Política de Segurança da Informação

Informações Gerais

Título	Política de Segurança da Informação
Número da Versão	
Aprovador	Gabriela Bergamo
Data da Aprovação	01/01/2023
Data da Próxima Revisão	01/01/2024
Departamento Responsável pela Política	Tecnologia da Informação
Classificação da Informação	Interno

Histórico das versões

Versão	Motivo da Alteração	Data da alteração	Autor	Departamento
1	Inicial	01/01/2023	Décio Moreno	TI

Aprovação

Data da Aprovação	Aprovador	Departamento
01/01/2023	Gabriela Bergamo	Jurídico

1. OBJETIVO

Definir as diretrizes que tratam das normas e padrões para a proteção da informação, envolvendo sua geração, armazenamento, utilização, distribuição, integridade, confidencialidade, confiabilidade e disponibilidade, independentemente do meio em que esteja armazenada ou da mídia utilizada para sua transmissão.

2. RESPONSABILIDADE

Esta Política de Segurança é de responsabilidade do Departamento de Tecnologia da **D3 PAGAMENTOS** e de sua direção. Quaisquer alterações neste documento devem ser aprovadas pelo Departamento de Tecnologia da **D3 PAGAMENTOS** e por sua direção.

3. DATA DE INÍCIO DA VALIDADE

Esta Política de Segurança entra em vigor na data de sua publicação, presente ao final deste instrumento.

4. PÚBLICO-ALVO

Esta Política de Segurança se aplica a todas as unidades operacionais, a todos os departamentos da **D3 PAGAMENTOS**, seus colaboradores, parceiros e terceirizados.

5. DIRETRIZES GERAIS

5.1. GERAÇÃO DA INFORMAÇÃO

Todos os processos de obtenção, captura ou coleta de informação devem utilizar apenas meios homologados pelo Departamento de Tecnologia da **D3 PAGAMENTOS**, sendo mantida a confidencialidade com uso de tecnologias de criptografia e canais seguros de comunicação.

5.2. TRATAMENTO DA INFORMAÇÃO

Toda a informação mantida e armazenada pela **D3 PAGAMENTOS**, independentemente de serem de clientes, fornecedores, parceiros, usuários, colaboradores ou terceiros, devem ser protegidas contra acesso indevido e não autorizado.

A Obtenção, Geração, Utilização, Consulta, Análise, Armazenamento, Manutenção, Manipulação, Distribuição, Descarte e Destruição da Informação devem ser realizadas conforme a necessidade da **D3 PAGAMENTOS**, sendo que todos esses processos devem ser devidamente documentados.

A **D3 PAGAMENTOS** reserva-se o direito de consultar e analisar informações a ela pertinentes, que estejam armazenadas em meios sob sua responsabilidade, incluindo documentos físicos e eletrônicos, gerados ou recebidos através de seus recursos humanos, materiais ou tecnológicos.

Para o compartilhamento seguro da informação, devem ser utilizados somente meios e recursos autorizados e previamente homologados pelo Departamento de Tecnologia da **D3 PAGAMENTOS**.

O prazo para o armazenamento das informações deve ser pelo tempo determinado pela **D3 PAGAMENTOS** ou pela legislação vigente, valendo a maior. Deve haver meios para recuperação das mesmas, caso necessário.

O armazenamento das informações deve ser apropriado e devidamente protegido contra intempéries, sinistros e acessos não autorizados.

5.3. ACESSO À INFORMAÇÃO

Toda utilização de redes de comunicação externas à **D3 PAGAMENTOS**, tais como: Internet, túneis, redes privadas, etc. devem ter seus usos controlados e monitorados através de tecnologias de *Firewall*, *Antimalwares*, *Antivirus*, *Antispam*, Detecção de Intrusão e outras, que garantam e limitem a comunicação para que somente os recursos necessários estejam disponíveis para o uso, mitigando os riscos para o ambiente operacional.

Os acessos realizados pela Equipe de Suporte Técnico, Prestadores de Serviços ou Colaboradores devem ser monitorados, controlados e restritos aos serviços necessários. Deve-se ainda manter em registro os recursos e ações tomadas por indivíduo. As soluções aplicadas devem ser formalizadas e documentadas.

