela divisão de Tecnologia da Informação, devendo a mesma estar em conformidade com esta Política de Segurança da Informação.

5.10.2 Toda documentação e registro referente à Segurança da Informação deverá ser arquivada em local seguro para efeito de auditoria.

5.10.3 Todos os processos de gestão relativos à geração de produtos e serviços de TI deverão atender aos requisitos deste manual.

5.11 Auditoria

5.10.4 O diretor de Tecnologia da **DANCAL** terá acesso, sempre que julgar necessário, ao conteúdo das mensagens de correio e dos arquivos armazenados, bem como de todas as informações de que trata esta política, exceto às informações de cunho privado de empregado.

5.10.5 O diretor de Tecnologia da **DANCAL** somente poderá ter acesso às informações de que trata o item anterior por meio de solicitação formal à divisão de Tecnologia da Informação, à gerência de Gestão de Pessoas (HR) ou ao

diretor presidente da **DANCAL**.

6. Monitoramento de Ambiente e Sistemas

Para garantir as regras mencionadas nesta PSI, a **DANCAL** poderá:

6.1 Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede e sistemas. A informação gerada por esses sistemas de monitoramento poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

6.2 Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

6.3 Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

7. Computadores e recursos tecnológicos

Os equipamentos disponíveis aos colaboradores e funcionários são de propriedade da **DANCAL**, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um analista de TI da **DANCAL**, ou de quem este determinar.

Os gestores que necessitarem fazer testes deverão solicitá-los previamente ao Setor de TI, ficando responsáveis jurídica e tecnicamente pelas ações

realizadas.

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 acionar o setor técnico responsável mediante registro de chamado no service desk (CRM) da **DANCAL**.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede ou no site do Sharepoint.

Os colaboradores da **DANCAL** ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de TI da **DANCAL**.

No uso dos computadores, equipamentos e recursos de TI, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de Sistema Operacional para restringir o acesso de colaboradores não autorizados;
- Os colaboradores devem informar ao departamento técnico da TI qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de TI de propriedade da **DANCAL** para qualquer tipo de reparo que não seja realizado por um analista da área de TI da empresa ou por terceiros devidamente

contratados para o serviço;

- O colaborador deverá manter a configuração do equipamento disponibilizado pela **DANCAL**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e sistemas quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela **DANCAL** devem ter imediatamente suas senhas padrões (default)alteradas;

Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da **DANCAL**.

- 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;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- 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.

8. Política de senhas

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

8.1 A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo essa ser imediatamente alterada no caso de suspeita de sua divulgação;

8.2 A senha inicial só será fornecida ao próprio colaborador, pessoalmente ou por algum outro meio que a área de TI julgue como confiável ou aceitável;

8.3 É proibido o compartilhamento de login para funções de administração de sistemas;

8.4 As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);

8.5 As senhas deverão seguir os seguintes pré-requisitos:

- Tamanho mínimo de oito caracteres;
- Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;
- Não devem ser baseadas em informações pessoais de fácil dedução

(aniversário, nome do cônjuge etc.).

- O uso do MFA (Autenticação Multifator) poderá ser obrigatório no procedimento de login de sistemas internos da empresa e deverá ser configurado e utilizado sempre que solicitado pelo sistema.

8.6 O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações:

- Desligamento do colaborador;
- Mudança de função do colaborador;
- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

8.7 Para os cancelamentos acima mencionados, a área de Gestão de Pessoas (HR) da **DANCAL** é a responsável por informar prontamente a área de TI acerca dos desligamentos e mudança de função dos colaboradores.

9. E-MAIL e Ferramentas de Colaboração

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

9.1 O e-mail corporativo e as ferramentas de colaboração e produtividade (Ex: Sharepoint e Microsoft Teams) são destinados a fins profissionais, relacionados às atividades dos colaboradores;

9.2 Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

9.3 É proibido enviar, com endereço eletrônico corporativo, mensagens com

anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;

9.4 É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

9.5 É proibido enviar qualquer mensagem por meios eletrônicos que torne a **DANCAL** vulnerável a ações civis ou criminais;

9.6 É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

9.7 Produzir, armazenar, transmitir ou divulgar mensagem que:

- Contenha ameaças eletrônicas, como: spam, phishing, vírus, malwares ou equivalentes;
- Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .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;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Inclua material protegido por direitos autorais sem a permissão do

detentor dos direitos.

