

Política de Segurança da Informação

POL.SGSI.001

2.0

SUMÁRIO

1	Objetivo.....	4
2	Abrangência.....	4
3	Documentação relacionada.....	4
4	Definições.....	4
5	Descrição da Política	4
5.1	Princípios e Diretrizes	5
5.2	Papéis Responsabilidades	5
5.2.1	Diretoria /CISO.....	5
5.2.2	Colaboradores, Estagiários e terceiros	5
5.2.3	Gestores e Líderes de área.....	6
5.2.4	Proprietario da informação	6
5.2.5	Comitê SGSI	6
5.2.6	Governança Operacional e Estratégica.....	7
5.2.7	Jurídico	7
5.2.8	Recursos Humanos.....	7
5.3	Classificação da Informação.....	7
5.4	Acesso Lógicos e Físicos	8
5.5	Segurança Operacional.....	8
5.6	Gestão de incidentes de Segurança da Informação	9
5.7	Gestão de Riscos	9
5.8	Gestão de Fornecedores	9
5.9	Continuidade de Negócios.....	9
5.10	Conscientização e Treinamentos	9
5.11	Conformidade, auditoria e melhoria contínua.....	9
6	Penalidades.....	9
7	Anexo	10

Matriz de Responsabilidades

Atividades	Alta Direção	Comitê SGSI	Governança	Colaboradores
Aprovar e apoiar a divulgação da Política de Segurança da Informação	A	I	R	-
Revisão da Política de Segurança da Informação	C	C	R	-
Publicar e comunicar a Política de Segurança da Informação			R	I

Histórico de Versão

Versão	Data	Motivo da revisão	Elaborado por	Aprovado por
1.0	22/05/2025	Versão Inicial	Governança Caio Nunes	Joaquim de Almeida Ferraz Junior
1.1	15/05/2025	Ajuste de capa, controle, matriz e introdução	Governança Caio Nunes	Joaquim de Almeida Ferraz Junior
1.2	13/11/2025	Ajuste de capa, controle, matriz e introdução	Governança Caio Nunes	Joaquim de Almeida Ferraz Junior
2.0	11/06/2026	Nova estrutura template, integração Vita e Cyber, revisão do conteúdo.	Talita Carvalho Governança	Joaquim de Almeida Ferraz Junior Governança

1 OBJETIVO

Este documento tem como objetivo estabelecer diretrizes e princípios para proteger os ativos de informação da **Vivo VITA**, garantindo a confidencialidade, integridade e disponibilidade, bem como assegurar a conformidade com requisitos legais, regulatórios e normativos, incluindo a ISO/IEC 27001.

2 ABRANGÊNCIA

Este documento apresenta um conjunto de diretrizes, requisitos e boas práticas que devem ser cumpridas por:

- Todos os colaboradores, estagiários e terceiros;
- Fornecedores e parceiros com acesso à informação;
- Todos os ambientes físicos e digitais da Vivo VITA;
- Todos os ativos de informação, incluindo sistemas, dados e infraestrutura;

3 DOCUMENTAÇÃO RELACIONADA

- Norma ISO/IEC 27001:2022
- Norma ISO/IEC 27002:2022

4 DEFINIÇÕES

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação. Além disso, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Backup: refere-se ao armazenamento da cópia de segurança de dados para ser utilizada na recuperação de informações sempre que necessário. O backup tem por finalidade restaurar as informações de forma íntegra visando garantir a continuidade do trabalho.

Classificação da Informação: processo de identificar e definir níveis de proteção adequados para as informações, que garantam a sua confidencialidade, integridade e disponibilidade, de acordo com o seu grau e importância para a organização.

Incidente de Segurança da Informação: um ou múltiplos eventos de Segurança da Informação (SI) indesejados, que podem comprometer as operações do negócio e ameaçar a segurança da informação.

Privacidade de dados: direito à confidencialidade de dados de um indivíduo, mantendo-os reservados e limitando o acesso para a finalidade para a qual os dados são fornecidos.

Comitê SGSI: um grupo multidisciplinar que reúne representantes de diversas áreas da empresa e atua nas definições e direcionamentos sobre o escopo do Sistema de Gestão de Segurança da Informação (SGSI).

