viveo

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. OBJETIVO

A presente Política tem como objetivo fornecer as diretrizes necessárias e fundamentais que orientam os funcionários, prestadores de serviço e fornecedores da Viveo, a desempenhar um papel ativo na proteção das informações e recursos tecnológicos. Tais diretrizes tem como objetivo final proteger os ativos da Viveo, garantindo um ambiente seguro e confiável para o negócio.

2. ABRANGÊNCIA

A Política de Segurança da Informação do ecossistema Viveo é aplicável a todos os sócios, diretores, executivos, colaboradores (incluindo temporários), terceiros subcontratados e parceiros de negócio da Viveo, presentes no território nacional e internacional que tenham acesso aos recursos de tecnologia e informações da Viveo.

3. DOCUMENTOS DE REFERÊNCIA

- Código de Conduta Ética
- Política de backup (documento interno)
- Política de Incidentes de segurança da informação

4. GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Todos os funcionários, prestadores de serviços e fornecedores devem ter conhecimento sobre a estrutura de segurança vigente na Viveo e estar em conformidade com as políticas, normas e procedimentos de segurança definidos.

- A área de segurança da informação é responsável por criar, manter e divulgar as políticas e normas de segurança da informação, bem como avaliar qualquer necessidade de modificação ou exceção. E, assegurar que todos os procedimentos formalizados estejam aderentes às políticas e normas de segurança da informação.
- O Comitê de Segurança da Informação, que é composto pela liderança executiva de áreas de negócio e suporte, é responsável pela aprovação das

modificações nas políticas de segurança da informação ou exceções às políticas e normas.

- Os líderes de cada área devem assegurar que os procedimentos e atividades de suas áreas sigam as políticas, normas e procedimentos de segurança da informação, garantindo aos funcionários e prestadores de serviços, que estejam sob sua responsabilidade, condições de trabalho que permitam o seu cumprimento. Caberá a cada líder identificar e relatar à área de segurança da informação eventuais deficiências em seus processos.
- Os processos das áreas de negócio e suporte, relacionados à segurança da informação, devem ser auditados pela auditoria interna, e podem ser auditados pela auditoria externa.
- Toda e qualquer iniciativa ou projeto que envolva recursos de tecnologia ou processamento, armazenamento, envio e recebimento de informações da Viveo, deve ser submetida para análise e aprovação da área de segurança da informação, que irá avaliar o grau de exposição dos riscos na empresa e a aderência junto à política de segurança.
- Os proprietários dos ativos – ex.: recursos de tecnologia, informações, etc. – devem identificar e definir em conjunto a área de segurança da informação, todos os requisitos de segurança existentes para o ativo pelo qual é responsável. Tais requisitos devem estar condizentes com a política de segurança da informação.
- Os proprietários dos ativos devem monitorar se todos os requisitos de segurança existentes sobre o ativo, pelo qual é responsável, estão sendo cumpridos.

5. USO DOS RECURSOS DE TECNOLOGIA

Os recursos de tecnologia utilizados para armazenamento, processamento, recebimento e envio das informações da Viveo devem ser usados exclusivamente para fins de negócio, relacionados aos objetivos e atividades da Viveo. E, devem estar adequadamente protegidos contra ameaças internas e externas, assegurando seu correto funcionamento. Além das políticas e normas, os procedimentos – documentos

operacionais complementares à esta política – para gestão e operação de todos os recursos de tecnologia devem ser seguidos por todos os funcionários, prestadores de serviço e fornecedores.

5.1. COMPUTADORES, NOTEBOOKS E DISPOSITIVOS MÓVEIS

- O uso de computadores, notebooks e dispositivos móveis – dispositivos – é exclusivo para a execução das funções de negócio, relacionadas aos objetivos da Viveo, não podendo serem usados para fins pessoais ou que possam causar danos ao negócio ou a terceiros, tais como roubo ou vazamento de informações, danos à reputação ou imagem da Viveo, envio ou recebimento de arquivos maliciosos ou documentos e softwares licenciados ou protegidos por direitos autorais, bem como causar indisponibilidade dos serviços de negócio.
- As informações de propriedade da Viveo, só podem ser armazenadas ou processadas nos dispositivos de propriedade da Viveo, e só podem ser usadas e compartilhadas conforme sua classificação e o nível de acesso de cada pessoa.
- Para executar as funções corporativas, devem ser usados os dispositivos de propriedade da Viveo, registrados no inventário de tecnologia, atualizados, homologados e autorizados pela área de Tecnologia, não sendo permitido o uso de quaisquer dispositivos pessoais para o processamento e armazenamento de informações de propriedade da Viveo.
- Todo e qualquer acesso aos dispositivos de propriedade da Viveo deve ser identificado (Pessoa) e autenticado (Senha e/ou MFA) e o seu uso é individual e intransferível, não podendo o acesso ser usado ou compartilhado com outra pessoa que não seja o proprietário.
- A cópia de informações para fora das dependências da Viveo ou o uso de mídias removíveis, como por exemplo, HD Externo, Pen Drive e outros, para extrair ou transferir informações devem ser solicitadas e aprovadas pela área de Segurança da Informação.

