POIÍTICA SEGURANÇA DA INFORMAÇÃO

Criado em: 25/08/2021
Última atualização: 22/11/2021

ÍNDICE

1. DECLARAÇÃO DA POLÍTICA

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas do VIVA RIO para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

As informações do VIVA RIO serão preservadas e protegidas de acordo com os seguintes fundamentos de segurança da informação:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Sigilo:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

Os Dirigentes do VIVA RIO estão comprometidos e apoiam os princípios estabelecidos nesta PSI de proteção de seus recursos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade com o ambiente legal, primando pelo sigilo, integridade, disponibilidade, autenticidade e legalidade das informações.

2. Aplicação da PSI

Esta política e seus anexos aplicam-se a qualquer pessoa física ou entidade jurídica que cria, acessa, processa, armazena ou comunica informações do VIVA RIO ou em nome deste, especialmente os colaboradores.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou do Comitê de Riscos sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte ou qualquer outra atividade que envolva informações de uso restrito ou confidencial.

3. RESPONSABILIDADE DOS COLABORADORES

Entende-se por colaborador toda e qualquer pessoa física, contratada sob o regime celetista ou prestadora de serviço por intermédio de pessoa jurídica, ou não, que exerça alguma atividade dentro ou fora da instituição, incluindo os dirigentes, funcionários, estagiários, contratados, parceiros e subsidiárias.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao VIVA RIO e/ou a terceiros, em decorrência da não obediência às diretrizes dessa política.

É responsabilidade de todo colaborador:

- Seguir as normas aprovadas pelo Comitê de Riscos;
- Aplicar o nível de sigilo adequado às informações, conforme explicitado no item “11.1 - Classificação das Informações” deste documento;
- Zelar pela segurança das informações da Instituição e de seus parceiros comerciais,

informando quaisquer anormalidades percebidas ao superior imediato ou ao Comitê de Riscos.

4. CONFORMIDADE E DIREITOS DO VIVA RIO

Esta política não confere qualquer garantia de privacidade para o uso pessoal dos recursos de Informática da Instituição. Assim, em conformidade às leis e regulamentos aplicáveis:

- A Instituição reserva-se o direito de monitorar e auditar o uso de seus recursos, determinar o que constitui uso apropriado, interceptar e colocar em quarentena correspondências eletrônicas, mensagens e outras transações, e reportar qualquer atividade ilegal;
- A Instituição pode, sem aviso prévio, a seu critério e dentro das leis e regulamentos aplicáveis, bloquear, restringir e suspender o acesso aos seus recursos ou remover conteúdo que a prejudique ou viole esta política, assim como qualquer outra norma interna, lei e/ou regulamentos aplicáveis.

5. PROCESSO DE APROVAÇÃO DA POLÍTICA DA SEGURANÇA DE INFORMAÇÃO

A Política de Segurança da Informação, bem como suas revisões e atuliazações, deverá ser aprovada pelo Comitê de Riscos do VIVA RIO e referendada pela sua Diretoria Executiva.

6. ORGANIZAÇÃO DA SEGURANÇA DE INFORMAÇÃO

O programa de Segurança da Informação será governado da seguinte forma:

6.1. Comitê de Riscos

O Comitê de Riscos é uma entidade estratégica, multidisciplinar, composto por representantes das seguintes áreas:

- Tecnologia da informação
- Controle interno
- Compliance

6.2. Atribuições do Comitê de Riscos

- Analisar, criticar e aprovar a Política de Segurança da Informação e seus anexos.
- Analisar, criticar e definir as ações corretivas pertinentes aos incidentes de Segurança da Informação, quando indeferidos pelo gerente responsável.
- Analisar, criticar e definir as iniciativas para aumentar o nível de Segurança da Informação na Instituição.
- Reavaliar o planejamento estratégico da Segurança da Informação priorizando as ações para os próximos meses.
- Difundir a cultura de Segurança da Informação na Instituição.

6.3. Atuação do Comitê de Riscos

O Comitê de Riscos deve ser reunido, no mínimo, a cada 3 (três) meses para tratar de assuntos relacionados a Segurança da Informação. Esta reunião pode ser presencial ou através de quaisquer outros métodos que possibilitem a interação de todos os seus membros.

