PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

A Política de Segurança da Informação é uma declaração formal da DILLON acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus funcionários.

2. ABRANGÊNCIA

Todos os funcionários, diretores, executivos, acionistas, prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da DILLON, suas Unidades, subsidiárias e/ou coligadas.

3. MISSÃO

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da DILLON.

4. DOCUMENTOS DE REFERÊNCIA

- NBR ISO/IEC 17799:2005
- ABNT 21:204.01-010
- Lei 9.609/98 – Lei do *Software*
- *GDPR - General Data Protection Regulation*
- LGPD – Lei Geral de Proteção de Dados Pessoais - Lei 13.709 de14/08/2018

5. TERMOS E DEFINIÇÕES

- TI: Tecnologia da Informação
- *Software*: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de *softwares*.
- *Backup*: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais.
- Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, *Pen Drive*, cartão de memória entre outros.
- *USB:* É um tipo de conexão em computadores que permite a de uma mídia removível ou periféricos (teclado, mouse, etc).
- VPN (*Virtual Private Network*): Modalidade de acesso remoto à rede corporativa estando o computador fisicamente fora das instalações da companhia. Comumente é utilizado por funcionários em trânsito.
- *Softwares* de Mensageria: São softwares que permitem a troca de mensagem (textos, imagens, sons, arquivos, etc) entre mais de um usuário através da rede corporativa (exemplo: Microsoft Office Communicator, Yahoo Messenger, Gtalk, Skype, etc).
- *Firewall:* É um dispositivo utilizado em redes de computadores para segmentar e controlar os acessos entre redes internar e/ou externas.

- *File Share*: É um ambiente para armazenamento de arquivos na rede corporativa.
- *LOG*: É o termo técnico para descrever o registro das transações que ocorrem quando um software é utilizado.
- *Criptografia*: É um mecanismo com objetivo de impedir que informações trocadas na rede corporativa sejam lidas por pessoas indevidas.
- *Twitter*: WebSite para adição de pequenos trechos de frases ou artigos.
- *Blog*: Site para adição de grandes textos de informação.
- *Modem* 3G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como *Tablets* (com suporte 3G), *notebooks, netbooks, desktops*, etc. objetivando conexão com a internet.
- *Phishing:* Que vem do inglês e corresponde a "pescaria", tem o objetivo de "pescar" informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários, senhas e dados pessoais de um site qualquer, como também são capazes obter dados de contas bancárias e cartões de crédito.

6. DIRETRIZES

6.1. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A informação é um ativo que, como qualquer outro importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação objetiva proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada por:

a) Autenticidade garante a identidade de quem está enviando a informação, ou seja, propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mudanças ao longo de um processo.

b) Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

c) Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

d) Disponibilidade, garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Para assegurar esses quatro itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

A Política de Segurança da Informação da DILLON é aprovada e revisada regulamente pelas Diretoria de Compliance e Riscos.

6.2. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

6.2.1. **Definição**

Cabe a todos os funcionários, estagiários e prestadores de serviços cumprir fielmente a Política de Segurança da Informação; buscar orientação de gestores em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela DILLON; cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual; e comunicar imediatamente a empresa quando do descumprimento ou violação desta política.

6.2.2. **Diretorias, Gerências e Coordenações**

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação; e comunicar imediatamente eventuais casos de violação de segurança da informação através do canal de denúncia.

6.2.3. **Área de Diretoria de Compliance e Riscos**

Cabem as áreas proporem ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

6.3. ENGENHARIA SOCIAL

6.3.1. Engenharia social é um termo utilizado para representar a habilidade de enganar pessoas, visando obter informações sigilosas.

6.3.2. A Engenharia Social manifesta-se de diversas formas, e podemos dividi-los em dois grupos. No entanto, o grande ponto onde engenheiros sociais se baseiam é na falta de conscientização do usuário com relação à Segurança da Informação e na exploração da confiança das pessoas para a obtenção de informações sigilosas e importantes, e como uma simples informação poderia trazer prejuízos à empresa:

6.3.2.1. Diretos: São aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente, pois engenheiro social nem sempre é alguém desconhecido.

