Política de Segurança da Informação

1. INTRODUÇÃO

A Política de Segurança da Informação (PSI), é o documento que orienta e estabelece as diretrizes corporativas do Grupo Dahruj para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da organização.

Para o Grupo Dahruj, a informação é um ativo muito importante para o crescimento sustentável do negócio e deve ser adequadamente manuseada e protegida por todos os colaboradores, por meio da presente PSI.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2013, reconhecida mundialmente como um código de prática para gestão da segurança da informação, bem como está de acordo com a legislação vigente em território nacional.

A norma ABNT NBR ISO/IEC 27001:2013 recomenda que a política de segurança da informação deve ser definida, aprovado pela Direção, publicada e comunicada aos funcionários e partes externas relevantes.

O Grupo Dahruj compreende que as questões relacionadas à segurança da informação devem ser tratadas como tema sensível e de suma importância, por isso a criação de uma cultura de segurança da informação se mostra tão importante.

2. OBJETIVO

Esta Política de Segurança da Informação objetiva estabelecer diretrizes que permitam aos colaboradores, clientes e demais interessados seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa.

Esta PSI tem o intuito de nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. O propósito do PSI é preservar as informações do Grupo Dahruj quanto à:

▪ **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

▪ **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

▪ **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Ainda, esta PSI tem como finalidade:

▪ Declarar, formalmente, o comprometimento da direção do Grupo Dahruj na proteção de seus ativos tangíveis e intangíveis, de acordo com as necessidades de negócio e em conformidade legal;

▪ Definir as melhores práticas, padrões e recomendações de uso aplicáveis aos ativos do Grupo Dahruj por meio de regras e diretrizes, resguardando a Segurança das Informações da organização;

▪ Estabelecer as responsabilidades e limites de atuação dos colaboradores do Grupo Dahruj em relação à segurança da informação, reforçando a cultura interna e priorizando as ações necessárias conforme o negócio.

3. RESPONSABILIDADE

DIREÇÃO E SÓCIO GERENTE DE TECNOLOGIA DA INFORMAÇÃO:

(i) Analisar, aprovar e declarar formalmente o seu comprometimento com esta PSI.

GRUPO PARA TRATAR SOBRE SEGURANÇA DA INFORMAÇÃO (GRUPO):

(i) Analisar e aprovar esta PSI e eventuais documentos complementares;

(ii) Cumprir e fazer cumprir esta PSI e eventuais documentos complementares por todos os colaboradores do Grupo Dahruj;

(iii) Garantir que o Grupo seja composto por uma equipe multidisciplinar, tenha atuação permanente e reuniões semestrais;

(iv) Promover e realizar a gestão da Segurança da Informação, garantindo a implementação de controles, modelos, padrões e recursos necessários para a proteção da informação;

(v) Orientar para que as atividades desempenhadas pela Segurança da Informação/Suporte Técnico estejam adequadas aos objetivos do negócio do Grupo Dahruj;

(vi) Aprovar os investimentos em segurança da informação do Grupo Dahruj, considerando a viabilidade e os impactos de sua aplicação à qualidade dos processos de negócio;

(vii) Analisar e aprovar, ou não, os pedidos de exceções a esta PSI;

(viii) Analisar procedimento disciplinar para apuração de responsabilidades dos envolvidos em Incidente de Segurança da Informação e aplicar as penalidades, quando necessário.

SETORES DE INFORMÁTICA E F&I:

Nomear um responsável pela Segurança da Informação e comunicar a todos os colaboradores do Grupo Dahruj;

(i) Manter esta PSI atualizada e submetê-la para aprovação do Grupo;

(ii) Elaborar e manter atualizado os documentos de Segurança da Informação;

(iii) Avaliar a utilização dos dispositivos móveis particulares, conforme as necessidades dos negócios do Grupo Dahruj;

(iv) Homologar os repositórios digitais e os dispositivos removíveis de armazenamento de informações para serem utilizados pelos colaboradores do Grupo Dahruj de acordo com a necessidade para o negócio e os documentos de Segurança da Informação;

(v) Avaliar, autorizar, ou não, fundamentar e formalizar as exceções a esta PSI;

(vi) Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias;

(vii) Apoiar para que os procedimentos de gestão da Continuidade de Negócios sejam executados em conformidade com os requisitos de segurança da informação;

(viii) Auxiliar nos processos de aquisição, manutenção ou desenvolvimento de softwares com relação aos requisitos de segurança da informação e controles de acesso;

(ix) Definir, analisar e priorizar ações necessárias, balanceando custo x benefício;

(x) Realizar campanhas de capacitação e divulgação da segurança da informação, com o auxílio dos demais setores internos da empresa e, se necessário, terceiros;

(xi) Receber, analisar e tratar os incidentes de segurança da informação reportados e submeter relatório para deliberação do Grupo, sempre que necessário.