Toda a transmissão ou transferência de informação para fora das dependências da **D3 PAGAMENTOS** deve ser aprovado e formalizado pelos gestores responsáveis pela informação, levar em conta os riscos envolvidos e a real necessidade. Em caso de real necessidade devem ser adotados procedimentos que garantam total controle e registro das operações. A integridade das informações deve ser garantida, assim como também a autenticidade e legitimidade do receptor.

5.4. DESCARTE DA INFORMAÇÃO

Ao atingir o final de seu ciclo de vida, a Informação deverá ser totalmente descartada ou destruída. Tais procedimentos devem ser documentados e realizados sob controle dos gestores responsáveis pela informação. No intuito de permitir sua recuperação, em casos de necessidade, apenas cópias de segurança mantidas em locais seguros e protegidos contra acessos não autorizados são permitidas.

5.5. SISTEMAS E APLICAÇÕES

Todos os Sistemas e Aplicações desenvolvidos pela equipe técnica da **D3 PAGAMENTOS** ou por seus colaboradores devem ser devidamente documentados de acordo com as boas práticas da área. Todas as correções e/ou alterações realizadas devem ser salvas com a utilização de versionamento e armazenamento seguro da biblioteca de fontes. Devem constar documentadas todas as informações necessárias para uma eventual reconstrução dos códigos.

No caso de Sistemas e Aplicações desenvolvidos externamente e de propriedade de terceiros, devem ser respeitadas as licenças de uso. Devem, ainda, serem mantidas fontes e/ou instaladores para eventuais procedimentos de restaurações. Caso o desenvolvimento por terceiros seja específico, deve ser realizado sob cuidados da equipe técnica especializada da **D3 PAGAMENTOS**, para que a aplicação esteja isenta de falhas e de códigos maliciosos.

Vazamento de códigos fonte e o mau uso de sistemas, seja de forma acidental ou deliberada, devem ser combatidos utilizando técnicas de restrições de execução, fragmentação de atividades, segregação de funções administrativas, permissões de acesso e isolamento de códigos. Todas as atividades e acessos devem ser registrados para que se possam identificar ações e os responsáveis por elas.

Para que riscos e falhas nos sistemas sejam mitigados, a disponibilidade e capacidade dos recursos tecnológicos devem ser planejados com antecedência e frequentemente reavaliados. No caso de

novas versões de sistemas e aplicações os requisitos operacionais devem ser levantados, documentados e testados antes de serem homologados e habilitados em ambiente de produção. Para sistemas e aplicações em uso e já consolidadas, projeções periódicas de demanda de recursos e carga devem ser realizadas no intuito de se reduzir riscos de indisponibilidade por sobrecarga.

6. DIRETRIZES ESPECÍFICAS

6.1. PROPRIEDADE DA INFORMAÇÃO

Para cada conjunto de informações utilizadas pelos sistemas e aplicativos da **D3 PAGAMENTOS**, devem ser nomeados dois proprietários, obrigatoriamente diretores da **D3 PAGAMENTOS**. Um deles deve ser o diretor responsável pela categoria e pertinência da informação e o outro deve ser o diretor de tecnologia. No caso da categoria e pertinência da informação ser tecnológica, outro diretor deverá ser designado segundo proprietário por meio de eleição ou atribuição. O que for considerado o mais adequado pelo conselho deliberativo da **D3 PAGAMENTOS**.

São atribuições dos proprietários das informações:

I. Nomear o gestor das informações, que será responsável por definir as regras de acesso e utilização delas.
II. Aprovar as regras de acesso e utilização das informações, conforme proposta apresentada pelo gestor.

São atribuições do gestor das informações:

I. Definir as regras de acesso e utilização das informações, que deverão ser apresentadas aos proprietários das informações para aprovação.
II. Monitorar, acompanhar e controlar todas as operações que afetam de forma direta ou indireta as informações sob sua gestão.
III. Indicar um gestor substituto para exercer suas funções em caso de ausência. Este substituto precisará ser aprovado pelos proprietários da informação.

Cada gestor e seu substituto deverão possuir credenciais individuais com as devidas permissões para exercerem suas funções, seguindo assim as normas para o tratamento da informação.

6.1.1. NORMAS PARA O TRATAMENTO DA INFORMAÇÃO

As regras para a proteção da informação devem ser claras e absolutas, para evitar perdas, acessos não autorizados e permanência da informação além de seu ciclo de vida.

