Política de Segurança da Informação

07 de Novembro, 2018

Índice

1 DECLARAÇÃO DA POLÍTICA

Proteger a confidencialidade, integridade e segurança das Informações do Viva Rio, levando em consideração: (1) os riscos de segurança associados a diferentes classes de informação; (2) requisitos legais, regulamentares e comerciais para proteger tipos específicos de informação; e (3) os custos, a eficácia e os aspectos práticos da implementação de controles para mitigar os riscos e atender aos requisitos externos.

1.1 CONCEITO DE INFORMAÇÃO

A informação pode existir em diversos formatos, tais como: impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, mostrada em filmes ou transmitida em conversas. Independentemente da forma apresentada, ou do meio pelo qual a informação é compartilhada ou armazenada, ela deve estar protegida de acordo com as diretrizes corporativas de Segurança da Informação.

1.2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

- Confidencialidade – característica das informações que estão disponíveis somente para sistemas ou pessoas autorizadas.
- Integridade - característica das informações que somente podem ser alteradas por pessoas permitidas.
- Disponibilidade - característica das informações que somente podem ser acessadas por pessoas autorizadas quando for necessário.
- Segurança da informação - preservação da confidencialidade, integridade e disponibilidade da informação.

1.3 OBJETIVO E APLICABILIDADE

1.3.1 Objetivo

Esta política documenta a abordagem geral do Viva Rio a fim de proteger suas informações e articula o quadro de governança para o Programa de Segurança da Informação.

A Política de Segurança da Informação é composta por este documento e por seus anexos, apresentados ao longo deste documento e que são partes integrantes desta.

Este documento e seus anexos são aplicáveis a:

- Todo hardware, software e pessoa que cria, retém, arquiva, processa, distribui, ou destrói informações do Viva Rio;
- Todos os terceiros ou entidades que possuem acesso às informações ou à infraestrutura do Viva Rio;
- Todas as normas contidas neste documento e em seus anexos foram elaboradas e aprovadas levando-se em consideração a legislação vigente.

1.3.2 Aplicabilidade

Esta política e seus anexos aplicam-se a qualquer pessoa física ou entidade jurídica que acessa, processa, armazena ou comunica informações do Viva Rio ou em nome deste, incluindo os funcionários, os contratados e subsidiárias.

1.4 Responsabilidades dos Colaboradores

É responsabilidade de todo colaborador:

- Seguir as normas aprovadas pelo Comitê de Segurança da Informação;
- Aplicar o nível de sigilo adequado às informações, conforme explicitado no item "Classificação das Informações" deste documento;
- Zelar pela segurança das informações da empresa e de seus parceiros comerciais, informando quaisquer anormalidades percebidas ao superior imediato ou à Área de Segurança da Informação.

1.5 Conformidade e Direitos do Viva Rio

Esta política não confere qualquer garantia de privacidade para o uso pessoal dos recursos de Informática da empresa. Sujeito às leis e regulamentos aplicáveis:

- À empresa 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 empresa 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 política, lei e/ou regulamentos aplicáveis.

2 Governança e Implementação da Política

2.1 Processo de Aprovação da Política da Segurança de Informação

A Política de Segurança é aprovada pelo Comitê de Segurança de Informação do Viva Rio.

2.2 Registros de Segurança de Informação

O Viva Rio mantém registros de segurança relevantes, incluindo incidentes de segurança, pedidos de exceções à política e resultados de auditoria.

3 Organização da Segurança de Informação

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

3.1 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

3.1.1 Membros

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

- Tecnologia da informação
- Controle interno
- Compliance

3.1.2 Atribuições

- 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 empresa.
- Reavaliar o planejamento estratégico da Segurança da Informação priorizando as ações para os próximos meses.
- Difundir a cultura de Segurança da Informação na empresa.

3.1.3 Atuação

O Comitê de Segurança da Informação deve ser reunido, no mínimo, a cada 3 (três) meses. 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.

3.2 ÁREA DE SEGURANÇA DA INFORMAÇÃO

3.2.1 Atribuições

- 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 confidenciais, 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 empresa, através de denúncias, críticas e sugestões.

4 NORMAS DA SEGURANÇA DE INFORMAÇÃO

4.1 CLASSIFICAÇÃO DA INFORMAÇÃO

Esta norma dispõe sobre a criação, a classificação, o uso e o descarte de informações no ambiente operacional do Viva Rio estabelecendo os requisitos mínimos de segurança da informação necessários para a manutenção adequada da confidencialidade, da disponibilidade e da integridade de informações.