6.3.2.2. Indiretos: Caracterizam-se pela utilização de *softwares* ou ferramentas para invadir, como, por exemplo, vírus, cavalos de Tróia ou através de sites e *e-mails* falsos para assim obter informações desejadas. Podem ser mensagens que contenham avisos de premiações
milionárias em loterias, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc. O melhor a fazer é ignorar a oferta tentadora e apagar o *e-mail* imediatamente.

6.4. CLASSIFICAÇÃO DA INFORMAÇÃO

6.4.1. É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com os critérios a seguir:

6.4.1.1. **Pública**: É uma informação da DILLON ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

6.4.1.2. **Interna**: É uma informação da DILLON que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e prestadores de serviços da DILLON.

6.4.1.3. **Confidencial**: É uma informação crítica para os negócios da DILLON ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à DILLON ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

6.4.1.4. **Restrita**: É toda informação que pode ser acessada somente por usuários da DILLON explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

6.4.1.5. **Phishing:** O phishing pode se manifestar de diversas formas. Algumas são bastante simples, como conversas falsas em softwares de mensagens instantâneas e e-mails que pedem para clicar em links suspeitos. Fora isso, existem páginas inteiras construídas para imitar sites de bancos e outras instituições. Todas essas maneiras, no entanto, convergem para o mesmo ponto: roubar informações confidenciais de pessoas ou empresas. O Melhor a fazer é excluir a possível mensagem falsa e em caso de dúvidas entrar em contato com o time de TI e Segurança da Informação.

6.5. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

6.5.1. As máquinas (servidores) que armazenam sistemas da DILLON estão em área protegida fisicamente – *Data Center* localizado na Matriz.

6.5.2. A entrada ao *Data Center* têm acesso devidamente controlado e monitorado.

6.5.3. A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

6.5.4. O uso dentro das dependências da empresa de quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da área de Comunicação e mediante supervisão de um gestor DILLON.

6.5.5. Mesmo para funcionários, os acessos são restritos e permitido apenas para aqueles com responsabilidade de executar tarefas relativas à manutenção do *Data Center*.

6.6. REQUISITOS DE SEGURANÇA DE PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

6.6.1. A DILLON não tem planos de contratação de serviços de processamento, armazenamento de dados e computação em nuvem, a curto ou médio prazos.

6.6.2. Caso haja necessidade de contratação futura destes serviços, a DILLON observará a plena conformidade à Resolução 4.568/2018, em especial ao seu art. 12.

6.7. BOAS PRÁTICAS DE COMUNICAÇÃO VERBAL DENTRO E FORA DA EMPRESA

6.7.1. Cuidado ao tratar de assuntos da empresa dentro e fora do ambiente de trabalho, em locais públicos, ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo fornecedor.

6.7.2. Não é permitido nomes e tratativas de assuntos confidenciais, nestas situações, fora da empresa ou próximos a pessoas desconhecidas.

6.8. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

6.8.1. **Diretrizes Gerais**

6.8.1.1. Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

6.8.2. **Diretrizes Específicas**

6.8.2.1. **Sistemas/Softwares**

6.8.2.1.1. Não executar programas que tenham como finalidade a decodificação de senhas, o
monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

6.8.2.1.2. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da empresa.

6.8.2.1.3. Não enviar informações confidenciais para *e-mails* externos sem proteção. No mínimo, o arquivo deve contar com a proteção de criptografia ou uma senha “robusta”.

6.8.2.1.4. As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada regular e amostralmente e mantida atualizada;

6.8.2.1.5. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da
autorização deve ser claramente definido e registrado;

6.8.2.1.6. A área de Tecnologia da Informação não pode garantir a entrega e o recebimento de mensagens enviadas por e-mail através da Internet, visto que a mensagem está fora do
ambiente de rede (infraestrutura / sistemas / softwares) das empresas aqui mencionadas.