Reuniões extraordinárias podem ser solicitadas, a qualquer momento, por quaisquer membros do comitê nas situações que se seguem:
Surgimento de necessidade de negócio que demande a elaboração, alteração ou aprovação imediata de norma(s) de Segurança;
Acontecimento, denúncia ou identificação da iminência de Incidente de Segurança da Informação crítico;
Após as reuniões deve ser elaborada uma documentação com os principais temas deliberados.

6.4. Área de Segurança da Informação

- Elaboração da Política de Segurança da Informação e seus anexos;
- Elaboração e análise de soluções técnicas para a implantação da Política de Segurança da Informação e seus anexos;
- Criar as metodologias e processos específicos para execução prática da Segurança da Informação nas atividades diárias do VIVA RIO, incluindo:
- Avaliações de Risco;
- Auditoria Interna de Segurança da Informação;
- Atividades Preventivas e Corretivas;
- Identificação e Tratamento de Incidentes;
- Recuperação de Desastres;
- Executar um programa periódico de conscientização de segurança.
- Participar no planejamento dos projetos do VIVA RIO, fornecendo recomendações de segurança e auxiliando o entendimento da Política de Segurança da Informação e seus anexos.
- A Área de Segurança da Informação pode vetar um projeto que envolva acesso a informações sigilosas, caso este viole a Política de Segurança.
- Avaliar a adequação e coordenar a implantação de controles específicos de Segurança da Informação para novas aplicações e/ou serviços.
- Disponibilizar canais de comunicação para que os colaboradores possam contribuir com o controle de segurança das informações da Instituição, através de denúncias, críticas e sugestões.

7. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

7.1. Interpretação

Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, no contexto de uso de informações e recursos de Tecnologia da Informação e Comunicação (TIC), tudo o que não estiver expressamente permitido só deve ser realizado após prévia autorização do Comitê de Riscos do VIVA RIO, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

7.2. Publicidade

Esta PSI e seus documentos complementares devem ser divulgados aos colaboradores e terceiros, visando a sua disponibilidade para todos os que se relacionam com o VIVA RIO, ou que, direta ou indiretamente, são impactados.

7.3. Propriedade

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos colaboradores e terceiros no exercício de suas atividades profissionais com o VIVA RIO, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de propriedade exclusiva do VIVA RIO e devem ser empregadas exclusivamente em atividades de interesse institucional.

7.4. Inspeção dos Recursos de TIC

O VIVA RIO, sempre que considerar necessário, poderá auditar ou inspecionar os recursos de TIC que interagem com seus ambientes lógicos, físicos ou com suas informações, incluindo os recursos de TIC de propriedade de terceiros, quando autorizada a entrada nas dependências da Instituição, independentemente da interação com seus ambientes e informações.

7.5. Revisão das Políticas

O VIVA RIO deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares. A revisão deve ocorrer a cada ano, ou quando mudanças significativas são propostas ou ocorrem, visando a garantia de que todos os requisitos de segurança técnicos e legais implementados sejam cumpridos, atualizados e em conformidade com a legislação vigente.

8. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

8.1. Uso dos Recursos de Tecnologia da informação e comunicação:

Os recursos de TIC de propriedade do VIVA RIO devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente. Os colaboradores devem utilizar apenas recursos de TIC previamente homologados e autorizados pela Gerência de TI para a realização de suas atividades profissionais, sejam eles onerosos, gratuitos, livres ou licenciados.

As ferramentas corporativas, colocadas à disposição dos colaboradores, são de uso exclusivo para o desenvolvimento das atividades profissionais e de acordo com os interesses do VIVA RIO. A Área de Segurança da Informação poderá acessar registros, sistemas e quaisquer informações existentes nos ambientes do VIVA RIO, a qualquer momento, sempre que julgar necessário.