4.1.1 Diretrizes

- Toda informação deve ser classificada no ato da sua criação ou aquisição.
- A classificação das informações deve ser realizada com base nas exigências de negócio do Viva Rio, considerando-se o valor da informação e os possíveis impactos causados por essa classificação ao negócio;
- Na classificação da informação, deve-se buscar o grau de segurança menos restritivo possível, visando aperfeiçoar ou agilizar o processo de tratamento e reduzir os custos com sua proteção;
- A classificação das informações é de responsabilidade do gestor da área que criou a informação que deverá, se julgar necessário, reclassificar as informações criadas ou recebidas pela área.
- Os ativos, físicos e lógicos, assumem automaticamente a classificação de maior nível de segurança atribuída a uma informação suportada por eles.
- Para fins de classificação quanto à exigência de sigilo, a informação pode ser classificada como “Restrita”, “Confidencial”, “Interna” ou “Pública”.
- O uso, a cópia e o transporte, interno ou externo, de informação “Confidencial” ou “Interna” poderão ser realizados apenas mediante a autorização formal do gestor da informação.
- A informação que não possuir uma classificação explícita quanto à sua confidencialidade será automaticamente classificada como “Comum”.

4.1.2 Classificação por confidencialidade

4.1.2.1 **RESTRITA**

- Restrita é uma informação associada a interesses estratégicos, de negócios e/ou financeiros do Viva Rio. Se revelada, pode trazer prejuízos financeiros, impactos ao negócio ou repercussões negativas à imagem do Viva Rio e/ou de seus Financiadores.
- Toda informação classificada como “Restrita” deve indicar quais pessoas, ou grupos de pessoas, devem possuir permissão de acesso a ela.
- Toda informação física classificada como “Restrita” deve ser armazenada com cautela para evitar a violação da mesma.
- O descarte ou destruição de uma informação Restrita física ou lógica deve ser feito de forma que não seja possível recuperá-la.

4.1.2.2 **CONFIDENCIAL**

- Confidencial é toda informação cujo conhecimento, em razão de lei, interesse de determinado departamento ou preservação de direitos individuais, deve ficar limitado a um número reduzido de pessoas autorizadas. Se revelada, pode trazer prejuízos e repercussões negativas à imagem do Viva Rio.
- Toda informação classificada como “Confidencial” deve indicar quais pessoas, ou grupos de pessoas devem possuir permissão de acesso a ela, e/ou possuir mecanismos que restrinjam o acesso aos colaboradores devidos.
- O descarte ou destruição de uma informação Confidencial física ou lógica deve ser feito de forma que não seja possível recuperá-la

4.1.2.3 **INTERNA**

- Interna é toda informação cujo conhecimento e uso estão limitados ao âmbito interno e aos propósitos do Viva Rio, estando disponível para todos os usuários autorizados a circular em suas dependências.

4.1.2.4 **PÚBLICA**

- Pública é toda informação que pode ser divulgada para o público interno e externo ao Viva Rio.
- Serão classificadas como “Públicas” as informações, dados, processos ou documentos que:
    - Tenham natureza pública em virtude de lei ou sejam de domínio público;
    - Sejam relativas a quaisquer contratos celebrados por escritura pública ou arquivados perante notário público ou em junta comercial.
- Excetuam-se do acesso público irrestrito os documentos cuja divulgação comprometa a intimidade, a vida privada, a honra e a imagem das pessoas e, aqueles integrantes de processos judiciais sob segredo de justiça.

4.1.3 Reclassificação

Apenas o responsável pela classificação, ou seus superiores hierárquicos, pode alterar a classificação de uma informação.

4.1.4 Gestão de Mídias

4.1.4.1 INFORMAÇÃO CONFIDENCIAL

- É proibida a reutilização de mídias físicas ou óticas, que armazenem informações confidenciais.
- Mídias magnéticas (ex.: discos rígidos) que armazenem informações confidenciais devem ser formatadas de forma segura antes de serem reutilizadas.

4.1.4.2 MÍDIA FÍSICA

Este tipo de mídia não deve ser utilizado nas seguintes situações:

- Sobrescrever informações com outras de diferente classificação;
- Sobrescrever informações internas ou confidenciais destinadas a públicos distintos daquele da gravação original.