5 DESCRIÇÃO DA POLÍTICA

A **Vivo VITA** estabelece um Sistema de Gestão de Segurança da Informação (SGSI), comprometendo-se a:

- Proteger informações contra acessos não autorizados, divulgação indevida ou perda;
- Garantir que a informação esteja disponível quando necessária;
- Implementar controles de segurança adequados ao nível de criticidade;
- Promover a conscientização contínua de todos os colaboradores;
- Atender requisitos legais, regulatórios e contratuais;
- Melhorar continuamente os processos de segurança;

5.1 PRINCÍPIOS E DIRETRIZES

A Segurança da Informação na **Vivo VITA** é orientada pelos seguintes princípios:

- Confidencialidade: garantir que a informação seja acessada apenas por pessoas autorizadas;
- Integridade: assegurar que as informações sejam mantidas integras, sem alterações indevidas ;
- Disponibilidade: garantir que usuários autorizados tenham acesso às informações sempre que necessário;
- Privacidade: proteção de dados pessoais conforme a LGPD;
- Gestão baseada em riscos: identificação, avaliação e tratamento contínuo de riscos;
- Melhoria contínua: evolução permanente do SGSI por meio do ciclo PDCA.

Todas as informações devem ser protegidas conforme esta Política, sendo a segurança da informação uma prioridade contínua em todas as áreas da **Vivo VITA**, a fim de reduzir riscos e evitar danos à empresa e a terceiros.

As informações produzidas ou recebidas no exercício das atividades profissionais pertencem à organização, incluindo os recursos e equipamentos utilizados, salvo exceções formalizadas em contrato. O uso pessoal de recursos de TI não é permitido no ambiente do SOC **Vivo VITA**.

A empresa poderá monitorar o uso de sistemas e serviços para garantir a segurança e a disponibilidade das informações.

5.2 PAPÉIS RESPONSABILIDADES

A seguir, estão descritas as responsabilidades e obrigações atribuídas a cada função dentro da **Vivo VITA**:

5.2.1 Diretoria /CISO

- Prover os recursos necessários para garantir a eficácia do grupo SGSI;
- Aprovar a composição do Comitê SGSI da **Vivo VITA**;
- Assessorar o Comitê SGSI quanto a qualquer decisão relacionada ao Sistema de Gestão de Segurança da Informação (SGSI);
- Apoiar as políticas, as diretrizes e as normas do Sistema de Gestão de Segurança da Informação da **Vivo VITA**;
- Receber relatórios de violações da política, diretrizes e das normas do SGSI da **Vivo VITA** quando aplicável;
- Receber relatórios e acompanhar as não conformidades identificadas no ambiente;
- Realizar a análise crítica do SGSI e propor melhorias nos processos, com o objetivo de promover a melhoria contínua;

5.2.2 Colaboradores, Estagiários e terceiros

- São responsáveis por proteger as informações da organização, garantindo sua confidencialidade, integridade e disponibilidade;
- Devem utilizar os recursos disponibilizados exclusivamente para fins profissionais, cumprir as normas e leis aplicáveis, e formalizar o compromisso com a segurança da informação por meio do termo de confidencialidade;
- Participar das ações de conscientização e manter-se atualizado sobre boas práticas;
- Em caso de dúvidas, devem buscar orientação com o superior imediato ou a equipe de Governança;
- Qualquer incidente, vulnerabilidade ou descumprimento da política deve ser comunicado imediatamente, contribuindo para a melhoria contínua do ambiente de segurança da informação;

5.2.3 Gestores e Líderes de área

- As lideranças e responsáveis por áreas devem garantir o cumprimento e a disseminação da Política, normas e procedimentos do SGSI, assegurando que suas equipes tenham pleno conhecimento e entendimento dessas diretrizes.
- Devem atuar de forma proativa na identificação, documentação e melhoria de processos, além de apoiar a elaboração e atualização de normas quando solicitado.
- Também é sua responsabilidade manter evidências dos processos, comunicando prontamente quaisquer violações à equipe de Governança.
- Cabe ainda incentivar a adesão às práticas de segurança, gerenciar procedimentos sob sua responsabilidade e incorporar requisitos de segurança da informação e continuidade de negócio em projetos, protegendo os ativos e interesses da organização.