- Os dispositivos devem ser entregues às Pessoas com todas as configurações padrão de segurança antes que possam ser conectados à rede corporativa para uso, tais como: Antivírus, criptografia dos discos, Baseline de segurança do sistema operacional e todas as atualizações de segurança (Patches). Em caso de falha ou ausência de tais configurações, o recebimento do dispositivo deve ser suspenso.
- É responsabilidade de cada Pessoa cuidar do dispositivo sob sua responsabilidade bem como relatar o quanto antes a perda, o roubo ou o acesso não autorizado ao dispositivo ou às informações da Viveo armazenadas nele.
- Na ausência do responsável ou após cinco minutos de inatividade, a tela do dispositivo deve ser bloqueada, impedindo qualquer acesso não autorizado.
- A troca de informações deve ser restrita e protegida por meio de mecanismos que garantam que as informações confidenciais ou de uso interno da empresa não sejam divulgadas ou repassadas para pessoas não autorizadas, a fim de preservar o sigilo e a integridade.
- Somente a área de tecnologia pode adquirir, instalar, configurar, alterar, movimentar, remover ou desativar os recursos de tecnologia.
- As Pessoas não devem ter expectativa de privacidade no uso dos dispositivos e informações da Viveo e por motivos de segurança da informação e conformidade com esta política, ambos são monitorados.

5.2. ACESSO REMOTO

- O acesso remoto à rede corporativa da Viveo é exclusivo para a execução das funções de negócio, relacionadas aos objetivos da Viveo e só pode ser concedido mediante autorização do gestor do solicitante e da área de segurança da informação.
- Para realizar o acesso remoto, devem ser usados os dispositivos de propriedade da Viveo, registrados no inventário de tecnologia, atualizados,

homologados e autorizados pela área de tecnologia, não sendo permitido o uso de outros dispositivos.

- Todo e qualquer acesso remoto à rede corporativa da Viveo deve ser identificado (Pessoa) e autenticado **obrigatoriamente com duplo fator**, sendo a senha de acesso à rede e o código informado pelo aplicativo *Microsoft Authenticator,* e o seu uso é individual e intransferível, não podendo o acesso ser usado ou compartilhado com outra pessoa que não seja o proprietário.
- Todo e qualquer acesso remoto deve ser protegido por criptografia.

5.3. INTERNET

- A navegação na Internet para acesso à sites ou a qualquer serviço online que é externo à Viveo é exclusiva para a execução das funções de negócio, relacionadas aos objetivos da Viveo, **não podendo serem usados para fins pessoais ou que possam causar danos ao negócio ou a terceiros**, tais como roubo ou vazamento de informações, danos à reputação ou imagem da Viveo, envio ou recebimento de arquivos maliciosos ou documentos e softwares licenciados ou protegidos por direitos autorais.
- Somente é permitido o acesso para a navegação a partir de dispositivos de propriedade da Viveo, e em sites ou serviços seguros – protocolos *https, sftp,* etc. – e confiáveis, que não ofereçam riscos ao negócio da Viveo, sendo responsabilidade de cada Pessoa analisar cuidadosamente o acesso que fará.
- Sites ou serviços online considerados inseguros ou inapropriados para os propósitos de negócio da Viveo serão bloqueados automaticamente. Se for necessária a liberação de qualquer site ou serviço online, deve haver a aprovação da área de Segurança da Informação que fará a avaliação de riscos.
- Informações classificadas como de uso interno ou confidenciais não podem ser enviadas pela Internet, para sites ou qualquer serviço online que não seja de propriedade da Viveo.

- Não é permitido o acesso a serviços de e-mail online que não sejam da Viveo – ex.: Gmail, Yahoo, Outlook, Hotmail, etc. – ou mesmo o envio de quaisquer informações classificadas como de uso interno ou confidenciais.
- Não é permitido o acesso a serviços de armazenamento online que não sejam da Viveo – ex.: OneDrive, Google Drive, Box, Dropbox, etc. – ou mesmo o envio de quaisquer informações classificadas como de uso interno ou confidenciais.
- A troca de informações deve ser restrita e protegida por meio de mecanismos que garantam que as informações confidenciais da empresa não sejam divulgadas ou repassadas para pessoas não autorizadas, a fim de preservar o sigilo e a integridade.
- O acesso à Internet pode ser concedido aos visitantes única e exclusivamente por meio da rede sem fio – Wireless – específica para tal finalidade desde que identificado e autenticado, com data de expiração máxima de oito horas e em concordância com as políticas de uso aceitável deste recurso de Tecnologia.
- As Pessoas não devem ter expectativa de privacidade no uso da Internet para acesso a serviços online, e por motivos de segurança da informação e conformidade com esta política, todos os acessos são monitorados.

5.4. E-MAIL

- O uso do e-mail corporativo da Viveo é exclusivo para a execução das funções de negócio, relacionadas aos objetivos da Viveo, **não podendo ser usado para fins pessoais ou que possam causar danos ao negócio ou a terceiros**, tais como roubo ou vazamento de informações, danos à reputação ou imagem da Viveo, envio ou recebimento de arquivos maliciosos ou documentos e softwares licenciados ou protegidos por direitos autorais.
- Para acesso ao e-mail corporativo, devem ser usados os dispositivos de propriedade da Viveo, registrados no inventário de tecnologia, atualizados,

homologados e autorizados pela área de Tecnologia, não sendo permitido o uso de dispositivos pessoais.