Os usuários devem ser claramente definidos, assim como seus departamentos e grupos de atividades. Também devem ser claramente identificados os parceiros, terceiros e contratados. Todos devem seguir as regras definidas para os procedimentos de acesso às informações, protegendo-as de acesso por pessoas não autorizadas independentemente dos meios de armazenamento e transmissão utilizados. Toda e qualquer informação deve ser utilizada apenas para os fins e propósitos profissionais, de interesse exclusivo da empresa. Portanto nenhuma informação deve ser acessada, manipulada, copiada, divulgada ou disponibilizada, sob qualquer circunstância, sem a prévia autorização dos proprietários da informação.

Todas as informações importantes e relevantes devem possuir cópias de segurança em meios de armazenamento seguros e eficientes para pronta recuperação, caso necessário. Essas cópias de segurança deverão ser mantidas fora do alcance de pessoas não autorizadas e protegidas por

tecnologias de criptografia/senhas.

É expressamente proibida a transmissão das informações de propriedade ou sob a guarda da **D3 PAGAMENTOS** a terceiros, independentemente do meio, bem como a reprodução, cópia, utilização, divulgação ou exploração de informações privilegiadas sem a prévia e expressa autorização dos proprietários das informações.

Ficam vedadas as divulgações ou transmissão de conhecimentos e informações dos quais os colaboradores, parceiros ou contratados venham a tomar conhecimento durante a relação que mantiverem com a **D3 PAGAMENTOS**, sem prejuízo das ações de naturezas penais aplicáveis.

6.1.2. RECOMENDAÇÕES PARA O TRATAMENTO E MANIPULAÇÃO DAS INFORMAÇÕES

Manutenções realizadas em equipamentos que armazenam informações devem sempre ser acompanhadas pelo responsável pelo equipamento.

No caso de equipamentos ou mídias que armazenam informações que sejam descartados, vendidos, devolvidos, encaminhados para manutenção externa, remanejados para outras utilizações/funções de forma permanente ou provisória, deverão ter suas informações destruídas antes dos procedimentos. Caso possível, os dispositivos de armazenamento devem ser retirados e retidos.

Caso alguém receba indevidamente ou equivocadamente alguma informação, este deverá comunicar imediatamente o remetente para alertá-lo do ocorrido. As informações recebidas nessas condições deverão ser imediatamente excluídas, destruídas ou, no caso de meios físicos, devolvidas ao remetente.

Os gestores devem determinar regras claras para o acesso, distribuição e manipulação das informações, sempre considerando:

I. Riscos às Informações:
- Acesso por pessoas não autorizadas;
- Alteração indevida;
- Divulgação indevida;
- Cópia Indevida;
- Indisponibilidade.

II. Consequências:
- Problemas legais: Possibilidade de penalidades, multas, prejuízos, embaraços ou constrangimentos;
- Fraudes: Possibilidade de que a **D3 PAGAMENTOS**, outras organizações ou pessoas sejam lesadas de alguma forma;
- Perda de negócios: Possibilidade de gerar perdas financeiras ou intelectuais em negócios atuais ou previstos, ou de não se realizarem receitas previstas;
- Prejuízo à imagem da **D3 PAGAMENTOS**: Possibilidade de prejudicar a imagem da **D3 PAGAMENTOS** ou de seus colaboradores frente ao mercado, clientes ou concorrências;
- Problemas para restauração: Possibilidade de geração de custos para a recuperação de informações perdidas, alteradas ou danificadas.

6.2. SEGURANÇA DA INFORMAÇÃO

Com o objetivo de reduzir os riscos causados inadvertidamente, acidentalmente ou intencionalmente, todos os colaboradores da **D3 PAGAMENTOS** devem ser informados pelo departamento de Recursos Humanos e estarem cientes das responsabilidades e punições inerentes à divulgação e/ou tratamento inadequado dos dados sob custódia da **D3 PAGAMENTOS**. Este conceito também deve ser aplicado para terceirizados contratados, prestadores de serviços e clientes.