Exemplos de mídia:

- Impressão
- Anotações de uma Reunião Interna

4.1.4.3 MÍDIA ÓTICA

Este tipo de mídia não deve ser utilizado para sobrescrever informações internas ou confidenciais destinadas a públicos distintos daquele da gravação original.

Exemplos de mídia:

- CD, DVD e Blu-Ray

4.1.4.4 MÍDIA ELETRÔNICA

Este tipo de mídia deve ser submetida por uma checagem de antivírus antes de realizar qualquer tipo de transferência de arquivos entre a mesma e um computador do Viva Rio.

Exemplos de mídia:

- Pen Drive

4.1.5 Exemplos de classificação

- Restrita
  - Planejamento Estratégico do Viva Rio
  - Prontuário dos pacientes
- Confidencial
  - Cargos e Salários
  - Sistemas ERP
  - Active Directory
- Interna
  - Organograma de Área
  - Apresentações Executivas

- Relatórios Gerenciais
- Sistemas de Apoio Operacional
- Ramais do Viva Rio na intranet
- Conteúdo de lista “todos” de e-mail

- Pública
  - Política de recursos humanos
  - Relatórios publicados na área de transparência do site

4.1.6 Métodos de descarte de Mídias

- Trituração
- Incineração
- Formatação Segura (Wipe)
- Desmagnetização

4.2 GESTÃO DE PESSOAS

4.2.1 Diretrizes

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.

Os funcionários contratados e terceirizados deverão reconhecer anualmente, por escrito, a aceitação de suas responsabilidades de segurança da informação, conforme definido na Política de Segurança da Informação do Viva Rio.

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

Funcionários das áreas de TI e de Segurança serão notificados imediatamente de todas as Movimentações internas de funcionários contratados ou terceirizados para que o acesso às informações anteriores seja revogado.

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.

4.2.2 Adesão a Política de Segurança da Informação

Todos os funcionários do Viva Rio devem assinar um termo de adesão à Política de Segurança da Informação. Este termo deve permanecer armazenado, ao menos, até o encerramento do vínculo empregatício.

Cláusulas de adesão à Política de Segurança da Informação deverão constar em todos os contratos de empresas terceiras que prestam serviços ao Viva Rio.

4.2.3 Treinamento

Todo funcionário deve receber o treinamento básico em Segurança da Informação após sua contratação e em prazo a ser definido pelo setor de RH. Este treinamento deve ser evidenciado, devendo tais registros ser armazenados conforme a legislação vigente, quando obrigatório, ou as normas internas da área de Gestão de Pessoas.

A Segurança da Informação deve efetuar atividades de treinamento e conscientização periodicamente, com abrangência corporativa. A participação é obrigatória aos funcionários e terceiros que acessam informações classificadas como restrita ou confidencial.

4.2.4 Prestadores de Serviço

A contratação de prestadores de serviço deve seguir as normas e procedimentos definidos pela Gestão de Pessoas.

Todo prestador de serviço que for atuar no Viva Rio por mais de 90 (noventa) dias corridos deve receber um crachá personalizado, com foto.

Todo prestador de serviço que for atuar com informações classificadas como confidenciais deve assinar um Termo de Confidencialidade com o Viva Rio ou aderir ao Termo de Confidencialidade assinado pela empresa contratada.

4.2.5 Contratação

O candidato deve ler e aceitar a Política de Segurança da Informação antes da contratação, e assinar o Termo de Confidencialidade válido por 15 anos. Os controles também se aplicam a terceirizados.

4.2.6 Desligamentos

A comunicação de encerramento do vínculo de trabalho deve incluir:

- Devolução de ativos corporativos;
- Suspensão ou exclusão de acessos físicos e lógicos.

4.2.7 Segregação de funções

Uma pessoa não pode possuir permissões em processos e tecnologias para executar duas das atividades abaixo listadas de forma sequenciada:

- Solicitar;
- Aprovar;
- Criar/Remover/Executar;
- Validar;
- Auditar;

4.2.8 Processo disciplinar

Toda ação disciplinar por violação da Política de Segurança da Informação deve iniciar com um relatório de incidente de segurança, informando:

- Tipo de Incidente;
- Impactos causados;
- Controle violado;
- Evidências da violação;
- Pessoas envolvidas;
- Análise da área de Segurança da Informação.

As punições por violações da Política de Segurança da Informação podem incluir:

- Advertência escrita;
- Suspensão temporária;
- Demissão sem justa causa;
- Demissão por justa causa.

É responsabilidade da área de Gestão de Pessoas conduzir o processo disciplinar.