8.2. Acesso à Internet (Celulares e computadores)

Não é permitido o uso da Internet, entre outros, para:

- Download de softwares, músicas, vídeos, entre outros arquivos que não façam parte da rotina de trabalho do colaborador;
- Violar leis e acessar conteúdos incompatíveis com os valores da VIVA RIO, tais como: pornografia, incitação à violência, pedofilia, preconceitos em geral, entre outros;
- Acessar sites de relacionamento, chat, ferramentas de mensagem instantânea, e outras ferramentas que permitam o envio de informações para fora da Instituição sem prévia autorização da Áreade Segurança da Informação;
- Comprometer a privacidade ou o sigilo das informações de terceiros;
- Realizar acesso remoto a computadores e redes, pessoais ou corporativas, fora do controle da Instituição, exceto quando autorizado pela área de TI;
- Alterar ou excluir informações armazenadas em computadores sem a devida autorização do gestor da área;
- Praticar qualquer tipo de hostilidade eletrônica, tais como: difamação da instituição e\ou colaboradores em redes sociais, falsificação de identidade e marca do VIVA RIO, entre outros.

É vedado o acesso a sites que não sejam considerados de interesse da Instituição ou que possam comprometer sua imagem ou a segurança das informações.
O acesso à Internet deve ser realizado através dos mecanismos providos pelo Viva Rio.
O VIVA RIO irá monitorar regularmente o uso da Internet na Instituição, a fim de preservar a integridade das informações, identificar vulnerabilidades e falhas de segurança, bem como verificar o seu uso adequado.
Os serviços disponibilizados através da Internet podem ser desativados temporariamente caso haja indício de tentativas de quebra de segurança, ou outras ações que ponham em risco a imagem ou a operação do VIVA RIO ou de seus parceiros comerciais.
Todos os colaboradores que possuem celular institucional e fazem parte de grupos de aplicativos de troca de mensagens (ex.: Whatsapp) devem utilizar tais aplicativos com cautela, observando se o teor das mensagens é sensível, e evitando compartilhamento indevido de informações e dados que de alguma forma possam prejudicar a imagem ou operação do VIVA RIO.

8.3. Correio Eletrônico e Mensageria

Com relação ao envio de correio eletrônico, não é permitido, entre outros, o envio de:

- Spam;
- Conteúdo pornográfico, incitação à violência, pedofilia, preconceitos em geral, entre outros;
- Informações classificadas como sigilosas, sem consentimento do gestor responsável no setor.

A concessão de contas de correio eletrônico aos colaboradores deve ser realizada de acordo com os interesses do VIVA RIO, que pode a qualquer momento revogar o acesso a tais contas.
As mensagens de correio eletrônico enviadas são de responsabilidade de seu remetente, devendo ser observado, especialmente, o conteúdo daquelas endereçadas ao ambiente externo.
O uso de aplicativos de mensagens, nos dispositivos corporativos, está restrito ao essencial, às atividades profissionais do colaborador.
O Comitê de Sindicância do VIVA RIO poderá acessar os e-mails de uma conta institucional, computadores, notebooks, tablets e smartfones, sem a ciência e permissão do funcionário, em caso de um processo de investigação.

8.4. Acesso Remoto

O acesso remoto à rede corporativa deve ser realizado exclusivamente através das ferramentas homologadas para este fim.
O acesso remoto à rede corporativa para atividades de suporte e monitoria de serviços críticos, além de ser realizado pelas áreas responsáveis por estas tarefas, deve ser previamente autorizado.
Os demais acessos devem ser avaliados pela Área de Segurança da Informação.

8.5. Telefonia Convencional

O uso dos recursos de telefonia deve ser gerido pelo gestor de cada área.
É prerrogativa do Viva Rio gravar as ligações efetuadas através dos dispositivos de telefonia corporativos.
O Comitê de Sindicância do Viva Rio poderá monitorar as ligações entre ramais sem a ciência e permissão do funcionário em caso de um processo de investigação.
O gestor da área deve informar ao setor de Tecnologia da Informação o afastamento do colaborador que possui celular institucional no caso de necessidade de bloqueio da linha telefônica.