I. Colaboradores: A Declaração de Responsabilidade deve ser lida e assinada por todos os colaboradores antes de assumirem suas funções. Esta declaração deve ser arquivada na respectiva pasta funcional. É da responsabilidade do Departamento de Recursos Humanos que todos os colaboradores tenham sua Declaração de Responsabilidade devidamente assinada. Essa declaração poderá ser em formulário eletrônico, desde que seja aprovado pelo Conselho Administrativo e que os colaboradores utilizem assinatura digital válida e oficialmente certificada;
II. Prestadores de Serviços e Terceirizados: A Declaração de Responsabilidade deve ser uma das cláusulas do contrato; (**Anexo**)
III. Clientes: A Declaração de Responsabilidade deve ser uma das cláusulas do termo de adesão ou de documento equivalente, no caso de o cliente receber alguma senha de acesso às informações.

6.3. SEGURANÇA LÓGICA DE REDES, SISTEMAS, APLICATIVOS E COMPUTADORES

Este item trata do controle de acesso aos Computadores, Redes, Sistemas e Aplicativos em operação a serviço da **D3 PAGAMENTOS**.

Cada Sistema ou Aplicativo possui um conjunto de operações que afetam os dados e as informações sob seu domínio, que normalmente são operações de Inclusão, Alteração, Consulta e Exclusão.

O acesso a Computadores e a Redes normalmente é definido através de Perfis e Grupos, que definem as operações que podem ser executadas por uma determinada classe de usuários ou por um indivíduo.

Todo acesso e operação realizada deve gerar registros que possibilitem aos gestores identificarem o indivíduo que a executou, as operações realizadas, os registros de informações afetadas, contendo a data e a hora de cada procedimento e outras informações relevantes definidas pela Direção de Tecnologia da **D3 PAGAMENTOS**.

6.3.1. SEGURANÇA LÓGICA DE COMPUTADORES E REDES

A Política de Segurança de Redes deve ser definida baseada em Grupos com base nos requisitos operacionais de cada área ou departamento. Perfis individuais com permissões especiais devem ser evitados, salvo em casos específicos definidos pela Direção de Tecnologia. Todos esses casos devem ser devidamente documentados com menção aos motivos para tal.

Atualizações de segurança (*patches*) devem ser aplicadas mensalmente para evitar falhas que possam ser exploradas por códigos maliciosos. Tais atualizações devem ser realizadas tanto nos servidores como em estações de trabalho e equipamentos pessoais que se conectem à **D3 PAGAMENTOS**. Atualizações de Sistemas Operacionais dos servidores devem ser realizadas anualmente.

6.3.2. SEGREGAÇÃO ENTRE REDES

As Redes Lógicas devem ser separadas em Ambiente de Produção e Ambiente de Desenvolvimento. Estas devem estar segregadas. Apenas a Direção de Tecnologia, o Administrador de Redes e usuários autorizados podem ter acesso ao Ambiente de Produção. Os demais usuários e desenvolvedores devem possuir acesso somente ao Ambiente de Desenvolvimento.

Toda e qualquer alteração que deva ser aplicada ao Ambiente de Produção deve ser submetida a análise da Direção de Tecnologia para homologação.

Qualquer transferência de dados, sistemas e aplicações entre os Ambientes distintos apenas pode ser realizado através de solicitação formal da Direção de Tecnologia e deve ser executado somente pelo Administrador de Redes ou por usuários autorizados.

6.3.3. ACESSO AOS SISTEMAS E APLICATIVOS

As Informações mantidas pela **D3 PAGAMENTOS** devem ser analisadas pelos respectivos gestores da informação, para que se possam definir as regras de acesso a serem aplicadas.
Os Sistemas e Aplicativos, tal como o acesso as Redes, devem possuir recursos que possibilitem o acesso controlado, conforme definição pelos respectivos gestores da informação.

6.3.4. ADMINISTRAÇÃO DE USUÁRIOS

Devem ser definidos, formalmente, todos os procedimentos de definições de acessos. Tanto para os Computadores, as Redes, os Sistemas e os Aplicativos. Indo desde a criação de um novo usuário, definição de privilégios, sua inserção em um ou mais grupos de acesso, senha e sua posterior exclusão.

6.3.5. CONTROLE DE ACESSO À REDE E AOS COMPUTADORES

Os Acessos aos Recursos Computacionais pelos usuários devem sempre ocorrer através de procedimentos seguros, os quais devem ser planejados de forma a mitigar as oportunidades de acessos não autorizados.

Deve-se assegurar que os usuários não comprometam a segurança dos Computadores, Redes, Sistemas e Aplicativos ou quaisquer outros recursos através de um controle rígido de suas Permissões de Acesso Individual e de Grupo, assim como de suas responsabilidades definidas na sua Declaração de Responsabilidade.