- Somente é permitido o acesso ao e-mail corporativo a partir de dispositivos de propriedade da Viveo, sendo responsabilidade de cada Pessoa analisar cuidadosamente o tipo de conteúdo que será enviado por e-mail, bem como não abrir e-mails, links ou anexos suspeitos, mensagens de pessoas desconhecidas, ou mesmo mensagens não solicitadas.
- Mensagens ou remetentes considerados inseguros ou inapropriados para os propósitos de negócio da Viveo serão bloqueados automaticamente. Se for necessária a liberação de qualquer mensagem ou remetente considerados inseguros, deve haver a aprovação da área de Segurança da Informação que fará a avaliação de riscos.
- Informações classificadas como de uso interno ou confidenciais não podem ser enviadas para fora da Viveo, especialmente para serviços de e-mail online públicos, tais como Gmail, Yahoo, Outlook, Hotmail, etc.
- Todos os anexos, enviados ou recebidos, devem ser analisados quanto ao seu conteúdo a fim de identificar violações desta política, tais como o vazamento de informações, código malicioso que possa prejudicar o negócio, softwares ou documentos protegidos por licenciamento ou direitos autorais.
- Mensagens de e-mail, enviadas ou recebidas, que possuam anexos criptografados ou protegidos por senha serão bloqueados e excluídos caso não seja possível analisar seu conteúdo, a fim de identificar o vazamento de informações de propriedade da Viveo ou outras atividades maliciosas.
- A troca de informações deve ser restrita e protegida por meio de mecanismos que garantam que as informações confidenciais da empresa não sejam divulgadas ou repassadas para pessoas não autorizadas, a fim de preservar o sigilo e a integridade.
- Todas as mensagens de e-mail da Viveo enviadas para destinatários externos devem conter em seu rodapé o seguinte texto: "*Aviso 1: Este e-mail pode conter informações e documentos confidenciais e/ou protegidos por lei. Se você não for o efetivo destinatário, pedimos, por favor, que*

desconsidere completamente o seu conteúdo e os devolva ao seu remetente e os apague imediatamente, ficando proibida a sua cópia e/ou encaminhamento para terceiros." e *"Aviso 2: Apesar da Viveo tomar todas as cautelas necessárias para evitar que nenhum vírus esteja presente nessa mensagem, ela não se responsabiliza por eventuais perdas ou danos eventualmente causados por esse e-mail ou seus anexos."*

- As Pessoas não devem ter expectativa de privacidade no uso do e-mail corporativo da Viveo para o envio, recebimento e armazenamento de mensagens de e-mail, e por motivos de segurança da informação e conformidade com esta política, todos os acessos são monitorados.

6. CLASSIFICAÇÃO E CONTROLE DE ATIVOS

Os ativos de informação devem ser inventariados e classificados, de acordo com os requisitos de confidencialidade, integridade e disponibilidade, e protegidos pelos funcionários, prestadores de serviços ou fornecedores, de acordo com a criticidade que representam para os negócios da Viveo, determinada pela classificação vigente.

- Todos os ativos de informação (hardware e software) devem ser identificados, inventariados e classificados de forma que estejam registrados e atualizados nos recursos adotados para tal finalidade.
- Todas as informações devem ser classificadas de acordo com a importância que representam para o negócio da Viveo e deve ser feita pelo responsável dela, de acordo com as definições deste documento, podendo a área de segurança da informação ser consultada para orientação.
- O processo de classificação da informação deve considerar o impacto de perda de confidencialidade decorrente das possibilidades de compartilhamento e divulgação da informação e o responsável pela informação deve assegurar que as informações e os sistemas recebam os controles de segurança condizentes com a classificação recebida.
- Todas as informações da Viveo devem ser classificadas em uma das três categorias definidas neste documento: CONFIDENCIAL, DE USO INTERNO ou PÚBLICA e de acordo com a criticidade que representam para o negócio.

TIPO	DESCRIÇÃO	COMPETÊNCIA
CONFIDENCIAL	Informações com requisitos de disseminação mais restritos do que as informações DE USO INTERNO. Informações que se reveladas podem causar danos graves e irrecuperáveis de nível político e estratégico, comprometendo os negócios ou a imagem da empresa. Também assegura à empresa a obtenção e manutenção de vantagens competitivas. Exemplos de informações classificadas como CONFIDENCIAL: • Segredo Industrial: Marcas, patentes, receitas, segredos de marca, práticas e metodologias de negócio, fórmulas, etc. • RH: Datas de pagamento, benefícios, salários, dados pessoais, etc. • Regulatória: Assuntos com restrição e disseminação legal, retenção, dados de clientes, etc. • Segurança: Senhas, PINs, tokens**, etc.	• Presidente • Vice-Presidente • Diretores • Gerentes Executivos
DE USO INTERNO	Informações apropriadas para acesso e uso interno da Viveo, e que o acesso deve ser concedido baseado em uma necessidade de negócio. Toda informação que não possuir explicitamente designada uma	• Funcionários em qualquer nível da estrutura organizacional

	categoria deve ser considerada como DE USO INTERNO.	
PÚBLICA	Informação adequada para uso aberto para qualquer pessoa a qualquer instante. Por existirem riscos de negócio insignificantes para este tipo de informação, estas podem ser publicadas abertamente, como, por exemplo, em mídias sociais, campanhas publicitárias, acesso por meio da Internet, ou outros meios de disseminação não autenticáveis. A publicação de informações da Viveo em meios públicos está sujeita às políticas corporativas, além das políticas e normas de segurança da informação.	• Funcionários em qualquer nível da estrutura organizacional e pessoas externas