4.2.9 Comunicação

No âmbito do Viva Rio, define-se por Comunicação o processo de instruir os colaboradores na utilização pessoal da segurança da informação.

Esta comunicação deve ocorrer em todas as mídias e métodos descritos 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.

4.2.10 Conscientização

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.

Esta comunicação deve ocorrer em todas as mídias e métodos descritos abaixo:

- 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.

4.3 ACESSO LÓGICO

4.3.1 Gestão de credenciais

Os acessos necessários devem ser concedidos, preferencialmente, através de perfis pré-estabelecidos.

A elaboração/manutenção da documentação de perfis de acesso deve ser executada pelo gestor responsável pelo ativo ou sistema gerenciado, sob supervisão da Segurança da Informação.

A cada colaborador deve ser atribuído o mínimo privilégio necessário para o bom andamento das atividades sob sua responsabilidade.

Os acessos devem ser geridos através de processos pré-estabelecidos. Estes processos devem contemplar, no mínimo:

- Procedimento de aprovação e criação/alteração do acesso.
- Procedimento suspensão/exclusão de acessos.
- Referência aos documentos que explicitem os perfis de acesso disponíveis e seus privilégios, quando aplicável.

Deve ser concedido a todos os colaboradores o privilégio de alterar suas respectivas senhas a qualquer momento.

Os acessos temporários devem ser aprovados pelo proprietário da informação e removidos na data determinada.

A criação ou alteração de credenciais de acesso somente deve ser executada com a autorização formal do gestor da informação.

As senhas de acesso devem ser criadas de forma aleatória e configuradas para exigir a alteração durante o primeiro acesso.

A identidade do usuário será verificada antes de redefinição de senhas.

As credenciais de acesso de usuários afastados por licença devem ser suspensas enquanto perdurar o afastamento.

Quando da transferência do colaborador para outra função ou área, suas permissões de acesso vigentes devem ser revogadas. É responsabilidade do gestor da nova função solicitar a alteração dos acessos para a nova função, incluindo a revogação dos acessos antigos.

As credenciais de acesso dos colaboradores desligados, sejam funcionários ou prestadores de serviço, devem ser bloqueadas mediante solicitação da equipe de Gestão de Pessoas ou do gestor da área pelo tempo determinado para o perfil em uso pelo colaborador desligado.

As contas de usuários locais devem ser desativadas ou removidas, salvo as de uso do Sistema Operacional.

As contas de convidado ou anônima devem ser desativadas ou removidas.

4.3.2 Acesso a sistemas e informações

O acesso aos ativos e sistemas do Viva Rio deve ser concedido a colaboradores identificados, autorizados e autenticados, através de credenciais individuais e intransferíveis, sendo vedado ao titular compartilhá-las com outros, exceto, em casos previamente autorizados pela área de segurança da informação.

O acesso às informações e aos ativos de informação deve ser disponibilizado de acordo com os requisitos das atividades profissionais do colaborador, sendo sempre o mínimo necessário.

Os grupos que possuam todos os usuários do domínio corporativo devem ser utilizados apenas para acesso a informações Internas ou Públicas.

O privilégio administrativo aos diretórios que contenham informações internas ou confidenciais deve ser atribuído apenas às equipes responsáveis pela manutenção ou gestão de acessos do ativo que hospeda a informação. Este acesso deve ser concedido às contas administrativas individuais.

O acesso às informações de aplicações e sistemas deve ser concedido aos usuários através de perfis de acesso.

O acesso administrativo aos ativos de rede deve ser realizado de forma criptografada.

As sessões locais ociosas serão automaticamente bloqueadas após 5 (cinco) minutos de inatividade

As sessões remotas ociosas serão automaticamente desconectadas após 10 (dez) minutos de inatividade.

4.3.3 Gestão de Acesso dos Prestadores de Serviço

O acesso de terceiros aos ativos e informações do Viva Rio deve ocorrer mediante aprovação do gestor da área, conforme procedimento vigente.

O gestor que autorizar o acesso do terceiro é o responsável por quaisquer danos causados por tal terceiro às informações da empresa, salvo para prestadores vinculados a contratos formais com outras empresas.

Cabe ao aprovador solicitar a suspensão/bloqueio de todos os acessos, conforme procedimento vigente.

Nos casos de transferência do prestador para outra área, cabe ao novo gestor solicitar a alteração de acessos, conforme procedimento vigente.