8.6. Pastas de Rede

O acesso as pastas de Rede do servidor de Arquivos da Sede (Cambito), bem como os servidores locais das unidades (Clinicas da Família, Unidades de pronto atendimento, Centros de Atenção Psicossocial e demais unidades administradas pelo VIVA RIO) é de uso exclusivo dos funcionários do Viva Rio, para armazenamento estritamente de arquivos relacionados com sua rotina de trabalho.

Os funcionários devem armazenar seus arquivos de trabalho em pasta do seu setor, no Cambito. Caso o mesmo não tenha acesso à pasta do setor para gravação e\ou para criação de uma nova pasta, o mesmo deverá abrir um chamado no sistema Help Desk com a solicitação de acesso.

Para o caso de funcionários alocados em unidades do VIVA RIO que não possuam acesso ao Cambito e que tenham a necessidade de armazenar arquivos de trabalho, a orientação é que os mesmos entrem em contato com o setor de Tecnologia da Informação.

A pasta de rede TRANSFER no Cambito tem o objetivo de servir de armazenamento temporário de documentos que contenham informações de uso não confidencial, e que precisam ser compartilhados entre setores do VIVA RIO. Como trata-se de área temporária de armazenamento,

todos os arquivos constantes no TRANSFER serão apagados semanalmente. Documentos que sejam de uso exclusivo do setor não devem ser armazenados na pasta TRANSFER, mas sim nas pastas de cada setor no Cambito. Vale ressaltar que os documentos existentes no TRANSFER estão acessíveis a todos os funcionários da Sede do VIVA RIO e, portanto, podem ser visualizados, editados e até deletados.

8.7. Uso dos Recursos de Tecnologia da informação e comunicação Particulares:

O uso de recursos de TIC particulares na execução de qualquer atividade profissional, na interação com os ambientes físicos ou lógicos ou com as informações do SISTEMA VIVA RIO não poderão ocorrer por meio da rede cabeada e wifi de transmissão de dados, exceto quando autorizado pelo responsável da Gerência de TI do VIVA RIO.

8.8. Repositórios digitais

É vedado aos colaboradores e terceiros o uso de repositórios digitais não homologados pelo responsável da Gerência de TI do VIVA RIO para armazenar ou publicar informações de propriedade do VIVA RIO ou sob sua responsabilidade, salvo casos em que a informação esteja previamente classificada como “pública”.

9. PRIVACIDADE, SIGILO E USO DAS MÍDIAS SOCIAIS

9.1. Privacidade e Proteção de Dados

O VIVA RIO respeita a privacidade dos titulares de dados e garante a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte de acordo com a sensibilidade do dado pessoal, a finalidade e a gravidade dos riscos, seguindo agindo em conformidade com a **PPR-TI-01 - Política de Privacidade.**

9.2. Mídias Sociais

A participação do colaborador nas mídias sociais deve ser realizada em acordo com as vedações previstas no no Código de Ética do VIVA RIO. Não é permitido que os colaboradores e prestadores realizem publicações que incorram na divulgação de dados confidenciais, restritos ou que contenham dados de clientes, pacientes ou terceiros.

Dirigentes, colaboradores e terceiros são responsáveis por suas condutas no uso das mídias sociais. Por isso, cuidados devem ser tomados: ao excesso de exposição (rotinas, trajetos, intimidade, etc.), no uso de conteúdos autorizados e legítimos e na preservação do sigilo profissional.

9.3. Sigilo

É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade do VIVA RIO sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja previamente classificada como "pública".

9.4. Áudio, Vídeos e Fotos:

É vedada qualquer atividade relacionada à captura de dados e seu compartilhamento público, inclusive no âmbito acadêmico, na internet e/ou nas mídias sociais, envolvendo gravação de áudio, vídeo ou foto de informações sigilosas, sensíveis ou enquadradas como dados pessoais, que sejam utilizadas na realização das atividades profissionais do VIVA RIO, sem a prévia e formal autorização para tanto, exceto se ocorrer em razão justificável como necessário para cumprimento das atividades profissionais prestadas pelo colaborador.