- Nenhum ativo pode ter sua classificação alterada sem o devido consentimento formal do responsável pela informação ou do líder da área. O responsável pelo ativo poderá solicitar auxílio da área de segurança da informação quando julgar necessário.
- O método de disseminação de informações não deve mudar a classificação destas. A disseminação deve ser realizada de acordo com a classificação do ativo.
- As informações classificadas como CONFIDENCIAL ou DE USO INTERNO, devem ser armazenadas em servidores ou dispositivos da rede corporativa da Viveo. Caberá à área de segurança da informação dirimir sobre dúvidas se determinado dispositivo de armazenamento está apto ou não para esta finalidade.
- A classificação de segurança deve aparecer no início e rodapé de cada documento (exemplo: Documento CONFIDENCIAL)

- As informações classificadas como CONFIDENCIAL ou DE USO INTERNO devem estar protegidas por criptografia quando em repouso – armazenadas – ou quando em trânsito – envio ou recebimento.
- Os documentos impressos devem ser tratados adequadamente, conforme a classificação da informação nele contida.
- Os documentos impressos, classificados como informação CONFIDENCIAL ou DE USO INTERNO, gerados ou não no ambiente da Viveo, devem receber a indicação da respectiva classificação.
- Funcionários devem solicitar autorização para o proprietário do documento, antes de copiar ou imprimir o mesmo, quando classificado como CONFIDENCIAL.
- Documentos impressos classificados como CONFIDENCIAL ou de USO INTERNO, devem ser descartados de maneira segura, como por exemplo, triturando ou destruindo documento, sujeitando-os as políticas e normas de retenção.
- Quando houver suspeita de perda ou revelação de informação classificada como CONFIDENCIAL ou DE USO INTERNO para partes não autorizadas, deve ser iniciado o procedimento de incidente de segurança.

7. GESTÃO DE ACESSO AOS RECURSOS DE TECNOLOGIA

O acesso às informações e recursos de tecnologia da Viveo deve ser concedido somente aos funcionários, prestadores de serviço e fornecedores que possuam uma justificativa válida de negócio para execução de suas funções. A inclusão, exclusão e modificação de acessos ou privilégios deve ser aprovada pelo gestor do solicitante e pelo proprietário do ativo. A revisão frequente deve ser realizada com o intuito de garantir a validade e necessidade dos privilégios concedidos.

7.1. DIRETRIZES GERAIS

- Todos os ativos de tecnologia devem possuir um gestor – proprietário do ativo – responsável pela aprovação das solicitações de concessão de acesso naquele ativo, que deve validar criteriosamente a necessidade de

conceder tal acesso, bem como verificar a existência e a validade do termo de confidencialidade assinado pelo solicitante.

- As contas de acesso – *logins* – são únicas, pessoais e intransferíveis, e devem possuir informações suficientes que identifiquem os seus proprietários. Contas não podem ser compartilhadas, devendo ser protegidas pelo responsável. Se houver qualquer indício de comprometimento, a conta deve ser bloqueada até que a senha seja alterada.
- As senhas iniciais ou primeira senha devem obrigatoriamente serem alteradas pelo proprietário no momento do recebimento.
- As senhas devem ser complexas, possuindo o tamanho mínimo de dez caracteres compostos por letras (maiúsculas e minúsculas), números e símbolos.
- O tempo de vida de uma senha deve ser no mínimo um dia e no máximo quarenta e cinco dias, não podendo ser reutilizadas em hipótese alguma.
- Os sistemas devem fazer uso de perfis de acesso, de maneira que as funções sejam atribuídas a eles e não diretamente às contas de acesso ou usuários.
- Todas as contas padrão dos sistemas devem ser desabilitadas e terem suas informações de nome e senha, alteradas.
- Após cinco tentativas de autenticação sem sucesso, a conta deve ser bloqueada e só pode ser liberada para uso mediante a verificação de identidade do solicitante.
- Toda concessão de acesso deve ser validada perante a matriz de combinações tóxicas ou de conflitos de interesses.
- Devem usar duplo fator de autenticação todas as contas usadas para acesso privilegiado, acesso remoto à rede e acesso às aplicações publicadas na internet.
- Devem ser bloqueados temporariamente todos os funcionários e terceiros que estiverem de férias ou em licença formal superior a noventa, enquanto durar o período da ausência.

- As contas que não estiverem em uso por mais de noventa dias, devem ser bloqueadas automaticamente.
- Funcionários e terceiros desligados devem ter seus acessos revogados no momento do desligamento ou distrato.

7.2. PRESTADORES DE SERVIÇOS E FORNECEDORES

- Todos os contratos de prestação de serviços com terceiros devem possuir um gestor responsável – gestor de contrato – que deve validar criteriosamente a necessidade de concessão de acessos para prestadores de serviços e fornecedores, bem como a validade do termo de confidencialidade contratual e para cada terceiro.
- O acesso concedido aos prestadores de serviços e fornecedores não pode ultrapassar o período contratual e deve expirar em no máximo noventa dias, de maneira que sejam revisados e certificados após este período.

7.3. CONTAS PRIVILEGIADAS

- Contas de acesso privilegiado devem ser concedidas exclusivamente para o funcionário que desempenhe a função de administração dos ativos de tecnologia e devem ser rigorosamente controladas. (colocar as exceções devido a características do nosso ambiente).
- Devem ser criadas contas separadas – diferente daquelas usadas para o trabalho diário – com o propósito específico de administração dos ativos de tecnologia. A nomenclatura deve ser definida de maneira que não caracterize o propósito administrativo. Todas as contas com privilégio administrativo devem usar duplo fator de autenticação obrigatoriamente em todas os acessos realizados.
- O funcionário deve realizar a solicitação para criação da conta, que será aprovada pelo gestor imediato, pelo proprietário do ativo e por último pelo diretor de tecnologia, e em seguida, executada pela área de segurança da informação. Na solicitação deve ser anexado o termo de responsabilidade para contas privilegiadas, que descreve quais são os privilégios daquela

conta, qual o propósito deste acesso para o funcionário solicitante e quais são os outros funcionários que já possuem o mesmo acesso no momento da solicitação. Senhas das contas privilegiadas ou contas de serviço devem ser complexas, possuindo o tamanho mínimo de 20 caracteres compostos por letras, números e símbolos.