4.3.4 Utilização de Contas e Senhas

As contas e senhas fornecidas aos colaboradores são de uso individual.

As senhas de acesso são classificadas como informação confidencial e, como tal, devem possuir os controles definidos na norma “Classificação das Informações”.

Os colaboradores são responsáveis por todas as ações realizadas mediante as contas e senhas que lhes são atribuídas.

As senhas de acesso devem ser alteradas em intervalos de 4 meses. É proibida a reutilização da última senha válida.

As senhas de acesso devem ser compostas por, no mínimo, 8 (oito) caracteres alfanuméricos.

4.3.5 Gestão do Ambiente de Trabalho

É proibido escrever credenciais de acesso aos sistemas corporativos ou de parceiros comerciais em papel;

Não é recomendado o manuseio de alimentos e bebidas em ambientes nos quais existam estações de trabalho, servidores ou documentos que acessem e/ou hospedem informações classificadas como confidenciais, ficando o responsável pelo dano ciente das punições cabíveis.

4.3.6 Rastreabilidade de Acessos

A criação, alteração e exclusão de perfis de acesso, bem como a atribuição de perfis, devem ser registradas. Através deste registro, deve ser possível identificar:

- O executor;
- O objeto (usuário ou perfil afetado);
- A data e a hora da execução.
- Os registros de acesso às principais informações de processo nos sistemas podem ser acessados mediante solicitação ao setor de Tecnologia da Informação.

4.4 ACESSO FÍSICO

4.4.1 Diretrizes

A Segurança das instalações com relação ao acesso físico tem como objetivos específicos:

- Diminuir o risco e controlar o acesso não autorizado a informações e instalações físicas da Unidade/Departamento;
- Minimizar o risco de perda, dano ou comprometimento dos ativos;
- Diminuir o risco de exposição ou roubo de informação.

A área de Segurança Humana, em parceria com as demais áreas técnicas, é responsável pela revisão da norma intitulada "Gestão de acesso físico".

4.4.2 Controle de acesso

As instalações do CPD (áreas de armazenamento ou processamento de informações sensíveis) ou outras áreas classificadas como confidenciais devem ser equipadas com controles de entrada apropriados e monitoramento de câmeras, de forma que somente pessoal autorizado tenha acesso liberado;

Com exceção das unidades que funcionam 24 horas, todas as portas externas e de áreas classificadas como confidenciais devem ser bloqueadas fora do horário comercial normal;

Qualquer pessoa dentro de uma área classificada como confidencial deverá dispor de identificação de acordo com a função por ela exercida;

Os funcionários não podem permitir a estranhos o acesso aos recursos de rede;

O ingresso de visitantes deve ser controlado de tal forma a impedir o acesso ao CPD (áreas de armazenamento ou processamento de informações sensíveis), salvo acompanhados e com autorização da área de tecnologia do Viva Rio ou Gestor da unidade;

A área de segurança humana deverá realizar um mapeamento anual dos pontos de vulnerabilidade das unidades.

4.5 ATIVOS

4.5.1 Definições

Ativos físicos são todos os prédios, veículos, mobiliário, computadores, telefones, material de escrita e similares utilizados por colaboradores do Viva Rio.

Ativos lógicos são os softwares utilizados pelos colaboradores através de computadores, dispositivos móveis, smartphones e similares.

4.5.2 Dispositivos estruturais

A temperatura e a umidade nos centros de processamento de dados (CPD), nas salas de telecomunicações e nas salas de dispositivos de gestão elétrica (geradores, no-breaks, entre outros) devem ser controladas e estar em conformidade com as especificações dos fabricantes dos equipamentos.

Sistemas de combate a incêndio devem ser instalados de acordo com a legislação vigente.

4.5.3 Gestão de ativos

Apenas os Sistemas Operacionais homologados pela empresa devem ser utilizados nos ativos dos ambientes Produção e Homologação.

O horário de todos os equipamentos deve ser sincronizado, de modo a garantir sua acurácia em tempo integral.

A manutenção dos equipamentos deve ser realizada somente por pessoal autorizado.

Todas as estações de trabalho e servidores devem possuir um sistema adequado de combate a códigos maliciosos, instalado e atualizado.

A instalação de softwares somente deve ser realizada pelas equipes responsáveis pelo suporte especializado. Tal instalação deve ser realizada mediante autorização do responsável pelo ativo e aprovação pela área de TI.

A área de TI deve documentar o hardware e os softwares de cada ativo do Viva Rio.