6.8.2.2. **Máquinas – Estação de Trabalho**

6.8.2.2.1. As estações de trabalho, incluindo equipamentos portáteis, e informações devem ser protegidos contra danos ou perdas, bem como o acesso, uso ou exposição indevidos.

6.8.2.2.2. 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.

6.8.2.2.3. O acesso a estação de trabalho deverá ser encerrado no final do expediente, desligando o equipamento.

6.8.2.2.4. Quando se ausentar da mesa, deverá bloquear a estação de trabalho com senha. Esta ação aplica-se a todos os funcionários com estações de trabalho, incluindo equipamentos portáteis.

6.8.2.2.5. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da DILLON, só devem ser utilizadas em equipamentos com controles adequados.

6.8.2.2.6. Apenas pessoal autorizado de TI pode instalar softwares nas estações de trabalho dos usuários e devem utilizar apenas *softwares* licenciados pela DILLON. Em caso de dúvidas, deverá consultar a área de TI através dos canais de suporte (Service Desk).

6.8.2.2.7. A área de Infraestrutura de TI deverá estabelecer os aspectos de controle, distribuição e instalação de *softwares* utilizados.

6.8.2.3. **Utilização de equipamentos particulares / terceiros dentro da empresa**

6.8.2.3.1. *Notebooks* particulares para serem utilizados na rede corporativa, precisam ser avaliados pela área de suporte de TI.

6.8.2.3.2. É responsabilidade da área contratante de terceiros/prestadores de serviço incluir no contrato da prestação de serviço cláusula declarando a responsabilidade da empresa
terceira sobre todo e qualquer software instalado nos equipamentos dos mesmos. E deverá
ser reavaliado semestralmente.

6.8.2.3.3. É responsabilidade da área contratante encaminhar os terceiros sob sua responsabilidade para ao suporte para serem verificadas atualizações do antivírus, existência de vírus e a instalação do certificado digital para acesso a rede corporativa.

6.8.2.4. **Boas práticas de segurança para Impressões**

6.8.2.4.1. Documentos enviados para a impressão deverão ser retirados imediatamente caso a impressora não possua o recurso de impressão por crachá.

6.8.2.4.2. Documentos confidenciais devem ser imediatamente recolhidos das impressoras pelo responsável após a sua impressão.

6.8.2.4.3. Documentos confidenciais não devem ficar expostos com fácil acesso, como por exemplo, sobre as mesas.

6.8.2.5. **A Instalação de *Softwares***

6.8.2.5.1. Qualquer *software* que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado a área de Suporte Técnico – Infraestrutura TI, para que o mesmo possa ser
homologado pelos responsáveis de TI e só assim serem disponibilizados para a área requerente.

6.8.2.5.2. A empresa respeita os direitos autorais dos *softwares* que usa e reconhece que deve pagar o justo valor por eles, coibindo e monitorando o eventual uso indevido de programas não licenciados. É terminantemente proibido o uso de *softwares* ilegais (sem licenciamento) na DILLON.

6.8.2.5.3. A Gerência de TI poderá valer-se deste instrumento para desinstalar, sem aviso prévio, todo e qualquer *software* sem licença de uso, em atendimento à Lei 9.609/98 (Lei do *Software*).

6.8.2.6. **Diretrizes quanto à utilização da Rede Corporativa**

6.8.2.6.1. Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

6.8.2.6.2. Somente os empregados que estão devidamente autorizados a falar em nome da empresa para os meios de comunicação podem escrever em nome da empresa em sites de Bate-Papo (*Chat Room*), *Blogs*, *Twitter*, *Facebook*, *Linkedin, Whatsapp* ou Grupos de Discussão (fóruns,
newsgroups). Em caso de dúvidas, procurar a área de Comunicação.

6.8.2.6.3. Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (*backup*). O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a diretriz acima citada.

6.8.2.6.4. Não é permitida o uso dos recursos de TI para armazenamento de arquivos particulares (músicas, filmes, fotos, etc). Os mesmos podem ser excluídos sem aviso prévio.