9.8 Transmitir ou divulgar dados pessoais sem prévio consentimento ou autorização do respectivo titular;

9.9 O uso de e-mails pessoais dentro da **DANCAL** é aceitável, se usado com moderação, em caso de necessidade e quando:

- Não contrariar as normas aqui estabelecidas;
- Não interferir, negativamente, nas atividades profissionais individuais ou na produtividade de outros colaboradores;

EMPRESA

10. Uso das estações de trabalho

As estações de trabalho (sejam desktops ou notebooks) devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas.
Assim, algumas medidas de segurança devem ser tomadas, são elas:

10.1 É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;

10.2 Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

10.3 É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe de suporte da TI;

10.4 É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe de TI da **DANCAL**;

10.5 As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de maior ausência do colaborador;

10.6 Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede ou Sharepoint corporativo, os quais possuem controle de acesso adequado;

10.7 Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede ou Sharepoint corporativo, nunca unicamente no disco local da máquina;

10.8 É proibido o uso de estações de trabalho para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- 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.

10.9 O suporte de TI da **DANCAL** não se responsabiliza por prestar manutenção de hardware ou instalar softwares, mesmo que sejam para execução das atividades da empresa, em computadores que não sejam de propriedade da **DANCAL**, porém este poderá prestar o devido suporte e auxílio para que o

seu proprietário possa fazê-lo;

10.10 As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

11. Uso de equipamento particular e dispositivos móveis

O objetivo da **DANCAL** é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores e prestadores de serviços, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da **DANCAL** ou particular com prévia aprovação e permissão da área responsável da TI ou equivalente, como: notebooks e smartphones

Todas as regras do tópico “Estações de Trabalho” se enquadram nesta seção, adicionalmente a:

11.1 Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna da **DANCAL** mediante autorização do gestor imediato ou liberação da área de TI;

11.2 A área de TI da **DANCAL** poderá verificar as configurações de segurança do equipamento pessoal do colaborador, seja de forma manual ou automatizada através de sistema de gestão de dispositivos, para certificar-se que o equipamento possui aplicativos e recursos de segurança, como firewall, antivírus e anti-malware devidamente habilitados, configurados e atualizados, antes de permitir o acesso aos recursos e dados da **DANCAL**. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar

carga excessiva na rede, que não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem **DANCAL** não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;

11.3 É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos pessoais ou corporativos da **DANCAL** a serem utilizados em seus equipamentos;

11.4 É de responsabilidade do proprietário o controle sobre os aplicativos instalados em seu notebook;

11.5 Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede da **DANCAL**, acesso a informações sem a devida permissão ou informações confidenciais;

11.6 É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam à **DANCAL** não podem ser armazenados no disco rígido do notebook pessoal ou em dispositivos de armazenamento móvel (ex: pendrive), sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento destinado para tal, Sharepoint da organização ou em área de armazenamento autorizada pela área responsável da **DANCAL**;

11.7 Maiores detalhes sobre esse tópico poderão também ser encontrados no documento “TI - REV X.0 - Segurança da Informação - BYOD - Traga o seu próprio dispositivo”.

12. Backup

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma

organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer. Assim, estabelecem-se as regras:

12.1 Todo sistema ou informação relevante para a operação dos negócios da **DANCAL** deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;

12.2 As áreas de negócio ficarão responsáveis por classificar os dados de acordo com a relevância e provocar a área de TI sobre a necessidade de backup deles, sugerindo o tempo de retenção destas cópias;

12.3 Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

12.4 Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

12.5 A área de TI deve preparar semestralmente um plano para execução de testes de restauração de dados dos sistemas mais críticos da **DANCAL**, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;

12.6 Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade.

13. Restrições gerais

13.1 Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos ou estratégias de bypass de firewall;

13.2 É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;

13.3 O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pela **DANCAL** sem aviso prévio ou consentimento do usuário;

13.4 Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

13.5 Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

13.6 Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando área de TI da **DANCAL** deverá estar devidamente ciente e concedido autorização para tal;

13.7 É proibido o envio de informações restritas ou confidencias da **DANCAL** para destinatários que não sejam autorizados pela gestão da **DANCAL** a recebê-los.

14. Violação da Política e Penalidades

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário, prestador de serviço ou colaborador poderá sofrer as seguintes penalidades:

Advertência verbal
O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da **DANCAL** e será recomendado à leitura desta Norma;

Advertência formal
A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida.

A segunda notificação será encaminhada para o gestor imediato do infrator.

15. Considerações Finais

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas aos responsáveis pela área de Governança e Segurança da Informação para avaliação e decisão.

Esta PSI entra em vigor a partir da data de sua publicação e poderá ser alterada a qualquer momento, por decisão da área responsável por esse documento, mediante o surgimento de fatos relevantes que apareçam ou que não tenham sido contemplados nessa política.

Informações complementares sobre Segurança da Informação poderão também são

encontradas no documento “TI - REV X.0 - Segurança da Informação - Política de Mesa Limpa e Home Office”.

Diretrizes mais específicas no que tange ao tratamento de dados pessoais deverão ser consultadas através do documento da **DANCAL** que aborda a LGPD (Lei Geral de Proteção de Dados).