Deve haver segregação entre os ambientes de Produção, Homologação e Desenvolvimento, de forma a impedir acessos indevidos ou acidentais.

No ambiente interno, as mídias de armazenamento removíveis devem ter acesso controlado. Quando não estiverem sendo utilizados devem ser guardados trancados e com acesso restrito a pessoas autorizadas

6.3.6. NORMAS PARA O CONTROLE DE ACESSOS A COMPUTADORES, REDES SISTEMAS E APLICATIVOS

Um sistema de controle de acesso Seguro e Efetivo deve ser utilizado para autenticar os usuários: As principais características para esse controle são:

I. Os acessos aos Computadores e Redes devem ser protegidos por senhas fortes, com política avalizada pela Direção de Tecnologia;
II. As senhas deverão ser alteradas pelos usuários no momento de seu primeiro acesso, seguindo a política de senhas pré-definida. Isto vale tanto para acesso a Computadores e Redes quanto a Sistemas e Aplicativos;
III. As senhas poderão ser alteradas pelos usuários através de sistemas a qualquer momento;
IV. Os sistemas devem ser desenvolvidos de forma a nunca exibir a senha na tela;
V. Pode-se solicitar alteração das senhas, para os usuários, a qualquer momento. Isso vale para os casos de suspeitas de falhas de segurança, decorrência de prazo prescricional, alteração nas políticas de senhas ou quaisquer outras razões definidas, ou avalizadas pela Direção de Tecnologia;
VI. As senhas devem ser individuais e intransferíveis: **A SENHA É DE USO EXCLUSIVO, PESSOAL E INTRANSFERÍVEL, SENDO O COMPARTILHAMENTO PROIBIDO SOB QUAISQUER CIRCUNSTÂNCIAS. TAL ATITUDE É PASSÍVEL DE MEDIDAS DISCIPLINARES**;
VII. As senhas não devem ser triviais, previsíveis ou serem compostas por parte, ou ao todo por informações pessoais, tais como: Data de nascimento, nome próprio, telefone, etc.;
VIII. O tamanho mínimo para as senhas deve ser de 8 (oito) caracteres e deve possuir no mínimo 3 (três) dos seguintes itens: Letras minúsculas, letras maiúsculas, números e caracteres/símbolos especiais (Ex.: @#$%&*-+=[]{}()?!);
IX. As senhas dos usuários devem expirar a cada 90 (noventa) dias. As senhas alteradas ou expiradas devem ser armazenadas para efeito de bloqueio de utilização por no mínimo 10 (dez) alterações;
X. A sessão do usuário deve ser encerrada automaticamente caso haja inatividade por um período de 15 (quinze) minutos.

6.3.7. MONITORAMENTO DE USO E ACESSO AOS SISTEMAS E APLICATIVOS

Os Computadores, Redes, Sistemas e Aplicativos deverão:

I. Detectar tentativas de acesso não autorizado;
II. Registrar eventos de entrada e saída nos sistemas (*login* e *logoff*);
III. Armazenar trilhas de atividades para auditoria ou futuras investigações, registrando operações tais como: Identificação do usuário, identificação da estação de trabalho, data, hora, identificação do aplicativo utilizado e operações realizadas;
IV. Registrar trilhas de atividades adicionalmente em servidor de monitoração segregado, para evitar perda de registros ou exclusão deliberada, mantendo tais registros por um período mínimo de 2 (dois) anos;
V. Ter seus registros de trilhas de atividades verificadas diariamente para que se assegure a integridade dos sistemas;
VI. Disponibilizar relatórios gerenciais de acessos por usuário, grupo, aplicativos e outros que forem julgados necessários pela equipe de gestão, avalizada pela Direção de Tecnologia;

VII. Sofrerem processos periódicos de testes de intrusão, sendo utilizadas ferramentas próprias para cada um dos protocolos e serviços em uso pelos equipamentos e servidores em operação.

6.3.8. TRABALHO REMOTO

Aos usuários é permitido o uso de dispositivos pessoais para o acesso remoto apenas ao Ambiente de Desenvolvimento da **D3 PAGAMENTOS**.