- O acesso privilegiado concedido aos funcionários deve ser revisado e certificado quanto à sua necessidade a cada noventa dias.

7.4. CONTAS DE SERVIÇOS

- Contas de acesso para serviços, sistemas ou aplicações devem ser concedidas exclusivamente para o uso, identificação e concessão de privilégios para aquele serviço, sistema ou aplicação.
- Devem ser criadas contas separadas – diferentes para cada sistema, serviço ou aplicação – com o propósito de identificação e concessão de privilégios. A nomenclatura deve ser definida de maneira que identifique que se trata de um serviço, bem como qual serviço exatamente.
- Para serviços, sistemas e aplicações, a solicitação é feita pelo próprio proprietário do ativo, aprovada pelo diretor de tecnologia, e em seguida, executada pela área de segurança da informação. Na solicitação deve ser anexado o termo de responsabilidade para contas de serviços, que descreve quais são os privilégios daquela conta, qual o propósito deste acesso para o sistema e validade.
- Senhas das contas privilegiadas ou contas de serviço devem ser complexas, possuindo o tamanho mínimo de 20 caracteres compostos por letras, números e símbolos.
- O acesso concedido aos serviços, sistemas e aplicações deve ser revisado e certificado quanto à sua necessidade a cada doze meses.

7.5. REVISÃO FREQUENTE DOS ACESSOS

- A revisão dos acessos é obrigatória e deve ser realizada pelo time de segurança da informação com validação do usuário, gestor da área e do proprietário do ativo. A frequência da revisão depende do tipo da conta.

8. SEGURANÇA FÍSICA DO AMBIENTE

- Os recursos e instalações de processamento de informações críticas para o negócio da Viveo devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e recursos para controle de acesso.
- Todos os locais que contenham recursos considerados críticos para o negócio da Viveo devem estar segregados fisicamente das demais localidades e protegidos contra desastres físicos e ambientais. A classificação dos riscos deve ser conhecida pelos funcionários que possuem acesso aos mesmos. E, não devem estar indicados em mapas, placas ou qualquer outro meio de comunicação que possa informar a sua localização a pessoas não autorizadas.
- Todos os locais que contenham recursos considerados críticos para as atividades e negócios da Viveo devem ser mantidos de forma segura, com seu acesso restrito por meio de sistemas de controle de acesso e monitoração em regime 24x7 (vinte e quatro horas por dia e sete dias por semana).
- Os locais destinados a armazenar recursos críticos não devem estar próximos de outros que apresentem grandes probabilidades de riscos de acidentes, como depósitos de combustíveis. E, devem ser protegidos contra potenciais ameaças, como inundações, incêndios, invasão, furto, vandalismo, agentes químicos ou qualquer outro tipo de ameaça.
- O acesso aos locais que contenham recursos considerados críticos para as atividades da Viveo deve ser concedido pelo responsável da operação dos Data Centers e salas técnicas, de acordo com as necessidades dos funcionários, prestadores de serviços ou fornecedores para execução de

suas tarefas. A permissão de acesso deve ser concedida por um período ou cargo definido.

- Todo acesso realizado pelos funcionários, prestadores de serviços ou fornecedores aos locais restritos, os quais contêm recursos considerados críticos, devem ser registrados. Tais registros devem conter informações como a identificação do usuário, data e hora da entrada e saída.
- Os registros e procedimentos de visitas realizadas aos locais restritos, bem como as permissões de acesso concedidas aos mesmos, devem ser periodicamente revisados pelos responsáveis pela operação dos Data Centers e salas técnicas, e pela auditoria interna. Não conformidades devem ser corrigidas e reportadas para o gestor da área.
- O acesso de prestadores de serviços e fornecedores aos locais restritos deve ser acompanhado por funcionários autorizados.
- Os pontos de rede não utilizados devem ser desabilitados ou terem o seu acesso controlado por autenticação.

9. DESENVOLVIMENTO DE SOFTWARE

Os sistemas ou aplicações – sistemas – desenvolvidos internamente, por prestadores de serviços ou fornecedores de software de mercado, devem atender aos requisitos de segurança da informação especificados pelas políticas e normas de segurança da informação. Os requisitos devem ser aplicados durante toda o ciclo de vida dos sistemas: arquitetura e engenharia, desenvolvimento e implantação.

- Todos os sistemas devem ser identificados e registrados com todas as suas informações no catálogo de sistemas e terem um proprietário atribuído.
- Todos os controles necessários para contribuir com a segurança dos sistemas devem ser identificados durante a fase de planejamento – desenvolvimento ou aquisição – e introduzidos durante ciclo de vida do sistema. É responsabilidade das áreas de sistemas, em conjunto com a área de segurança da informação, identificar e introduzir esses controles.
- Em fase de desenvolvimento, durante a codificação do sistema, o código fonte deve ser analisado quanto à existência de vulnerabilidades, que

devem ser corrigidas ainda em ambiente de desenvolvimento, antes de serem implantadas em ambiente de homologação ou testes.