A área de TI deve controlar o licenciamento de softwares em uso nos ativos do Viva Rio.

Exceto quando autorizado pela área de TI, usuários não devem baixar, instalar ou executar programas de segurança ou utilitários com a finalidade de detectar fraquezas na segurança da rede do Viva Rio.

4.5.4 Desktops e Notebooks

Os colaboradores devem encerrar ou bloquear a sessão da estação de trabalho sempre que se ausentarem do local de trabalho.

Os colaboradores não poderão, em hipótese alguma, alterar os padrões definidos ou desativar os mecanismos de segurança disponibilizados pelo Viva Rio.

Apenas as equipes de suporte poderão adicionar, alterar ou remover equipamentos e softwares em estações de trabalho, servidores e outros ativos da empresa.

Apenas softwares homologados e licenciados devem ser instalados nas estações de trabalho e servidores da empresa.

A cópia de softwares, adquiridos ou desenvolvidos pelo Viva Rio, é vedada, salvo em casos de autorização da área de TI.

4.5.5 Aquisição de Hardware e Software

Todos os softwares devem ser adquiridos através da área de TI, independentemente da origem ou método de aquisição (ou seja, adquirido de uma loja ou baixado da internet);

Todo hardware de tecnologia (computador, tablet, celular, notebook, roteador e etc.) deve ser adquirido conforme especificação e/ou indicação realizada pela área de TI.

4.5.6 Utilização de Equipamentos Eletrônicos

O uso de aparelhos eletrônicos corporativos móveis, como celulares e tablets, para acesso às informações é livre, e devem ser configurados com senha para desbloqueio de tela;

Os equipamentos de financiadores, fornecedores e prestadores de serviço somente devem ser conectados à rede corporativa após prévia análise da Equipe de TI, e posterior aprovação do gestor da área visitada.

Dispositivos pessoais (computador, tablet, celular, notebook, roteador e etc.) não devem acessar a rede do Viva Rio, exceto com a aprovação da área de TI;

Nos locais aonde a área de TI aprovou o uso de laptop pessoal, o mesmo deve ser configurado da seguinte forma:

- Software antivírus;
- O login requerido do dispositivo com uma senha conforme os requisitos da política de senha.

4.6 UTILIZAÇÃO DA REDE, INTERNET E TELEFONIA

4.6.1 Diretrizes

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.

O comitê de Segurança da Informação poderá acessar registros, sistemas e quaisquer informações existentes nos ambientes do Viva Rio, a qualquer momento, sempre que julgar necessário.

4.6.2 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 empresa sem prévia autorização do Comitê de 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 empresa, 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 empresa 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 empresa, 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.

4.6.3 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 confidenciais 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 mensageria, nos dispositivos corporativos móveis, está restrito ao essencial, às atividades profissionais do colaborador.

A área de Compliance 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.

4.6.4 Acesso Remoto

O acesso remoto à rede corporativa deve ser realizado exclusivamente através das ferramentas homologadas para este fim, conforme norma intitulada “Gestão de Acesso Remoto”.

O acesso remoto à rede corporativa é previamente autorizado para atividades de suporte e monitoria de serviços críticos, desde que realizados pelas áreas responsáveis por estas tarefas. Os demais acessos devem ser avaliados pela Área de Segurança da Informação.

4.6.5 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.

A área de Compliance 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.

4.6.6 Pastas de Rede

O acesso as pastas de Rede do servidor de Arquivos (Cambito) 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.

4.7 DESENVOLVIMENTO DE APLICAÇÕES

O desenvolvimento de aplicações deve ser realizado exclusivamente pela área de Tecnologia da Informação, conforme a norma "Gestão de Softwares e Aplicações", observando boas práticas de codificação segura.

4.8 GESTÃO DE INCIDENTES

4.8.1 Notificação de Eventos e Incidentes

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

Procedimento descrevendo a coleta, a retenção e a apresentação de evidências, devem ser documentados em cooperação com as áreas de Gestão de Pessoas, Gestão Patrimonial e Jurídico, para permitir o uso legal das informações.

Os eventos e incidentes serão analisados pela Gestão de Segurança da Informação, e dependendo do caso, levado para deliberação do Comitê de Segurança da Informação.

4.9 CONTINUIDADE DO NEGÓCIO

O Plano de Recuperação de Desastres de TI e a Gestão de Continuidade dos Negócios devem estar em conformidade com os requisitos de segurança da informação;

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