10. RECURSOS HUMANOS

10.1. Conscientização e Treinamento

Quando houver novos Dirigentes, Colaboradores, Prestadores de Serviços e Parceiros do VIVA RIO, deverá ser assinado o Termo de Compromisso para Dirigentes e Colaboradores ou Termo de Compromisso de Segurança da Informação para Terceiros – Pessoa Jurídica caso estes venham a lidar com informações confidenciais.

Funcionários recém-contratados serão avisados de suas responsabilidades de segurança e deverão reconhecer, por escrito, a aceitação destas responsabilidades, conforme definido na Política de Segurança da Informação do VIVA RIO.

Funcionários das áreas de TI e de Segurança da Informação serão notificados imediatamente de todas as rescisões contratuais de funcionários contratados ou terceirizados para que o acesso às informações em computadores e da Instituição possa ser prontamente encerrado.

Funcionários das áreas de TI e de Segurança da Informação serão notificados imediatamente de todas as movimentações internas de funcionários contratados ou terceirizados para que o acesso às informações anteriores seja revogado, se for o caso.

É responsabilidade dos gerentes e coordenadores adotarem modelos de gestão e ambientes de trabalho capazes de motivar e comprometer os colaboradores com a estratégia de Segurança da Informação do VIVA RIO.

Os trâmites de devolução de ativos e restrição de acessos efetuados pela equipe de suporte deverão respeitar o descrito na **POLÍTICA DE GESTÃO DE ATIVOS(PGA-TI-01).**

10.2. Processo disciplinar

Toda ação disciplinar por violação da Política de Segurança da Informação deve iniciar com um

relatório de incidente de segurança gerado em função da violação constatada. A equipe da Compliance será responsável pelo acompanhamento do processo para alinhamento com as definições do Código de Ética do VIVA RIO.

10.3. Conscientização

Todo funcionário que atua em cargo de gestão deve receber o treinamento básico em Segurança da Informação em prazo a ser definido pelo setor de RH. Este treinamento deve ser evidenciado, devendo tais registros serem armazenados conforme a legislação vigente, quando obrigatório, ou na conformidade das normas internas da área de Gestão de Pessoas.

A Segurança da Informação deve efetuar atividades de treinamento e conscientização nesta PSI e em temas diversos de Segurança da Informação com abrangência corporativa. A participação é obrigatória aos funcionários e terceiros que acessam informações classificadas como restritas ou confidenciais.

Conscientização é o processo de divulgação da PSI. O processo de conscientização consiste em explicar:

- Porque determinada norma existe;
- Como esta norma beneficia a corporação e os colaboradores;
- A quais pessoas a norma se aplica;
- Como esta norma deve ser praticada diariamente.

Quanto à metodologia de comunicação nas atividades de conscientização, esta comunicação deve ocorrer em todas as mídias,conforme os métodos e descrições abaixo:

- Intranet: A Gerência de Segurança da Informação (GSI) deve disponibilizar informações sobre a área, onde e como aplicar SI nas rotinas de trabalho, FAQs, canal de contato e a PSI completa;
- E-mail de SI: A GSI deve reforçar os principais pontos da PSI e aplicação corporativa deles, bem como comunicar atualizações nas normas, novas ameaças virtuais e incidentes (apenas os aprovados pelo comitê) aos colaboradores.
- E-learning: A GSI deve, em conjunto com o RH, disponibilizar um curso neste formato, direcionado aos supervisores, analistas, técnicos e estagiários. A aplicação do mesmo é de responsabilidade do RH.
- Workshop de SI: A GSI deve disponibilizar cursos voltados para um público específico, que aborda os principais pontos da PSI aplicadas a este pessoal. A aplicação dos mesmos é compartilhada entre a GSI e as áreas de negócio.
- E-mail de SI: A GSI deve disponibilizar mensalmente instruções para o uso das ferramentas e técnicas de segurança da informação.