5.2.4 Proprietário da informação

O proprietário da informação é o colaborador ou responsável que decide sobre a finalidade, o conteúdo e o seu uso, garantindo a proteção e o uso adequado das informações.

Cabe a ele definir a classificação, aprovar e revisar acessos, orientar quanto ao uso das informações e assegurar que controles apropriados sejam aplicados ao longo de todo o seu ciclo de vida.

5.2.5 Comitê SGSI

- Responsável por aprovar políticas, normas e procedimentos de Segurança da Informação,
- Apoiar a gestão de riscos (avaliação, tratamento e aceitação) e garantir o alinhamento entre os objetivos organizacionais, tecnológicos e de segurança.
- Acompanhar os indicadores e auditorias, na definição e monitoramento de planos de ação, além de servir como fórum de decisão e alinhamento entre as áreas, assegurando a governança e a conformidade do SGSI.

5.2.6 Governança Operacional e Estratégica

- Responsável por consolidar, manter e evoluir o SGSI, garantindo o alinhamento com os objetivos estratégicos e requisitos legais da organização.
- Atuar na definição de políticas, gestão de riscos, acompanhamento de indicadores e auditorias, assegurando a conformidade e a eficácia dos controles de segurança da informação.
- Coordenar as atividades do SGSI e apoiar as instâncias de governança, contribuindo com informações para a tomada de decisão.
- Promover, quando necessário, ações de conscientização, treinamentos e iniciativas de melhoria contínua, além de acompanhar requisitos normativos e regulatórios aplicáveis, assegurando a atualização contínua do Sistema de Gestão de Segurança da Informação (SGSI).

5.2.7 Jurídico

- Manter as áreas da **Vivo Vita** informadas sobre eventuais alterações legais, regulatórias e de privacidade que impliquem responsabilidade e ações envolvendo o Sistema de Gestão de Segurança da Informação;
- Incluir na análise e elaboração de contratos de clientes, fornecedores, prestadores de serviços e parceiros de negócio, sempre que necessário e quando aplicável, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da organização;
- Avaliar, quando solicitado pelas áreas ligadas ao tema, as políticas, as diretrizes, as normas e procedimentos do Sistema de Gestão de Segurança da Informação da **Vivo Vita**.

5.2.8 Recursos Humanos

- São responsáveis por apoiar a Segurança da Informação por meio da gestão do ciclo de vida dos colaboradores, garantindo comunicação adequada sobre mudanças no quadro funcional e o controle de acessos, assim como colaborar na concessão e revogação de acessos conforme o perfil do colaborador.
- Devem assegurar que novos colaboradores recebam treinamento de segurança no onboarding e formalizem ciência das políticas e normas do SGSI.
- Promover campanhas de conscientização e avaliam sua eficácia, além
- Adicionalmente, apoiar a investigação de incidentes relacionados a comportamento inadequado, em conjunto com as áreas responsáveis, quando necessário.

5.3 CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações devem ser classificadas para indicar a necessidade, a prioridade e o nível de proteção aplicável. Essa classificação e sua rotulagem devem ser realizadas pelo Proprietário da Informação, que será responsável por mantê-la atualizada.

A classificação define requisitos de acesso, armazenamento, compartilhamento, retenção e descarte, conforme a importância para o negócio.

Foram definidos quatro (4) níveis de classificação de informações:

- **CORPORATIVO (USO INTERNO)**

Informações cuja divulgação, alteração ou indisponibilidade cause danos menores à reputação ou um pequeno impacto operacional. Ex.: Procedimentos, instruções técnicas, etc.

- **RESTRINGIDO**

Informações cuja divulgação, alteração ou indisponibilidade tenha um impacto significativo nas operações ou objetivos de negócios, nos interesses da Empresa, de seus clientes ou associados e funcionários. Ex.: Documentos técnicos de configurações de segurança, atas de comitês, etc.

- **RESERVADO**

Informação cuja divulgação, alteração ou indisponibilidade tenha um impacto grave nos objetivos de negócio ou coloque em risco a sobrevivência da Organização. Ex.: projetos em desenvolvimento, decisões estratégicas, oportunidades de negócios, etc.