- Em fase de homologação, durante os testes, o sistema deve ser analisado quanto à existência de vulnerabilidades no seu funcionamento, que devem ser corrigidas ainda em ambiente de homologação, antes de serem implantadas em ambiente de produção.
- Os sistemas só podem ser implantados em serviços de infraestrutura – servidores, plataformas, clouds, etc. – que estejam homologados pela área de infraestrutura e que possuam as configurações padrão de segurança.
- Devem existir ambientes separados para desenvolvimento, homologação e produção dos sistemas. Os ambientes devem estar segregados por servidores, domínios ou diretórios e as mudanças somente deverão ser efetuadas seguindo procedimentos de gestão de mudanças definidos pela área de governança.
- É proibido o uso de dados de ambiente de produção no processo de homologação dos sistemas, que só pode ser realizado com dados mascarados ou fictícios, sem prejuízo para a homologação e integridade das funções desempenhadas pelo sistema.
- Todos os sistemas devem possuir trilhas de auditoria para as transações ou funções críticas, a serem definidas pelo proprietário do sistema e a área de auditoria interna. Os eventos gerados devem ser enviados em formato padronizado para um repositório ou serviço centralizado e devem ser protegidos quanto à sua confidencialidade e integridade.
- Todos os dados que forem incluídos no sistema devem ser validados antes da inclusão ser efetivada. O processo de validação deve verificar valores fora dos limites esperados, existência de caracteres inválidos, dados incompletos, informações inconsistentes, formato incorreto, dentre outros critérios que devem ser determinados pelas áreas de sistemas e segurança da informação.
- Todos os sistemas devem possuir um mecanismo para identificação e autenticação dos usuários que o utilizam. Os sistemas de uso público, que

estão abertos na internet, devem fazer uso de autenticação de duplo fator, caso usem informações confidenciais ou de uso interno.

- Os sistemas devem atender a todos os requisitos de gestão de controle de acesso.
- As informações confidenciais ou de uso interno que estejam em repouso – armazenados em discos, arquivos, bancos de dados, etc. – ou em trânsito devem estar protegidas por criptografia.
- As chaves criptográficas utilizadas devem ser protegidas, de forma que somente os funcionários autorizados pela área de segurança da informação tenham acesso. A utilização de chaves criptográficas deve ser controlada e formalizada e não podem ser compartilhadas com pessoas não autorizadas.
- Só podem ser utilizadas as bibliotecas ou componentes de terceiros que estejam homologadas pela área de sistemas e aprovadas pela área de segurança da informação.

10. PROTEÇÃO DA INFRAESTRUTURA DE TECNOLOGIA

Todas as tecnologias – hardware e software – usados para o armazenamento, processamento ou transmissão de informações da Viveo devem possuir um padrão mínimo de configuração – *baseline* – que diminua o risco violação da confidencialidade, integridade ou disponibilidades das informações e recursos de tecnologia.

- Todas as tecnologias – hardware e software – usados para o armazenamento, processamento ou transmissão de informações da Viveo devem estar registradas nos respectivos inventários e possuírem um *baseline* associado.
- Antes que estejam em produção, os recursos de tecnologia devem possuir o *baseline* associado implementado e validado.
- Devem ser implementados mecanismos que regularmente assegurem que os *baselines* estejam em conformidade com o padrão que é estabelecido para cada tecnologia.

- Recursos de tecnologia sem conformidade com o baseline estabelecido devem ser desativados, removidos da rede produtiva e regularizados antes que possam ser usados novamente em ambiente produtivo.
- Os baselines devem ser revisados anualmente ou quando houver qualquer fato relevante que altere a análise prévia de riscos daquela tecnologia ou recurso.

11. CÓPIAS DE SEGURANÇA (*BACKUP*)

Todas as informações críticas utilizadas nas operações da Viveo devem possuir cópias de segurança. A área de infraestrutura e banco de dados é responsável pela realização das cópias de segurança das informações e recursos de tecnologia.

- As cópias de segurança devem atender aos requisitos operacionais, legais, históricos e de auditoria.
- A periodicidade com a qual são realizadas as cópias de segurança serão definidas de acordo com o grau de importância da informação, pelo proprietário da mesma em conjunto com a área de segurança da informação e a área de sistemas e infraestrutura. Backups automatizados devem ser formalmente planejados e documentados.
- As cópias de segurança programadas regularmente devem ser executadas em períodos de menor impacto para o ambiente.
- Devem ser realizados testes regulares, a cada seis meses e ao término do processo de backup, com as cópias de segurança, para assegurar que as informações possam ser restauradas quando necessário.
- É de responsabilidade da área de infraestrutura realizar os testes de restauração com as informações.
- O procedimento para restauração das cópias de segurança deve estar formalmente documentado. Esse procedimento deve ser elaborado pela equipe de infraestrutura e banco de dados em acordo com o proprietário da informação.