Para que os usuários possam acessar o Ambiente **D3 PAGAMENTOS** devem:

I. Possuir antivírus, homologado pela **D3 PAGAMENTOS**, instalado e devidamente atualizado;
II. Acessar o Ambiente **D3 PAGAMENTOS** através de conexão VPN criptografada;
III. Realizar as atividades através de Rede Privada Virtual e Ambiente Remoto (*Remote Desktop/VDI*);
IV. Desconectar-se imediatamente após o término de suas atividades.

6.4. SEGURANÇA NO ACESSO DE PRESTADORES DE SERVIÇOS

Este tópico estabelece os controles sobre os recursos computacionais da **D3 PAGAMENTOS** durante a execução de serviços realizados por contratados externos.

Sempre deverá ser realizada uma avaliação dos potenciais riscos envolvidos nas operações para determinar as implicações de segurança e os controles a serem aplicados. As definições tomadas devem ser explicitadas em contrato assinado entre as partes para que os procedimentos possam ser realizados. Nesse contrato também devem constar medidas legais cabíveis no caso de quebra do mesmo por parte do contratado.

6.5. SEGURANÇA FÍSICA DE COMPUTADORES E ESTAÇÕES DE TRABALHO

O Objetivo deste tópico é garantir que os usuários utilizem os Computadores e Estações de Trabalho de forma segura, aplicando medidas adequadas para que se respeitem a confidencialidade, integridade e disponibilidade das informações armazenadas, manipuladas e disponibilizadas através desses equipamentos.

6.5.1. NORMAS PARA A SEGURANÇA FÍSICA DE COMPUTADORES E ESTAÇÕES DE TRABALHO

Caso haja equipamentos desconectados das redes e que contenham informações relevantes aos negócios da **D3 PAGAMENTOS**, estes deverão estar instalados em local físico seguro e incluam sistemas que garantam o fornecimento adequado de energia elétrica e de recuperação de dados.

Os usuários conectados a uma rede e que tratam de informações relevantes à **D3 PAGAMENTOS**, devem sempre manter essas informações armazenadas nos servidores de rede adequados da **D3 PAGAMENTOS**.

6.5.2. RESPONSABILIDADE QUANTO A SEGURANÇA FÍSICA DE COMPUTADORES E ESTAÇÕES DE TRABALHO

A Direção de Tecnologia é responsável por elaborar e manter o inventário de software e de hardware atualizado utilizados na **D3 PAGAMENTOS**.

A área de Segurança Patrimonial é responsável por garantir o controle de acesso físico aos equipamentos.

6.6. GERAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

Este tópico se destina aos administradores de redes da **D3 PAGAMENTOS**, visando a correta utilização e a segurança dos recursos de informática para garantir a preservação dos dados, aplicativos e sistemas em caso de incidentes.

Para a elaboração de um plano de Geração de Cópias de Segurança (*backups*) devem ser consideradas 3 (três) modalidades distintas: Operacional, Contingencial e Histórica.

I. Operacional: É a cópia das informações estratégicas dos usuários, que visam garantir a continuidade de suas tarefas. Destina-se à recuperação imediata;
II. Contingencial: É a cópia das informações sensíveis de aplicações e sistemas vitais à continuidade dos negócios da **D3 PAGAMENTOS** e deve ser guardado em local externo devidamente protegido. Destina-se a permitir a restauração das informações em caso de situações catastróficas;
III. Histórica: É a cópia das informações determinadas por normas internas ou exigência legal e deve ser guardado em local externo devidamente protegido.

6.6.1. NORMAS PARA A GERAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

A elaboração do plano de Geração de Cópias de Segurança deverá levar em consideração a Periodicidade de Atualização dos Dados e as Particularidades de cada área da **D3 PAGAMENTOS**.

I. As informações consideradas fundamentais e imprescindíveis deverão fazer parte das rotinas de cópias de segurança Operacional e Contingencial conforme critérios definidos pela Direção de Tecnologia junto com a Equipe Técnica e Usuários Responsáveis;
II. As cópias de Segurança devem ser guardadas em local seguro e apropriado, devidamente protegidas de acesso por pessoas não autorizadas;
III. Deve-se manter uma cópia do plano de Geração de Cópias de Segurança junto com as Cópias de Segurança geradas;
IV. Devem ser realizados testes periódicos de Restauração das Cópias de Segurança, registrando-se os resultados obtidos, conforme definição no plano de Geração de Cópias de Segurança;
V. Devem ser mantidas, no mínimo, as duas últimas versões das Cópias de Segurança Operacional e Contingencial. Para as Cópias Históricas, a quantidade de versões será determinada por norma interna ou exigência legal.