11. GESTÃO DE ATIVOS E CLASSIFICAÇÃO DA INFORMAÇÃO

11.1. Classificação da Informação

Todas as informações de propriedade ou sob a responsabilidade do VIVA RIO devem ser classificadas e protegidas com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico, nos termos descritos na **POLÍTICA DE GESTÃO DE ATIVOS(PGA-TI-01).**

11.2. Gestão de Mídias

O Viva Rio adota Política específica par a Gestão de Mídias, a **POLÍTICA DE GESTÃO DE MÍDIAS - PGM-TI-01,** a qual possui como objetivo determinar o processo para a implementação de controles para o tratamento de mídias dentro do VIVA RIO.

12. GESTÃO DE ACESSO FÍSICO E LÓGICO

Controle de acesso

O VIVA RIO controla o acesso físico e lógico às suas dependências e aos seus recursos de Tecnologia da informação. Desse modo, colaboradores e terceiros devem possuir uma credencial de acesso de uso individual, intransferível e, sempre que aplicável, de conhecimento exclusivo.

Dirigentes, colaboradores e terceiros são responsáveis pelo uso e sigilo de suas credenciais de acesso. Não é permitido, em qualquer hipótese, compartilhar, revelar ou fazer uso não autorizado de credenciais de terceiros, sendo responsável direto pela conduta ou/e dano causado, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

O VIVA RIO dispõe instruções específicas e fundamentais relacionadas à Gestão de acesso físico e lógico, as quais estão disponíveis na Norma de Acesso Físico e Lógico do VIVA RIO.

Entretanto, cada unidade e atividade vinculada aos projetos e unidade tem sua norma de acesso físico em conformidade com as respecivas cláusulas de contratação.

13. DESENVOLVIMENTO DE APLICAÇÕES

O desenvolvimento de aplicações deve ser realizado exclusivamente pela área de Tecnologia da Informação, conforme a norma de Desenvolvimento Seguro do VIVA RIO e observando boas práticas de codificação segura.

14. MONITORAMENTO E RESPOSTA A INCIDENTES

14.1. Monitoramento:

O VIVA RIO realiza o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, recursos de TIC e seus ambientes físicos e lógicos, visando a eficácia dos controles implantados, a proteção de seu patrimônio e sua reputação, possibilitando ainda a identificação de eventos ou alertas de incidentes referente a segurança da informação.

14.2. Processo de Resposta a Incidentes

O VIVA RIO deve manter uma Equipe de Resposta a Incidentes em Segurança da Informação e Comunicação, interna ou terceirizada, com composição fixa o variável, competente e preparada para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação em conformidade com a **POLÍTICA DE GESTÃO DE INCIDENTES (PGI-TI-01)** e dependendo do caso, levado para deliberação do Comitê de Risco.

A Área de Segurança da Informação deve disponibilizar canais para os colaboradores notificarem eventos e/ou incidentes de segurança da informação.

15. CONTINUIDADE DO NEGÓCIO

O Plano de Gestão de Continuidade dos Negócios está em em conformidade com os requisitos de segurança da informação que podem ser encontrados descritos no **PCN-TI-01 – PLANO DE CONTINUIDADE DE NEGÓCIOS.**

A identificação dos processos que compõe a Cadeia de Valor do Viva Rio e os requisitos de segurançada da informação devem permitir a determinação das necessidades de negócio relacionadas a pessoas, instalações e ativos de TI.

VI. DISPOSIÇÕES FINAIS

- O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pelo VIVA RIO.
- Os casos omissos e eventual procedimento diverso do previsto nesta Política de Segurança da Informação e Comunicação serão submetidos à análise do Comitê de Riscos.
- Esta PSI, bem como os demais documentos que a complementam, encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Comitê de Riscos do VIVA RIO.
- Esta PSI entra em vigor na data de aprovação.

VII. HISTÓRICO DE ALTERAÇÕES

Documento Original	PSI-TI-01
Responsável pelo Documento	Tera Tecnologia
Classificação	Restrito
Alterações	Criação

Histórico de Versões

Versão	Data	Autor	Comentários
01	25/08/2021	Jonathan Vergetti	Criação inicial do documento

Revisões do Documento

Versão	Data	Revisor	Comentários
01	14/10/2021	Brenno Ottoni	Revisão do documento
01	12/11/2021	Jorge Henrique	Revisão do documento