SETORES DE INFORMÁTICA E F&I:

(i) Realizar a gestão e manutenção dos Recursos de Tecnologia da Informação e Comunicação de propriedade do Grupo Dahruj ou que estão sob sua responsabilidade;

(ii) Garantir que todos os Recursos de Tecnologia da Informação e Comunicação utilizados pelo Grupo Dahruj atendam às recomendações de seus desenvolvedores;

(iii) Realizar e manter atualizado o inventário de hardwares e softwares do Grupo Dahruj;

(iv) Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico do Grupo Dahruj;

(v) Realizar o registro e o monitoramento dos acessos aos ambientes lógicos do Grupo Dahruj;

(vi) Garantir que todos os ativos do Grupo Dahruj sob sua responsabilidade atendam as recomendações de seus fabricantes;

(vii) Realizar o registro e o monitoramento dos acessos aos ambientes físicos do Grupo Dahruj;

(viii) Estabelecer perímetros de segurança para proteção de ativos tangíveis do Grupo Dahruj e implementar controles necessários;

(ix) Autorizar, ou não, o uso de obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro de propriedade do Grupo Dahruj;

(x) Elaborar e manter procedimentos de salvaguarda das informações e dos dados necessários para recuperação dos sistemas do Grupo Dahruj.

SETORES DE RECURSOS HUMANOS, FINANCEIRO E CONTÁBIL:

(i) Disponibilizar esta PSI e eventuais documentos complementares do Grupo Dahruj, além de custodiar e colher assinatura no “Termo de Ciência e Responsabilidade” na admissão de novos colaboradores;

(ii) Estipular controles de segurança especificamente relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores.

ESCRITÓRIO DE ADVOCACIA (EXTERNO):

(i) Validar, previamente, as minutas de contratos de trabalho e de prestação de serviços, a fim de atender aos controles de segurança da informação aplicáveis.

GESTOR RESPONSÁVEL PELO COLABORADOR:

(i) Garantir e gerenciar o cumprimento desta PSI e demais documentos complementares pelos seus colaboradores;

(ii) Identificar e medir as vulnerabilidades e ameaças nos processos e atividades de sua responsabilidade, as quais devem ser tratadas diligentemente de modo a reduzir os impactos ao negócio;

(iii) Garantir que os ativos de propriedade ou sob responsabilidade do Grupo Dahruj sejam utilizados com cuidado e de acordo com as orientações do fabricante e da empresa;

(iv) Identificar incidentes de segurança da informação ou qualquer ação duvidosa praticada por seus colaboradores, comunicando o Segurança da Informação/Suporte Técnico, pelo e-mail seginfo@grupodahruj.com.br (sugestão para criação deste e-mail), imediatamente.

(i) Estar ciente de manter-se atualizado com esta PSI e eventuais documentos complementares;

(ii) Conhecer e assinar o termo de confidencialidade;

(iii) Utilizar os ativos de propriedade do Grupo Dahruj ou sob sua responsabilidade de acordo com as orientações do fabricante, do desenvolvedor e da empresa, com cuidado e zelo;

(iv) Utilizar os ativos e informações do Grupo Dahruj somente para fins profissionais e de forma ética e legal, respeitando os direitos e as permissões de uso concedidas;

(v) Preservar a integridade, a disponibilidade, a confidencialidade, a autenticidade, a privacidade e a legalidade das informações acessadas ou manipuladas;

(vi) Zelar pela segurança da sua integridade digital, não compartilhando, divulgando, excluindo ou transferindo a terceiros quaisquer de seus componentes;

(vii) Cumprir com a legislação nacional vigente e demais instrumentos regulamentares relacionados às atividades profissionais;

(viii) Reportar quaisquer incidentes, formalmente, ao Segurança da Informação/Suporte Técnico, pelo e-mail seginfo@grupodahruj.com.br (sugestão para criação deste e-mail).