- O processo de restauração das cópias de segurança deve seguir os procedimentos aprovados pelo proprietário da informação e pela Gerência de Segurança da Informação.
- A restauração das cópias de segurança deve ser feita somente mediante aprovação do proprietário da informação ou quando o procedimento de produção prever este fato.
- As cópias de segurança devem ser armazenadas de forma segura, distante das instalações físicas onde se encontram os servidores a partir dos quais foram geradas as cópias de segurança.
- O período de retenção das cópias de segurança dependerá do tipo de informação armazenada e da existência de legislação específica. Esse período deve ser determinado pelo proprietário da informação em conjunto com a área de segurança da informação, e deve ser revisado pela área jurídica, fiscal e controladoria, conforme sua natureza.
- Durante a gravação das cópias de segurança, a trilha de auditoria do sistema aplicativo utilizado para a finalidade deve estar ativa, a fim de possibilitar o registro das falhas ocorridas.
- Antes de serem realizadas alterações significativas nos sistemas operacionais, sistemas ou banco de dados ou quaisquer outros serviços e recursos, devem ser realizadas cópias de segurança deles.
- As mídias utilizadas para realização das cópias de segurança devem ser periodicamente substituídas, conforme as orientações fornecidas pelo fabricante. As informações devem ser gravadas em mídias que possuam um período de vida útil igual ou maior do que o período de retenção.
- As cópias de segurança das informações devem estar disponíveis quando solicitadas, conforme os prazos definidos nos procedimentos previamente acordados. As informações devem ter no mínimo duas cópias de segurança armazenadas em locais distintos, juntamente com a documentação dos procedimentos de recuperação delas.
- As áreas jurídicas, fiscal ou controladoria devem colaborar, quando consultadas pelo proprietário da informação ou pela área de segurança da

informação, na classificação das informações e na determinação do período de retenção destas, de acordo com a legislação vigente.

- As normas de retenção, para qualquer cópia de informação, devem ser reavaliadas seguindo as mudanças que possam ocorrer na classificação das informações.

12. GESTÃO DE TERCEIROS

Todos os prestadores de serviços e fornecedores – Terceiros – devem ser mapeados e avaliados quanto ao risco que ofereçam ao negócio da Viveo.

- Os Terceiros que tenham acesso aos recursos de tecnologia ou informações da Viveo devem estar mapeados e inventariados com todas as informações pertinentes à identificação e prestação de serviços. Ainda, devem possuir um contrato vigente com cláusulas de confidencialidade, aceitação formal das políticas e normas – pessoa jurídica e cada pessoa física.
- O treinamento de segurança da informação precisa ser realizado por todos os Terceiros e regularmente para aqueles cuja prestação de serviços é superior a doze meses.
- O acesso aos recursos de tecnologia e informações da Viveo só pode ser concedido após a aprovação de todos os envolvidos no processo de concessão.
- Uma análise de riscos de segurança da informação será realizada pela área de segurança da informação para aprovação final da concessão de acessos aos recursos de tecnologia e informação da Viveo.

13. TESTES DE SEGURANÇA DA INFORMAÇÃO

Testes de segurança da informação devem ser realizados com o intuito de descobrir vulnerabilidades nos recursos de tecnologia.

- Simulações **externas** contra os recursos de tecnologia devem ser realizadas semestralmente com o intuito de detectar vulnerabilidades que possam ser exploradas.
- Simulações **internas** contra os recursos de tecnologia devem ser realizadas semestralmente com o intuito de detectar vulnerabilidades que possam ser exploradas.
- Os testes de segurança devem ser realizados por uma entidade independente. Os resultados dos testes devem ser avaliados e aprovados pelas áreas de tecnologia e segurança da informação, que produzirá um plano de ação para as vulnerabilidades que venham a ser encontradas.
- A auditoria interna deve acompanhar a implementação do plano de ação que corrigirá as vulnerabilidades encontradas e um novo teste deve ser realizado com o intuito de validar a as correções, fechando o ponto de auditoria.

14. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de segurança devem ser tratados conforme processo e procedimentos estabelecidos para a detecção e análise, contenção e erradicação, revisão posterior e plano de ação. Funcionários, prestadores de serviços e fornecedores devem comunicar os incidentes de segurança em que estejam envolvidos ou que presenciem. A omissão deles será considerada uma violação de segurança, sendo que estas podem incorrer em penalidades previstas nas políticas e normas de segurança da informação.

- Os procedimentos para o tratamento de incidentes devem estar estabelecidos e serem atualizando semestralmente.
- Deve ser estabelecido o time de resposta à incidentes e os funcionários devem estar treinados quanto aos procedimentos para o tratamento de incidentes de segurança da informação. O time de resposta à incidentes deve estabelecer canais de comunicação com outros grupos, internos (ex.: Jurídico, Relações Públicas, Recursos Humanos e Tecnologia) e externos (ex.: agências de investigação e regulatórias).

- A revisão dos incidentes ocorridos e o plano de ação deve ser validado e acompanhado até a sua implementação pela área de auditoria interna.

15. CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Funcionários, prestadores de serviços e fornecedores que tenham acesso às informações ou recursos de tecnologia da Viveo devem ser treinados e conscientizados regularmente quanto à segurança da informação, para que conheçam as diretrizes necessárias e fundamentais sobre como desempenhar um papel ativo na proteção das informações e recursos tecnológicos da Viveo, com o intuito final de protegê-los, garantindo um ambiente seguro e confiável para o negócio.

- Os funcionários devem ser treinados na admissão e regularmente, a cada doze meses. Ao fim dos treinamentos deve ser registrada a participação e resultado da avaliação, que tem o intuito exclusivo de medir a absorção de conhecimento.
- Prestadores de serviços e fornecedores, que tenham acesso a informação e recursos de tecnologia da Viveo devem ser treinados antes de iniciar a prestação ou fornecimento de serviços e durante o período contratual, regularmente, a cada doze meses.
- A área de segurança da informação deve conduzir regularmente a simulação de situações de risco, com o intuito de avaliar a aderência e conformidade com as políticas e normas de segurança da informação, que irá avaliar os resultados e tomar as providências cabíveis.
- Caso as simulações apresentem reincidência de não conformidades, o usuário poderá ter o acesso suspenso temporariamente, à informação ou recursos de tecnologia.