6.6.2. PLANO DE GERAÇÃO E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA

I. Periodicidade: Intervalo de tempo após o qual os sistemas são submetidos à rotina de Cópia de Segurança;
II. Retenção: Prazo pelo qual as Cópias de Segurança devem ser mantidas;
III. Abrangência: Relação dos diretórios e arquivos a serem copiados no processo de Cópia de Segurança;
IV. Quantidade de Cópias: Número de Cópias de Segurança a serem geradas e mantidas em locais adequados;
V. Locais: Locais de armazenamento adequados e seguros para o armazenamento das Cópias de Segurança;
VI. Meios: Meios de armazenamento para as Cópias de Segurança;

VII. Procedimentos: Descrição dos procedimentos para Geração e Restauração das Cópias de Segurança;
VIII. Identificação dos Meios de Armazenamento: Os meios de armazenamento devem ser devidamente identificados, indicando conteúdo, data, hora e sequência das Cópias de Segurança;
IX. Registro de Uso das Cópias de Segurança: A manipulação dos meios de armazenamento deve ser controlada e registrada por no mínimo 90 (noventa) dias para futuras verificações;
X. Manutenção das Cópias de Segurança: No caso do prazo de retenção for superior ao especificado pelo fabricante do meio de armazenamento, deve-se adotar procedimentos para a regravação e/ou transferência dos dados para novo meio. Este procedimento deve ser periódico.

6.6.3. RESPONSABILIDADES QUANTO A GERAÇÃO E RESTAURAÇÃO DAS CÓPIAS DE SEGURANÇA

É de responsabilidade conjunta do Administrador de Redes e da Direção de Tecnologia elaborar, manter e documentar o plano de Cópias de Segurança, garantindo assim a execução dos procedimentos.

6.6.4. TESTES REGULARES

Todo e qualquer meio de armazenamento, assim como os procedimentos para a Recuperação das Cópias de Segurança devem ser regularmente testados para garantir sua efetividade. A periodicidade deve ser determinada pela Direção de Tecnologia em conjunto com o Administrador de Redes, considerando o nível de Risco ao Negócio. Os procedimentos devem ser devidamente registrados.

6.7. PIRATARIA

Este item é destinado a todos os usuários, administradores e diretores que utilizam os recursos de informática e equipamentos, nas dependências ou a serviço da **D3 PAGAMENTOS**. Isso inclui computadores, inclusive portáteis pessoais ou não, conectados ou não a uma rede. Tem-se como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de *softwares* na **D3 PAGAMENTOS**.

É expressamente proibida a aquisição, reprodução, utilização e cessão de cópias não autorizadas de programas e aplicativos ou de qualquer outro tipo de *software*, mesmo que desenvolvido internamente ou por terceiros para a **D3 PAGAMENTOS**.

6.7.1. NORMAS CONTRA A PIRATARIA

I. A quantidade de licenças de *softwares* não pode ser inferior a quantidade de *softwares* instalados, mesmo que para fins de treinamentos ou testes, a menos que esta situação seja coberta contratualmente junto aos detentores dos direitos dos *softwares*;
II. Não é permitido duplicar *software* de propriedade da **D3 PAGAMENTOS** a não ser com finalidade de Cópia de Segurança. Tal procedimento somente pode ser realizado por pessoas autorizadas;
III. *Softwares* de propriedade de terceiros, licenciados para terceiros ou para colaboradores da **D3 PAGAMENTOS** não podem ser instalados ou executados na **D3 PAGAMENTOS**;
IV. É proibida a utilização e/ou reprodução não autorizada de manuais, livros, revistas, periódicos ou quaisquer outros materiais protegidos por direitos autorais, sejam físicos ou digitais.

6.7.2. RESPONSABILIDADES QUANTO À PIRATARIA

É de responsabilidade do Administrador de Redes e da Direção de Tecnologia da **D3 PAGAMENTOS**, implementar mecanismos de coíbam e dificultem a pirataria através de qualquer forma e meio.