4. APLICAÇÃO DESTA POLÍTICA

Esta PSI é um documento interno, com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, junto aos colaboradores do Grupo Dahruj. Em outras palavras, aplica-se a todos os colaboradores desde o momento de sua publicação.

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa, poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientações sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte das informações.

5. PRINCÍPIOS DESTA POLÍTICA

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo Grupo Dahruj pertence à organização. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das suas atividades profissionais. O uso pessoal dos recursos é permitido, desde que não prejudique o desemprenho dos sistemas e serviços.

O Grupo Dahruj poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Assim, são princípios desta PSI:

▪ Preservar e proteger as informações do Grupo Dahruj e os Recursos de Tecnologia da Informação e Comunicação que as contêm, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte e formato;

▪ Prevenir e reduzir impactos gerados por incidentes de segurança da informação, assegurando a confidencialidade, integridade, disponibilidade, autenticidade, privacidade e legalidade no desenvolvimento das atividades profissionais;

▪ Zelar por relações profissionais transparentes e éticas de seus colaboradores.

6. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

Para esta PSI e seus documentos complementares, as atividades que porventura não forem tratadas nos normativos, só deverão ser realizadas após

prévia e formal autorização do responsável pela área, de acordo com a criticidade para o negócio. É o que se chama de **interpretação restritiva da PSI.**

Esta PSI e seus documentos complementares devem ser divulgados a todos os colaboradores do Grupo Dahruj.

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pelos colaboradores, bem como os demais ativos tangíveis e intangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo do Grupo Dahruj, devendo ser empregadas unicamente para fins profissionais.

A utilização de obras intelectuais, softwares, marcas, identidade visual ou qualquer outro sinal distintivo atual ou futuro de propriedade da Marrcovel em qualquer suporte, inclusive na internet e mídias sociais, deve ser vinculada as atividades profissionais ou ser formal e previamente autorizada pelo responsável da área.

É vedada a revelação de qualquer informação de propriedade ou sob responsabilidade do Grupo Dahruj, excetuando-se a hipótese de que a informação seja pública ou quando for expressamente autorizada.

Os ativos de propriedade ou sob a responsabilidade do Grupo Dahruj devem ser utilizados somente para fins profissionais e autorizados pelo responsável da área.

A gestão dos ativos no Grupo Dahruj deve atender as recomendações dos fabricantes ou desenvolvedores, sendo que qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente pode ser realizada pela área específica do Grupo Dahruj, de acordo com o tipo de ativo.

O setor de Informática, deve realizar inventário de hardwares e softwares do Grupo Dahruj, além de ser o responsável pelo seu registro, armazenamento e atualização.

Os recursos de Tecnologia da Informação e Comunicação de propriedade ou sob a responsabilidade do Grupo Dahruj devem ser utilizados apenas para fins profissionais, de modo lícito, ético e moral.

Os dispositivos móveis devem ser utilizados quando fornecidos pela organização, conforme as necessidades do negócio.

Quanto aos dispositivos móveis particulares, somente é permitido quando prévia e expressamente autorizado pelo responsável pela área e avaliado pelo Setor de Informática.

Somente é permitido o uso de aplicativos de comunicação instantânea homologados pelo Setor de Informática/Suporte Técnico para troca de informações corporativas. No uso desses aplicativos, o colaborador deve sempre

respeitar a legislação vigente, a criticidade da informação, a marca, a imagem e a reputação do Grupo Dahruj.

Somente é permitido aos colaboradores o uso de repositórios digitais homologados pelo Setor de Informática/Suporte Técnico para armazenar ou transmitir informações de propriedade ou sob a responsabilidade do Grupo Dahruj.

A publicação ou menção de quaisquer informações em nome ou relacionado ao Grupo Dahruj nas mídias sociais, deve ocorrer somente por colaboradores ou pessoas autorizadas em razão da atividade profissional com a empresa.

No caso de utilização do nome do Grupo Dahruj nas mídias sociais, o colaborador deve ser cauteloso, ético e seguro em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contratos e intimidades, além do dever de preservar o sigilo profissional nas mídias sociais.

É vedada qualquer atividade relacionada a gravação de áudio, vídeo ou foto dentro das dependências do Grupo Dahruj por seus colaboradores, sem a prévia e formal autorização da Diretoria, exceto quando realizado em razão das atividades profissionais ou contratadas pelo Grupo Dahruj.

Os sistemas e recursos de Tecnologia da Informação e Comunicação que suportam os processos e as informações do Grupo Dahruj devem ser confiáveis, íntegros, seguros e disponíveis a quem deles necessitem para execução de suas atividades profissionais.

Para garantir essa segurança, a organização deve contar com sistemas de proteção, sempre ativos e atualizados:

▪ Contra programas maliciosos e acesso indevidos, como antivírus e firewall;

▪ Para indicar tentativas de intrusão realizada aos ambientes lógicos, como Sistemas de Detecção a Intrusão (Intrusion Detection System) ou IPS (Intrusion Protection Systems);

▪ Contra mensagens eletrônicas indesejadas ou não autorizadas, como AntiSpam.

O Setor de Informática deve estabelecer perímetros de segurança para proteção de seus ativos tangíveis, além de:

▪ Implementar controles de acesso aos ambientes físicos, constando data, hora e área onde será realizado o acesso;

▪ Manter portas, janelas, gavetas e armários trancados;

▪ Implementar segurança patrimonial, câmeras, alarmes e fechaduras;

▪ Garantir que instalações críticas sejam localizadas de modo mais restrito.

O desenvolvimento interno e/ou aquisição externo de softwares, assim como a sua aquisição no mercado, devem garantir o cumprimento dos requisitos de segurança da informação e controles de acesso, além de serem realizadas somente pelo Setor de Informática.

O Setor de Informática deve definir e manter um processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (backup), a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes, ou sua recuperação o mais rápido possível.

O andamento e o resultado de uma mudança que impactar a Segurança da Informação, deve preservar os controles relacionados a disponibilidade, integridade, sigilo, autenticidade das informações e realizados somente após aprovação do Responsável pela Segurança da Informação.

Os Gestores de Áreas e Departamentos do Grupo Dahruj, devem analisar seus processos e ativos em intervalos regulares (semestralmente), zelando para que estejam devidamente inventariados e com os seus gestores identificados e cientes, assim como suas vulnerabilidades e ameaças de segurança mapeadas.

O Setor de Informática deve identificar e avaliar os riscos relacionados à Segurança da Informação e adotar as melhores práticas para o seu gerenciamento.

Os procedimentos de gestão da Continuidade de Negócios devem ser executados em conformidade com os requisitos de Segurança da Informação a partir do apoio do Segurança da Informação/Suporte Técnico para garantir a proteção das informações e dos ativos críticos do Grupo Dahruj.

O Grupo Dahruj deve garantir que as contratações em que ocorra o compartilhamento de informações de propriedade ou sob a responsabilidade do Grupo Dahruj ou a concessão de acesso aos seus ambientes ou ativos, sejam precedidas por termos de confidencialidade e cláusulas contratuais relacionadas à Segurança da Informação.

O Grupo Dahruj deve contar com um Grupo responsável por assessorar e gerenciar a implementação dos controles de Segurança da Informação que serão estabelecidos, analisar questões específicas ao tema e auxiliar com a melhoria constante dos padrões e observância desta PSI.

Este Grupo deve ser composto por uma equipe multidisciplinar e será de atuação permanente, reunindo-se no início de cada semestre para tratar das pautas relacionadas à Segurança da Informação.

O Grupo Dahruj possui um canal de comunicação divulgado aos seus colaboradores para reportar imediatamente os possíveis casos de incidentes de segurança da informação (dpo@grupodahruj.com.br).

Eventuais dúvidas sobre esta PSI poderão ser encaminhadas ao Setor de Informática por meio do endereço eletrônico: seginfo@grupodahruj.com.br (sugestão para criação deste e-mail).

Os ambientes físicos e lógicos do Grupo Dahruj são monitorados visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes de segurança da informação.

Os Recursos de Tecnologia da Informação e Comunicação que estiverem nas dependências do Grupo Dahruj ou que interajam com seus ambientes, podem ser auditados ou inspecionados sempre que necessário, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade de seus proprietários ou portadores.

Os investimentos em segurança da informação devem ser estudados e deliberados no Grupo, considerando a viabilidade dos investimentos (custo x benefício) e os impactos de sua aplicação à qualidade dos processos de negócio.

O Grupo deve estabelecer um plano anual de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos colaboradores componentes do Segurança da Informação/Suporte Técnico.

O Setor de Informática deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares sempre que se fizer necessário, após os encontros semestrais do Grupo, visando à garantia que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados. No caso de ocorrerem mudanças nesta PSI e seus documentos complementares, todos os colaboradores devem ser devidamente comunicados.

As exceções que ocorram de forma exclusiva e excepcional a essa PSI e demais documentos complementares devem ser formalizados e fundamentados pelos Gestores das Áreas Solicitantes, analisadas pelo Segurança da Informação/Suporte Técnico e aprovadas pelo Grupo, que poderá a qualquer tempo revogá-las.

Os pedidos devem ser encaminhados por escrito, através do e-mail seginfo@grupodahruj.com.br (sugestão para criação deste e-mail) e serão remetidos ao Setor de Informática para análise de viabilidade. Se necessário, o pedido de exceção será submetido ao Grupo para aprovação ou denegação.

Os incidentes de segurança da informação identificados devem ser avaliados pelo Setor de Informática que, ao constatar uma violação, deve encaminhar o relatório para o Grupo, que após análise, poderá apurar as responsabilidades dos envolvidos em procedimento disciplinar, visando aplicação de sanções cabíveis previstas em cláusulas contratuais e na legislação vigente.

As tentativas de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada com uma violação.

7. DISPOSIÇÕES FINAIS

Esta PSI deve ser lida e interpretada sob a égide das leis brasileiras, no idioma português, em conjunto com eventuais documentos aplicáveis pelo Grupo Dahruj.

Esta PSI e eventuais documentos complementares encontram-se disponíveis na rede interna do Grupo Dahruj e podem ser solicitados para o Setor de Informática, através do e-mail: seginfo@grupodahruj.com.br (sugestão para criação deste e-mail).

Esta PSI entra em vigor na data de sua publicação e comunicação a todos os colaboradores do Grupo Dahruj.

8. DEFINIÇÕES

AMEAÇA: causa potencial de um incidente indesejado, que pode resultar dano ao Grupo Dahruj;

APLICATIVOS DE COMUNICAÇÃO INSTANTÂNEA: conjunto de código e instruções compiladas, executadas ou interpretadas por um Recurso de Tecnologia da Informação ou Comunicação, hospedadas em um dispositivo ou, na nuvem, usado para troca rápida de mensagens, conteúdo e informações multimídia;

ATIVO: qualquer coisa que tenha valor ao Grupo Dahruj e precisa ser adequadamente protegido;

ATIVO INTANGÍVEL: todo elemento que possui valor para o Grupo Dahruj e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível;

AUTENTICIDADE: garantia de que a informação é procedente, fidedigna, sendo capaz de gerar evidências e não repudiáveis da identificação de quem a criou, editou ou emitiu;

BACKUP OU SALVAGUARDA: salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de recuperação em casa de incidente ou necessidade de restauração, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada do Grupo Dahruj.

COLABORADOR: empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venha a ter relacionamento profissional, direta ou indiretamente, com o Grupo Dahruj.

CONFIDENCIALIDADE: garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidos do conhecimento alheio.

DISPONIBILIDADE: garantia de que as informações e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário e mediante a devida autorização para o seu acesso ou uso.

DISPOSITIVOS MÓVEIS: equipamentos de pequena dimensão e facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a internet e outros sistemas, redes ou qualquer dispositivo.

DISPOSITIVOS REMOVÍVEIS DE ARMAZENAMENTO DE INFORMAÇÃO: dispositivos capazes de armazenar informações que pode ser removido do equipamento, possibilitando a portabilidade dos dados, tais como CD, DVD, pen drive, etc.

IDENTIDADE DIGITAL: é a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token, biometria, etc.

INFORMAÇÃO: é o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

LEGALIDADE: garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposição do ordenamento jurídico vigente.

RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (RECURSOS DE TIC): hardware, software, serviços de conexão e comunicação ou de infraestrutura física necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações.

REPOSITÓRIOS DIGITAIS: plataformas de armazenamento na internet, a exemplo, mas não se limitando ao Google Drive, OneDrive, Dropbox, iCloud, etc.

RISCO: combinação de probabilidade de concretização de uma ameaça e seus potenciais impactos.

SEGURANÇA DA INFORMAÇÃO: é a preservação da confidencialidade, integridade, disponibilidade, legalidade, privacidade e autenticidade da informação. Visa proteger a informação dos diversos tipos de ameaças para

garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e de novas oportunidade de transação.

TENTATIVA DE BURLA: fazer esforços para não respeitar ou tentar violar as diretrizes estabelecidas nos normativos do Grupo Dahruj.

VIOLAÇÃO: qualquer atividade que desrespeite as regras estabelecidas nos normativos do Grupo Dahruj.

9. RECOMENDAÇÕES

Com base na ABNT NBR ISO/IEC 27001:2013, recomenda-se que a PSI seja apoiada por políticas específicas, listadas abaixo, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

• Informação documentada:
Recomenda-se que a organização possua informação documentada para todos os requisitos da norma ISO 27001 e para qualquer requisito determinado pela própria organização, inclusive políticas específicas.

• Controle de acesso:
Recomenda-se que a política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e do negócio.

• Classificação e tratamento da informação:

Recomenda-se que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

• Segurança física e do ambiente:

Recomenda-se que perímetro de segurança sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas e sensíveis.

• Tópicos orientados aos usuários:

o Uso aceitável dos ativos;
Recomenda-se que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação sejam identificadas, documentadas e implementadas.

o Mesa limpa e tela limpa;
Recomenda-se que adotem uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

o Transferência de informações;
Recomenda-se que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recurso de comunicação.

o Dispositivos móveis;
Recomenda-se que uma política e medida que apoiam a segurança da informação sejam adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.
Recomenta-se que a política para uso de dispositivo móveis considere:

- Registro dos dispositivos móveis;
- Requisitos para a proteção física;
- Restrições quanto a instalação de software;
- Requisitos para versões de software e aplicações de patches;
- Restrições para conexão aos serviços de informação;
- Controle de acesso;
- Técnicas de criptográficas;
- Proteção contra malware;
- Desativação, bloqueio e exclusão de forma remota;
- Backups;
- Uso dos serviços web e aplicações web.

o Restrições sobre o uso e instalações de software;

Recomenda-se que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelo usuário.

• Backup:

Recomenda-se que cópias de segurança das informações, dos softwares e das imagens do sistema sejam efetuadas e testadas regularmente conforme política de geração de cópias de segurança definida. O plano de backup, recomenda-se ainda, que os seguintes itens sejam levados em consideração:

o Registro completo e exato das cópias de segurança e documentação apropriada sobre os procedimentos de restauração;
o Abrangência (por exemplo, completa ou diferencial) e a frequência de geração das cópias de segurança reflitam os requisitos de negócio da organização;
o Estratégia 3 cópias de segurança, 2 tipos de mídias para armazenamento, 1 Cópia de segurança sejam armazenadas em localidades remotas, a uma distância suficiente para escapar dos danos de um desastre no local principal.

• **Contra malware:**

Recomenda-se que sejam implementados controles para detecção, prevenção e recuperação para proteger contra malware, combinando com um adequando programa de conscientização do usuário.

• **Gerenciamento de vulnerabilidades técnicas:**

Recomenda-se que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso sejam obtidas em tempo hábil; convém que a exposição da organização a estas vulnerabilidades sejam avaliadas e que sejam tomadas as medidas apropriadas para lidar com os riscos associados.

• **Controle criptográficos:**
Recomenda-se que sejam desenvolvidas e implementada uma política sobre o uso de controles criptográficos para a proteção da informação.

• **Segurança nas comunicações:**
Recomenda-se que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
Recomenda-se ainda, que mecanismos de segurança, níveis de serviços e requisitos de gerenciamento de todos os serviços de rede sejam identificados e incluídos em qualquer acordo de serviço de rede, tanto para serviços de rede provido internamento como para terceiros.

• **Proteção e privacidade da informação de identificação pessoal:**
Para evitar violação de quaisquer obrigações legais, estatutárias e regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança, recomenda-se que a privacidade das informações de identificação pessoal seja assegurada conforme requerido por legislação e regulamentação pertinente, quando aplicável.

• **Processo de gestão de incidentes:**
Para que existam procedimentos para assegurar respostas rápidas, efetivas, e ordenadas aos incidentes de segurança da informação, permitindo que incidentes sejam controlados evitando problemas que podem deixar a organização indisponível.