16. REGISTRO E MONITORAMENTO

Os eventos relevantes para auditoria – logs – devem ser coletados, armazenados e protegidos durante o seu ciclo de vida (geração, transmissão, armazenamento, alertas, descarte), de forma a antecipar determinadas situações ou realizar investigações, e que

demonstre o que aconteceu, quais sistemas foram afetados, quando aconteceu e os envolvidos.

- Todos os ativos de tecnologia devem estar sincronizados com servidor de horário, através do protocolo NTP, de forma que os registros possam ser devidamente sequenciados mesmo que originados em diferentes fontes.
- Todos os ativos devem possuir a função de registro das atividades realizadas, que devem ser enviadas e armazenadas em servidor centralizado e para esta finalidade.
- Quando possível, os registros devem ser enviados em formato padronizado, preferencialmente JSON.
- Devem ser registrados minimamente os eventos: inicialização, reinício e desligamento de sistemas operacionais ou serviços, alterações ou falha nas conexões de rede, tentativa de alterações nos controles ou configurações de segurança (sucesso ou falha), tentativas de logon (sucesso ou falha), quaisquer alterações nas contas de usuários ou serviços, todas as ações executadas após login com sucesso, toda a atividade de contas privilegiadas ou de serviço.
- Para cada um dos eventos mencionados, devem ser coletados os seguintes dados: o evento em si, código de falha ou sucesso, status, identificação da conta (usuário ou sistema) e tipo de credencial usada, identificação do ativo e serviço utilizado para executar tal ação, data e hora (timestamp), endereços IP de origem e destino quando aplicável, tipo de cliente (ex.: navegador, terminal, etc.) e identificação da sessão.
- Os eventos armazenados devem ser protegidos contra acesso e alterações não autorizados, mantendo sua confidencialidade e integridade.
- Todos os eventos devem ser armazenados por um período mínimo de seis meses para consulta instantânea e posteriormente arquivados por um período adicional de dozes meses para consulta em até duas horas.
- Os eventos devem ser analisados, correlacionados e criados alertas de monitoramento com a finalidade específica de avisar sobre determinadas circunstâncias que tragam riscos à Viveo.

- Mensalmente devem ser revisados todos os eventos gerados em busca de atividades suspeitas ou ativos não autorizados que eventualmente estejam em operação no ambiente da Viveo.

17. EXCEÇÕES ÀS POLÍTICAS E NORMAS DE SEGURANÇA DA INFORMAÇÃO

As exceções às políticas e normas de segurança da informação devem ser submetidas à avaliação da área de segurança da informação e se necessário, submetidas ao comitê de segurança da informação para que sejam adequadamente tratadas.

- A área de segurança da informação define os procedimentos a serem seguidos para o envio de exceções às políticas e normas de segurança da informação ao Comitê de Segurança da Informação para análise.
- As solicitações para exceções às políticas e normas de segurança da informação devem ter uma justificativa de negócio documentada, e necessitam ser formalmente aprovadas pela área de segurança da Informação ou, quando for o caso, pelo Comitê de Segurança da informação para serem consideradas válidas. Uma vez aprovadas, as exceções às políticas serão válidas pelo período máximo de um ano e, no final desse período, serão reavaliadas quanto à sua relevância para o negócio.
- A área de segurança da informação avaliará quais controles adicionais devem ser adotados para reduzir os riscos decorrentes da exceção. Todas as exceções documentadas devem ser analisadas e consideradas em revisões futuras da política.
- O responsável pela exceção deve avaliar formalmente os riscos registrando a aceitação dos riscos decorrentes. A área de segurança da informação e a auditoria Interna revisarão periodicamente as avaliações de riscos.

18. PENALIDADES

Os funcionários, prestadores de serviços e fornecedores que violarem as políticas e normas de segurança da informação estão sujeitos às penalidades definidas no

Procedimento de Gestão de Consequências e Medidas Disciplinares e/ou demais normas ou leis aplicáveis.

- A violação a um controle de segurança ou a não-aderência às políticas e normas de segurança da informação e suas definições serão consideradas faltas graves, podendo ser aplicadas penalidades aos seus responsáveis, dependendo da gravidade e dos danos causados, de acordo com o Procedimento de Gestão de Consequências e Medidas Disciplinares, definido e gerido pelo departamento de Recursos Humanos. Além das medidas descritas no Procedimento de Gestão de Consequências e Medidas Disciplinares, outras medidas preventivas podem ser aplicadas, tais como:

➢ Perda temporária de acesso privilegiado a determinados recursos;

➢ Desativação das contas de senhas.

- A área de recursos humanos em conjunto com a área jurídica e a área de segurança da informação devem ser acionadas para apoiar na ponderação das penalidades a serem aplicadas, decorrentes de violações nas políticas e normas de segurança da informação de acordo com o impacto causado na Viveo.

19. RESPONSABILIDADES

A presente Política é de responsabilidade da área de Segurança da Informação.

20. HISTÓRICO DE REVISÕES

VERSÃO	RESPONSÁVEL PELA ELABORAÇÃO	RESPONSÁVEL PELA APROVAÇÃO	DATA DA APROVAÇÃO	PERIODICIDADE
V1	Segurança da Informação	Comitê de Auditoria, Gestão de Riscos e Compliance; Conselho de Administração	Fevereiro/2024	Anual