6.8. SEGURANÇA NA UTILIZAÇÃO DE EQUIPAMENTOS E SISTEMAS

Todos os equipamentos, fixos ou portáteis, que tenham capacidade de armazenamento de dados devem ser protegidos conforme normas definidas pela Direção de Tecnologia. No caso desses equipamentos possuírem informações sigilosas ou que não possam ser de conhecimento público, esses deverão ter suas informações criptografadas ou protegidas por senha.

6.9. FERRAMENTAS DE PRODUTIVIDADE

A **D3 PAGAMENTOS** disponibiliza, aos seus colaboradores, uma série de ferramentas de produtividade, tais como: Correio Eletrônico, Plataforma para Agendas, Reuniões e Trocas de Informações, Controle de Atividades e Tarefas, Controle de Versão de Desenvolvimento, entre outros. É de responsabilidade do usuário a correta utilização da tecnologia, de forma adequada e compatível com as leis e os princípios do negócio.

6.10. PLANO DE CONTINUIDADE DO NEGÓCIO

O Plano de Continuidade do Negócio visa garantir a recuperação dos processos críticos da **D3 PAGAMENTOS** quando da indisponibilidade de quaisquer recursos ou ambientes que venham impossibilitar o desenvolvimento e/ou as operações das áreas operacionais e de negócios de forma adequada.

É de responsabilidade de cada área envolvida nos processos e negócios da **D3 PAGAMENTOS** elaborar, testar e implantar seus planos de contingência.

6.10.1. ITENS E AÇÕES DA COMPOSIÇÃO DO PLANO DE CONTINUIDADE DO NEGÓCIO

Os itens abaixo devem ser observados para a elaboração de um Plano de Continuidade do Negócio:

I. As atividades e os processos críticos devem ser identificados e definidos;
II. Priorizar as atividades e os processos críticos;
III. Definir uma estratégia para a recuperação de cada atividade e processo crítico;
IV. Identificar as ações necessárias para a recuperação das atividades e processos;
V. Quantificar os recursos humanos e técnicos necessários para a execução do Plano;
VI. Documentar as atividades e os processos críticos;
VII. Identificar os responsáveis para a recuperação de cada atividade e processo;
VIII. Definir as ações para restabelecer a operação normal;
IX. Identificar eventuais recursos adicionais, tais como: Cópias de Segurança, equipamentos, programas, sistemas, aplicativos, telecomunicação etc.

6.10.2. Revisões e Acompanhamentos Periódicos do Plano de Continuidade do Negócio

O Plano de Continuidade do Negócio deve ser revisado periodicamente a fim de identificar pontos que necessitem de atualizações ou que não estejam adequados à situação atual. Deve-se observar:

I. Troca de colaboradores, fornecedores ou contratados;
II. Alterações de informações de contato;
III. Mudanças nas prioridades das atividades e dos processos;
IV. Alteração nas prioridades das atividades de Recuperação;
V. Interdependência entre sistemas e aplicativos;
VI. Mudanças nas atividades, funções e nos processos críticos do negócio;
VII. Alterações nas práticas operacionais.

6.11. PLANO DE CONSCIENTIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Para se garantir que a Segurança da Informação seja conhecida e compreendida por todos os colaboradores da **D3 PAGAMENTOS**, torna-se necessário a implementação de um Plano de Conscientização de Segurança da Informação. Esse plano deve promover a consciência sobre as melhores práticas, riscos, responsabilidades e requisitos. Deve também apontar as medidas a serem adotadas em caso de incidentes de Segurança a fim de proteger a informação e mitigar danos.

6.12. Diretrizes Básicas para o Plano de Conscientização da Segurança da Informação

I. Elaboração de treinamento contínuo, contemplando todos os níveis da **D3 PAGAMENTOS**;
II. Divulgação de materiais e notas rápidas referentes a Segurança da Informação para usuários, colaboradores, terceiros e clientes;
III. Criação de método de aferição do conhecimento dos usuários e colaboradores em geral;
IV. Organização de eventos que visem fortalecer a conscientização sobre os diversos aspectos de segurança de uma forma geral;
V. Revisão periódica do Plano, para adequá-lo as novas necessidades e realidades.

6.13. PLANO DE RESPOSTA A INCIDENTES

É de responsabilidade da Direção de Tecnologia publicar e revisar o Plano de Resposta a Incidentes Cibernéticos. Esse plano deve conter cada etapa de cada uma das tratativas a partir da identificação de um incidente, objetivando a criação de uma abordagem e de conduta mínima.