6.8.2.7. **Diretrizes quanto ao uso de Mídias Removíveis**

6.8.2.7.1. O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção.

6.8.2.7.2. Informações devem ser transmitidas usando as ferramentas corporativas (email, rede de dados, software de mensageria, etc) que proveem a segurança requerida.

6.8.2.7.3. O uso do modem 3G estando conectado à rede corporativa, não é permitido.

6.8.2.7.4. Os usuários de mídias removíveis, caso comprovado, serão responsabilizados quando os mesmos causarem dano à DILLON, seja por perda/vazamento de informação confidencial e/ou permitir a entrada de vírus ou *softwares* maliciosos na rede corporativa.

6.8.2.7.5. Caso seja necessário transportar arquivos através de mídias removíveis (HD Externo ou PenDrive) é recomendado que os arquivos sejam criptografados e apagados, posteriormente, afim de evitar vazamento de informação sensível.

6.8.2.8. **Diretrizes quanto ao uso da Internet**

6.8.2.8.1. A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

6.8.2.8.2. O acesso às páginas e *web sites* é de responsabilidade de cada usuário ficando vedado o acesso a *sites* com conteúdo impróprios e de relacionamentos.

6.8.2.8.3. O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

6.8.2.8.4. O acesso à internet é monitorado.

6.8.2.9. **Recomendações sobre o uso do Correio Eletrônico (E-Mail)**

6.8.2.9.1. É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral e que possam causar prejuízo moral e financeiro.

6.8.2.9.2. O Correio Eletrônico da DILLON pode ser monitorado e verificado para fins de auditoria.

6.8.2.9.3. Evitar utilizar o *e-mail* da empresa para assuntos pessoais.

6.8.2.9.4. Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou características suspeitas. Em caso de dúvida, comunicar a área de TI.

6.8.2.9.5. Não executar ou abrir links/endereços de e-mails suspeitos, como por exemplo bancos solicitando alguma informação pessoal. Verifique sempre se o e-mail ou o endereço do link são realmente de fontes conhecidas. Em caso de dúvida, comunicar a área de TI.

6.8.2.9.6. Não utilizar o *e-mail* para enviar grande quantidade de mensagens (*spam*) que possam comprometer a capacidade da rede, não reenviando *e-mails* do tipo corrente (criança
desaparecida, criança doente, materiais preconceituosos ou discriminatórios e os do tipo boatos virtuais, etc.) em caso de dúvida, comunicar a área de TI.

6.8.2.9.7. Utilizar o *e-mail* para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

6.8.2.9.8. A acesso externo ao e-mail da DILLON por funcionários em posições que possuam controle/reporte de jornada deve ser aprovado pelo Diretor da área.

6.8.2.10. **Uso de *Softwares* de Mensageria**

6.8.2.10.1. Recomenda-se a utilização do *Software Skype ou similar,* como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado e verificado para fins de auditoria.

6.8.2.10.2. A instalação de *software* de mensageria de terceiros e a liberação do acesso são restritas e sua utilização deve ser justificada à Diretoria de Compliance e Riscos.

6.8.2.11. **Controle de Acesso a VPN**

6.8.2.11.1. O uso do acesso via VPN deve ser restrito a funcionários que sua posição exige acesso a rede corporativa estando fora das localidades de trabalho da DILLON. Exceções deverão ser aprovadas pelo Diretor de Compliance e Riscos.

6.8.2.12. **Controle de Acesso Lógico (Baseado em Senhas)**

6.8.2.12.1. Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.

6.8.2.12.2. Utilizar senha com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

6.8.2.12.3. A senha não deve ser anotada em nenhum local, em hipótese alguma.

6.8.2.12.4. Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros de planilhas.

6.8.2.12.5. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI no primeiro acesso.

6.8.2.12.6. A troca de uma senha bloqueada só deve ser liberada por solicitação do próprio usuário e métodos de validação devem ser inseridos para garantir a autenticidade do solicitante.