- **PÚBLICO**

Informações que não são consideradas abrangidas pelas definições acima referidas e cuja divulgação, alteração ou indisponibilidade não implica danos. Ex.: Informações emitidas pela Área de Comunicação, fatos da Empresa comunicados pela Secretaria Geral, resumo das contas anuais publicadas pela Área Financeira, campanhas e promoções lançadas pela Área de Marketing, etc.

5.4 ACESSO LÓGICOS E FÍSICOS

O acesso às informações e sistemas deve obedecer ao princípio do menor privilégio, garantindo rastreabilidade, revisão periódica de acessos e segregação de funções.

A criação e gestão de contas de usuários devem seguir procedimentos específicos, sendo garantido que cada colaborador possua uma conta institucional única, pessoal e intransferível.

O uso do correio eletrônico corporativo deve ser restrito a finalidades profissionais, alinhadas às atividades da **Vivo Vita**.

O acesso físico às áreas e instalações, devem ser respeitados para garantir a proteção das pessoas, informações e equipamentos, assim como prevenir acessos não autorizados

A gestão de acessos lógicos e físicos deve seguir procedimentos formais para solicitação, transferência, revogação e revisão de acesso.

5.5 SEGURANÇA OPERACIONAL

Devem ser adotados controles para proteção dos ambientes físicos e lógicos, incluindo:

- Uso de senhas fortes, autenticação adequada, não reutilize as últimas senhas e as senhas são pessoais e intransferíveis;
- Backup periódico e testes de restauração;
- Monitoramento, auditoria e registro de atividades no ambiente computacional;
- Uso exclusivo de softwares homologados.

5.6 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todos os incidentes ou suspeitas devem ser reportados imediatamente .

Os incidentes de segurança da informação devem ser devidamente registrados, com evidências associadas, garantindo rastreabilidade e histórico das ações realizadas.

Seu tratamento deve assegurar a preservação da confidencialidade, integridade e disponibilidade das informações, em conformidade com a legislação vigente.

5.7 GESTÃO DE RISCOS

Os riscos de Segurança da Informação devem ser identificados, avaliados, tratados e monitorados continuamente, considerando impacto, probabilidade e requisitos legais, conforme as regras definidas pela **Vivo Vita**.

5.8 GESTÃO DE FORNECEDORES

Fornecedores e terceiros que acessam informações da organização devem ser avaliados quanto aos riscos de Segurança da Informação. É necessário garantir que atendam a requisitos de segurança alinhados aos padrões internos, por meio de cláusulas contratuais, acordos de confidencialidade e avaliações periódicas. Além disso, deve haver monitoramento contínuo para assegurar a conformidade e mitigar riscos ao longo do relacionamento.

5.9 CONTINUIDADE DE NEGÓCIOS

A organização deve manter planos de continuidade com testes periódicos para garantir a disponibilidade das informações e a continuidade das operações em caso de incidentes, falhas ou eventos adversos.

5.10 CONSCIENTIZAÇÃO E TREINAMENTOS

Todos os colaboradores devem participar de programas de conscientização e treinamento em Segurança da Informação, com avaliação periódica de eficácia, assegurando o entendimento de suas responsabilidades na proteção das informações.

5.11 CONFORMIDADE, AUDITORIA E MELHORIA CONTÍNUA

O SGSI será submetido a auditorias internas e externas. Não conformidades deverão ser tratadas por meio de ações corretivas, promovendo a melhoria contínua dos processos.

6 PENALIDADES

O não cumprimento das diretrizes estabelecidas neste documento, poderá resultar em ações disciplinares, conforme as políticas internas da organização e o processo de gestão de não conformidades vigente.

7 ANEXO

A área de Governança mantém uma Biblioteca de Documentos do Sistema de Gestão de Segurança da Informação (SGSI), destinada ao armazenamento e divulgação controlada das políticas, normas, procedimentos, padrões e demais documentos relacionados à segurança da informação.

A consulta à documentação vigente deve ser realizada por meio do repositório oficial disponível em: [Controle de Informações Documentadas](#)

Todos os colaboradores devem observar os requisitos estabelecidos nos documentos aplicáveis às suas funções e atividades, sendo responsáveis por acessar periodicamente o repositório para verificar atualizações, revisões e novas publicações.