6.8.2.12.7. A senha deve ser alterada regularmente conforme política da área de Compliance e Riscos.

6.9 PLANO DE AÇÃO E RESPOSTAS A INCIDENTES

6.9.1. O plano de ação, também conhecido como plano de contingência tem como objetivo descrever as medidas a serem tomadas no intuito de restabelecer os processos afetados por algum tipo de intercorrência.

Abaixo segue listagem das ameaças e procedimentos a serem adotados em cada caso:

Ameaça	Riscos	Envolvidos	Ação	Prazo de Resposta	Prazo Médio de Normalização
Interrupção do serviço de voz	POSSIBILIDADE MÉDIA Perder a comunicação via telefone	Departamentos Técnicos e Administrativos	Utilizar de forma emergencial os telefones celulares corporativos. Acionar a operadora de telefonia.	Imediato	4 horas
Interrupção do link de dados	POSSIBILIDADE ALTA Perder a comunicação com o sistema operacional	Departamentos Técnicos e Administrativos	Alterar o DNS e Gateway para um dos links de contingência.	5 minutos	2 horas
Vírus, Ransomware ou ataque hacker	POSSIBILIDADE BAIXA paralisação das operações	Departamentos Técnicos e Administrativos	Verificar origem do ataque, isolar o acesso. Varredura completa da rede. Sinalizar órgãos fiscalizadores	Imediato	3 horas

Ameaça	Riscos	Envolvidos	Ação	Prazo de Resposta	Prazo Médio de Normalização
Desastres (Incêndio, inundação, assalto)	POSSIBILIDADE BAIXA Impossibilidade de operação da empresa	Departamentos Técnicos, Administrativo, Compliance e Diretoria	Ativação do PCN – Plano de Continuidade de Negócios. Recuperação do back-up externo. Sinalizar órgãos fiscalizadores	6 horas	24 horas
Vazamento de dados e informações	POSSIBILIDADE BAIXA risco de integridade dos negócios	Departamentos Técnicos, Administrativo, Compliance e Diretoria	Verificar origem do vazamento, isolar o acesso. Varredura completa da rede. Sinalizar órgãos fiscalizadores	Imediato	2 horas
Quebra de Integridade de dados	POSSIBILIDADE BAIXA risco de integridade dos negócios	Departamentos Técnicos, Administrativo, Compliance e Diretoria	Verificar origem da injeção fraudulenta. Varredura completa da rede. Sinalizar órgãos fiscalizadores	Imediato	2 horas
Fraudes Eletrônicas	POSSIBILIDADE BAIXA risco de integridade dos negócios	Departamentos Técnicos, Administrativo, Compliance e Diretoria	Analisar potencial da fraude, verificar dano, realizar varredura completa. Sinalizar órgãos fiscalizadores	Imediato	2 horas

No caso de ocorrências de incidentes relevantes e das interrupções dos serviços que possam configurar situação de crise, tais ocorrências deverão ser imediatamente comunicadas ao Banco Central do Brasil e CVM – Comissão de Valores Mobiliários, detalhando o fato, as providências tomadas, e o prazo previsto para reinicio das atividades.

6.10. RELATÓRIOS E TESTES ANUAIS

6.10.1. Anualmente é elaborado o relatório anual descrevendo o plano de ação e resposta a ocorrências, relatório este que contempla tópicos como efetividade de implementação, resultados obtidos e ocorrências relevantes ligadas ao ambiente cibernético.

6.10.2. São executados periodicamente testes e varreduras no intuito de identificar vulnerabilidades para aprimorarmos os processos e documentarmos os resultados obtidos e observações pertinentes em nosso relatório, devendo-se acrescentar que este deve ser apresentado a diretoria da empresa e arquivado por no mínimo 5 anos.

6.11. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

6.11.1. Nos casos em que houver violação desta política, sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis**.**

6.11.2. O funcionário infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato, à diretoria correspondente e à Presidência.

6.12. VIGÊNCIA E VALIDADE

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado.