SUBTIC SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

FAZENDA GOV RJ

CARTILHA

Política de Segurança da Informação (PSI)

2024

FAZENDA GOV RJ

Secretário de Estado de Fazenda
Leonardo Lobo Pires

Subsecretário-Geral de Estado de Fazenda
Gustavo Alves Tillmann

Subsecretário de Tecnologia da Informação e Comunicação
Gabriel Mac Dowell Blum

Subsecretário-Adjunto de Planejamento e Governança
Lucas Antônio Gonçalves Salvetti

Assessor-Chefe de Segurança da Informação
Paulo Marcelo da Rocha Silva

Coordenadores de Segurança da Informação
Francisco Thiago Gomes Azevedo
Marcus Vinicius Caetano Da Silva

Elaboração
Bernardo Bruno Marques
Luana Almeida da Silva Fidelis

Diagramação
Nathasha Inácio de Lemos

SUBTIC SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Sumário

Segurança da Informação

1. Introdução

A segurança da informação, aplicável a qualquer organização, está baseada nos seguintes pilares: preservação da confidencialidade, integridade e disponibilidade da informação[1].

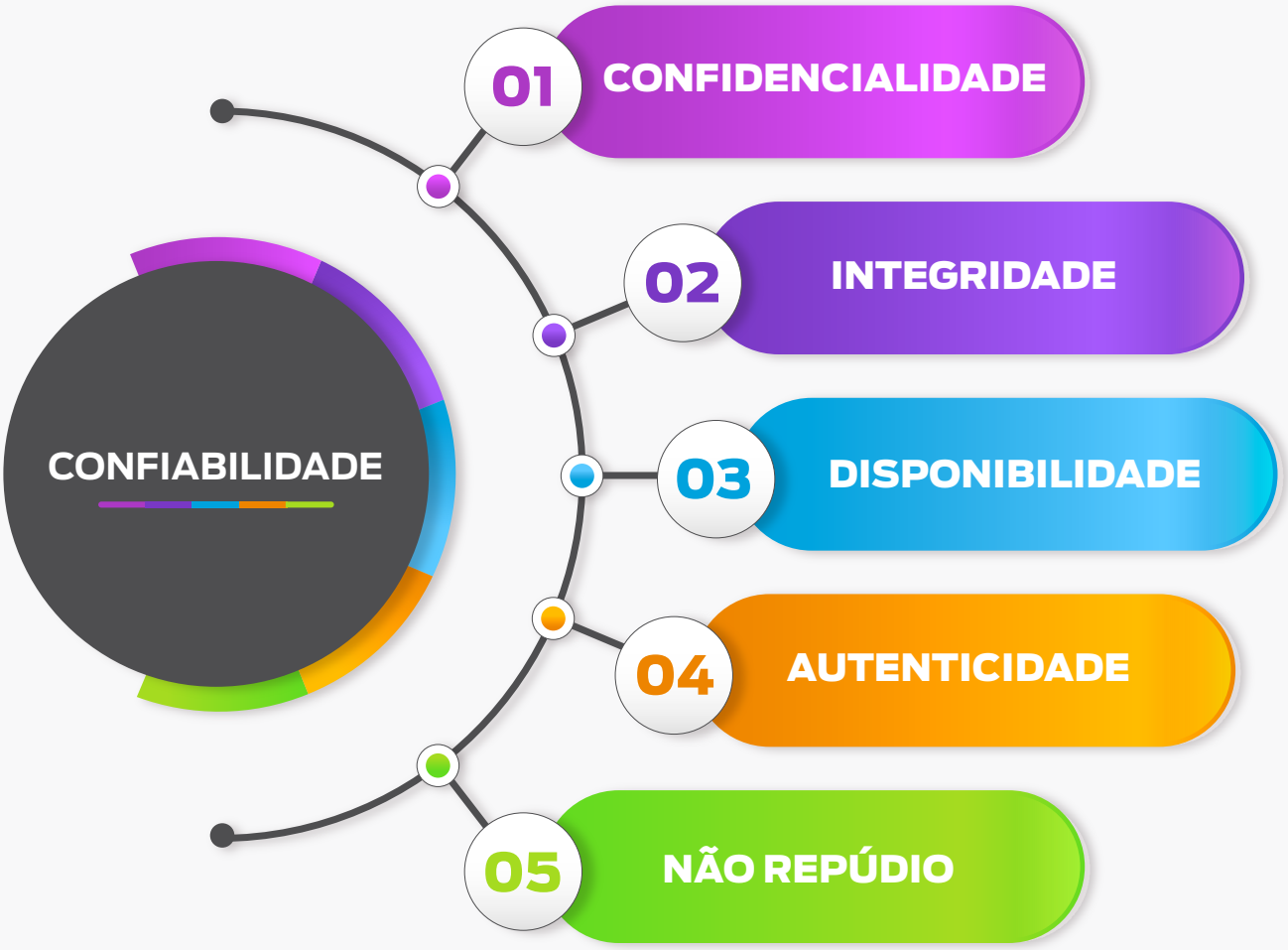
Confidencialidade é a premissa que visa garantir a privacidade e a proteção dos dados contra acessos indevidos. Esse pilar procura evitar que ações maliciosas exponham conteúdos indevidamente, causando prejuízos à organização. Afinal, as informações devem ser acessadas e reveladas somente a indivíduos, entidades e processos devidamente autorizados.

Integridade se relaciona com a manutenção da precisão das informações, sem erros e livres de alterações não autorizadas, para que possam ser empregadas de maneira segura pela organização. Assim, as informações devem ser protegidas contra manipulações e alterações indevidas.

Disponibilidade, por sua vez, tem o intuito de manter os dados ativos e disponíveis para serem usados quando for necessário, conforme o nível de desempenho almejado. Relaciona-se intimamente com a perfeita funcionalidade das áreas de negócio, na medida em que procura manter funcionando o atendimento aos clientes externos (contribuintes, órgãos de controle, órgãos parceiros, dentre outros) e aos internos (servidores e demais colaboradores das unidades integrantes da SEFAZ/RJ).

Adicionalmente, outras propriedades, tais como **autenticidade** (garantia de que a informação é procedente de fonte confiável e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu) e **Irretratabilidade / não repúdio** (garantia de que o emissor ou pessoa que tenha executado determinada transação de forma eletrônica não possa, posteriormente, negar sua autoria) podem também estar envolvidas.

A **confiabilidade** pressupõe a conformidade com esses cinco atributos ao longo do tempo. Os dados/informações deverão ser confidenciais, íntegros, disponíveis, autênticos e garantir a não negação de autoria.



Esses conceitos técnicos estão muito ligados ao nosso cotidiano. O conhecimento do significado deles aumenta a precisão da comunicação para temas que digam respeito à segurança da informação.

2. A Nova Política de Segurança da Informação da SEFAZ-RJ

A PSI é um documento previsto nos padrões ISO 27001 para auxiliar a implantação de um Sistema de Gestão de Segurança, minimizando possíveis ameaças e riscos para a organização. Segundo a ISO, a PSI possui as normas e as diretrizes que devem ser adotadas para gestão da informação nas organizações para proteger dados, principalmente aqueles considerados sensíveis e confidenciais.

Tendo em vista que a PSI anterior da SEFAZ-RJ havia sido editada em abril de 2018, constatada a impactante mudança ocorrida no ambiente tecnológico pelo mundo no intervalo de 5 (cinco) anos, identificou-se a necessidade de atualização. Inegável que diversas revoluções e implicações decorrentes da transformação digital foram verificadas no período.

No que se refere às alterações no ordenamento jurídico, podemos citar a aprovação da **Lei Geral de Proteção de Dados** (Lei nº 13.709 de 14 de agosto de 2018), poucos meses após a edição da PSI anterior e, mais recentemente, a edição da Instrução Normativa PRODERJ/PRE nº 02 de 28 de abril de 2022.

Apesar de a Lei nº 12.965 de 23 de abril de 2014 ser pretérita à PSI revogada, o **Marco Civil da Internet** impõe a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas (art. 3º, V).Os padrões internacionais (ISO, NIST, dentre outros) sofreram atualizações nos últimos anos (diversas normas técnicas foram editadas).

Nesse sentido, a edição da **Resolução SEFAZ Nº 599 de 28 de dezembro de 2023** que instituiu a Política de Segurança de Informação no âmbito da SEFAZ-RJ e aos novos diplomas legais e normativos.

2.1. Objetivos da PSI

A Política de Segurança da Informação é considerada a norma administrativa superior em matéria de segurança da informação. Neste sentido procura tratar dos temas de maior amplitude dentre aqueles relevantes. Uma analogia pertinente seria compará-la a uma "Constituição" da segurança da informação.

Princípios e diretrizes se amoldam a estas características, vindo a PSI em seu art. 3º, inciso I, estabelecer os primeiros objetivos da norma:

> I. estabelecer os princípios e as diretrizes estratégicas de um modelo de gestão da segurança da informação, por meio da implantação de controles para uso seguro, ético e legal dos ativos de TIC da SEFAZ-RJ;

Muito embora seja comumente identificada como matéria relacionada à unidade de tecnologia da informação, as PSI's acabam estabelecendo obrigações direcionadas a diversas unidades da organização. Em virtude disto, a edição de norma com status hierárquico de Resolução se revela adequada.

Nesta linha, a PSI em seu art. 3º, inciso II, estabelece o segundo objetivo da norma:

> II. declarar formalmente o compromisso da Instituição com a proteção dos ativos de TIC de sua propriedade ou sob sua guarda, devendo ser cumprida por todos os seus usuários;

A proteção dos pilares da segurança da informação deve contar com a colaboração de todos, seja horizontalmente (diferentes unidades), seja verticalmente (do maior ao menor nível hierárquico da organização).

NÍVEL ORGANIZACIONAL	ABRANGÊNCIA
Institucional	Toda a SEFAZ/RJ
Intermediário	Subsecretaria ou unidade colegiada
Operacional	Tarefas ou operações específicas

Considerando que estudos indicam que grande parte dos ataques e vazamentos de dados ocorrem devido a vulnerabilidades internas nas organizações (podendo decorrer de falhas humanas, em processos ou em tecnologias), a promoção de uma cultura de segurança da informação atuaria no sentido de mitigar tais fragilidades. Nesta esteira, a PSI em seu art. 3º, inciso III, estabelece mais um objetivo da norma:

> III. promover e motivar a criação de uma cultura de segurança da informação, abrangendo todos os usuários da SEFAZ-RJ na execução de suas atividades profissionais, bem como seus processos de trabalho, buscando o envolvimento de toda a Instituição, do nível operacional ao estratégico;

Obviamente, não poderia deixar de ser mencionada a necessidade de proteção aos pilares que constituem a base da segurança da informação (confidencialidade, integridade, disponibilidade e, adicionalmente, autenticidade, não repúdio e confiabilidade). Nesta linha, a PSI em seu art. 3º, inciso IV, estabelece o derradeiro objetivo expresso:

> IV. zelar pelos pilares da segurança da informação:

2.2. Privacidade e Proteção de Dados Pessoais

Na era da transformação digital, as informações sobre as pessoas estão se tornando cada vez mais valiosas. Com o advento das novas tecnologias, as organizações coletam e armazenam dados em grande escala.

Neste cenário surgem desafios específicos de segurança, especialmente os relativos a dados pessoais, devido à regulamentação rígida em relação à proteção de dados. Privacidade e proteção de dados pessoais passaram a ser prioridade para qualquer organização[2].

A SEFAZ/RJ, na medida em que processa **dados pessoais** de indivíduos localizados no território brasileiro, deve cumprir a Lei Geral de Proteção de Dados Pessoais (LGPD). Assim, a PSI apresenta as diretrizes em matéria de segurança da informação, prescrevendo algumas normas acerca do tratamento das informações no âmbito da SEFAZ/RJ (arts.5º ao 9º da PSI).

Por **tratamento**, nos termos da LGPD, entende-se toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação,utilização,acesso,reprodução,transmissão,distribuição,processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Lei nº 13.709/2018, art. 5º, inciso X).

2.2.1. Bases legais

De acordo com a LGPD, o tratamento de dados pessoais é autorizado caso se amolde às hipóteses expressamente previstas em seu artigo 7º, cuja redação é a seguinte:

> I. mediante o fornecimento de consentimento pelo titular;
>
> II. para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)vigência;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A lista de hipóteses que autorizam o tratamento é taxativa, não sendo possível alegar outra razão justificadora como base. Deste modo, deve-se identificar uma das hipóteses que autorizam o tratamento.

Deve ficar claro que a LGPD exige, ainda, que sejam informadas as hipóteses em que, no exercício de suas competências, as pessoas jurídicas de direito público realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (LGPD, art.23, I).

Para conferir proteção adicional, a LGPD define **dado pessoal sensível** como aquele que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

De acordo com a LGPD, o tratamento de dados pessoais sensíveis só será lícito nas hipóteses expressamente previstas em seu artigo 11:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

As mesmas observações realizadas acima para os dados pessoais são, por evidente, aplicáveis ao tratamento de dados pessoais sensíveis, os quais, por sua natureza, deverão estar sujeitos a proteções adicionais.

Nos casos de **cumprimento de obrigação legal ou regulatória** pelo controlador e de tratamento compartilhado de dados necessários à execução de **políticas públicas** previstas em leis ou regulamentos pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da LGPD.

2.2.2.Atuação de ofício por parte das unidades da SEFAZ-RJ

A PSI em seu art. 8º estabelece que as unidades integrantes da SEFAZ-RJ deverão atuar de ofício de modo a cumprir as exigências da Lei nº 13.709, de 14 de agosto de 2018. Trata-se de um **poder-dever** conferido às autoridades responsáveis pelas unidades da organização com o intuito de fazerem cumprir a lei.

Como forma de tornar possível o cumprimento dos preceitos supracitados da LGPD em ambientes informatizados (no que se refere aos sistemas utilizados pelas áreas de negócios) a PSI informa caber ao **Gestor de Sistema** (definido pela Resolução SEFAZ Nº 509 de 31 de março de 2023) informar as hipóteses em que no exercício de suas competências ocorre o tratamento de dados pessoais (PSI, art.9º). Os gestores deverão, também, fornecer informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, nos termos do art. 23, I da LGPD.

2.3. Vedações quanto ao uso de inteligência artificial não homologada para uso

Tecnologia de Inteligência Artificial Aplicada à Linguagem (*Large Language Model - LLM*)[3] teve uma aceitação muito rápida. Um exemplo conhecido de destaque desta tecnologia é o ChatGPT. Ao utilizar este tipo de tecnologia é necessário:

- Ter a devida diligência quanto às saídas geradas pelas ferramentas. Há discussões atuais acerca da ocorrência de prejulgamentos sobre grupos ou indivíduos não baseados em fatos.

- Ter cuidado com questões relativas à privacidade e à segurança. Dados confidenciais **não** devem ser solicitados da ferramenta de LLM, nem devem ser disponibilizados como entrada para a ferramenta (ou seja, para fora da organização).

O art. 12 da PSI assim dispõe:

> Art. 12. É vedada a inserção de informação confidencial, proprietária ou sensível da SEFAZ-RJ em ferramenta de inteligência artificial não homologada para uso pela SUBTIC.

2.4. Responsabilidade pelo conteúdo armazenado nos recursos de TIC particulares

A utilização de dispositivos pessoais para trabalhar é uma prática que vem se alastrando pelas organizações, tendo ganhado popularidade. A utilização de dispositivos próprios para trabalhar e se conectar às redes das organizações, todavia, oferece alguns riscos para a segurança da informação.

Alguns dispositivos utilizados pelos colaboradores nem sempre são avaliados pelos departamentos de TIC, nem seguem os mesmos padrões de segurança da organização. Isso, por evidente, pode gerar problemas em longo prazo, como o vazamento de dados ou até a invasão das redes.

Neste sentido a PSI se preocupou em prescrever algumas regras que visam reduzir os riscos para a SEFAZ-RJ. O art. 13 da PSI assim possui a seguinte redação:

> Art. 13. Os dispositivos de TIC particulares conectados à rede da SEFAZ-RJ poderão ser inspecionados pela área competente, caso necessário.
>
> § 1º A responsabilidade pelo conteúdo armazenado nos recursos de TIC particulares é do usuário.
>
> §2º Em nenhuma hipótese a SEFAZ-RJ se responsabilizará por danos em dispositivos pessoais, ainda que utilizados em conexão com o ambiente corporativo.

2.5. Obrigatoriedade quanto a utilização de autenticação multifator (MFA)

A autenticação multifator (MFA) é um método crucial para reforçar a segurança em ambientes digitais.

A MFA obriga que o usuário forneça dois ou mais fatores de identificação para acessar um recurso, como um sistema ou conta. Além da tradicional combinação de nome de usuário e senha, verificações adicionais são solicitadas. Isso significa que mesmo se alguém conhecer a senha, não terá acesso sem confirmar sua identidade de outra maneira.

2.5.1. Por que é importante?

- Segurança em várias camadas: A autenticação multifator cria barreiras adicionais, garantindo que apenas pessoas autorizadas acessem sistemas protegidos.
- Proteção contra vazamento de senhas: Com mais de 10 milhões de senhas vazadas mensalmente no Brasil, a autenticação multifator ajuda a mitigar riscos.
- Conformidade com regulamentações: À medida que as regulamentações de segurança de dados se tornam mais rigorosas, a implementação do MFA é recomendada.
- Mitigação de ameaças emergentes: A MFA fortalece a segurança das contas, protegendo contra tentativas de login suspeitas.

2.6. Gestão de Identidade e Acessos

A gestão de identidades e acessos (*Identity Access Management - IAM*) é uma prática essencial na área de segurança da informação. A IAM é um processo que visa garantir que as pessoas, máquinas e software tenham acesso devido aos recursos no momento correto, sendo um dos elementos fundamentais da segurança cibernética, impedindo ameaças internas e externas e garantindo que apenas indivíduos autorizados tenham acesso a informações sensíveis.

Neste sentido, a SEFAZ-RJ implementará gestão de identidades e acessos com promoção de equilíbrio entre segurança da informação e experiência do usuário, suportando os processos de negócio, atuando em conformidade com a legislação e aplicando controles apropriados contra fraude (art.18 da PSI).

2.6.1. Gestor de Usuários

Trata-se do responsável pela gestão do vínculo de uma pessoa física ou jurídica com a SEFAZ-RJ do qual resulte a concessão de credenciais de acesso ao ambiente corporativo. A depender da natureza do vínculo entre a pessoa e a SEFAZ-RJ este papel será exercido pelo(a):

- Fiscal administrativo de contrato (no caso dos prestadores de serviços);
- Titular da unidade da SEFAZ-RJ (no caso de convênios); ou
- Superintendência de Recursos Humanos (nos demais casos).

2.6.2. Do acesso aos ativos de TIC

O acesso a todo e qualquer ativo de TIC ocorrerá, preferencialmente, por meio de perfil de acesso padronizado, concedido mediante procedimentos automatizados (processo ordinário previsto no art.22 da PSI).Entretanto, na ausência destes, será concedido excepcional e precariamente de forma individual, desde que atendidas algumas condicionantes (parágrafo único do art.22 da PSI que remete aos requisitos previstos no art.24 da mesma norma).

O caput do art.24 da PSI afirma que a competência para autorizar o acesso individual será do subsecretário hierarquicamente superior no setor que necessite da informação, devendo considerar:

I. a real necessidade;

II. a confidencialidade da informação; e

III. o tipo de acesso (leitura, alteração, deleção) a ser autorizado.

Em se tratando de órgãos colegiados, a competência para autorização será do presidente ou da respectiva autoridade máxima (§ 1º do art. 24 da PSI). Não correspondendo a esta hipótese e inexistindo subsecretaria hierarquicamente superior ao setor do usuário que necessite da informação, competirá à Subsecretaria Geral da Fazenda decidir acerca da autorização (§ 2º do art. 24 da PSI).

Importante mencionar que, em qualquer dos casos excepcionais acima, a autorização concedida deverá conter termo de validade, não podendo superar 12 (doze) meses (§ 3º do art. 24 da PSI).

2.6.3. Dos meios de acesso à informação

Os meios de acesso à informação serão definidos pela SUBTIC (aspectos técnicos), devendo ser levada em consideração a necessidade do requisitante (art. 25 da PSI). Para esta finalidade, os meios mais seguros, eficientes e amigáveis aos usuários deverão ser buscados.

A concessão de acesso direto a bancos de dados a usuários do ambiente corporativo da SEFAZ somente será realizada nas hipóteses de inexistência de outro meio viável, devendo ser revogada tão logo sobrevenha alternativa (§ 2º do art. 25 da PSI).

Observação: Importante mencionar que, com relação a usuários externos, a concessão de acesso direto ao banco de dados está vedada.

Após autorização e definição do meio de acesso, a realização da configuração das credenciais de acesso referentes à solicitação ficará a cargo do gestor do ativo de TIC, o qual corresponderá (art. 26 da PSI):

> I. ao gestor do sistema, em se tratando de sistemas corporativos, transacionais ou analíticos, nos termos da Resolução SEFAZ Nº 509 de 31 de março de 2023;
>
> II. ao responsável designado para a concessão das credenciais no setor atinente à Governança de Dados da SUBTIC, em se tratando de acesso a dados diretamente em bancos de dados corporativos; ou
>
> III. ao Service Desk, para os demais ativos de TIC.

2.7. Da auditoria e da conformidade

Auditorias de verificação de conformidade em segurança da informação poderão ser realizadas periodicamente pela SUBTIC visando à adequação e ao aprimoramento dos controles de segurança aos objetivos estabelecidos pela PSI e pelas demais normas e procedimentos de segurança da informação (art.27 da PSI).

A periodicidade das auditorias poderá ser definida em função dos riscos associados aos recursos de TIC e da sensibilidade das informações, devendo os procedimentos e autorizações de auditoria serem classificados como restritos.

Nesta linha, a SEFAZ-RJ poderá auditar e realizar inspeções nos ativos de TIC próprios ou naqueles que interajam com seus ambientes lógicos ou físicos (art.28 da PSI).

3. Conclusão

Não resta dúvida de que o advento da Resolução SEFAZ Nº 599 de 28 de dezembro de 2023 representa um marco do comprometimento da instituição com a segurança da informação no âmbito da SEFAZ/RJ. Mais que isso, atendeu a uma necessidade premente de atualização, tendo em vista as novas exigências legais e infralegais que surgiram no interregno entre a PSI anterior e o ano em curso.

Esta breve cartilha procurou introduzir o tema da maneira mais direta e objetiva possível. Caso necessário, seus idealizadores se encontram à disposição para receber sugestões, críticas ou elogios, bem como para esclarecer dúvidas que possam surgir.

Obviamente, a Resolução SEFAZ Nº 599 de 28 de dezembro de 2023, por ser mais extensa, possui diversos pontos que não foram objeto de tratamento neste material, por extrapolar o escopo pretendido.

De qualquer forma, é importante lembrar que este é apenas o primeiro passo na busca pela tão desejada confiabilidade. A sustentação de um ambiente corporativo seguro pressupõe comprometimento de todos os interessados envolvidos.

Referências

1 - International Organization for Standardization (ISO). Disponível em: <https://www.iso.org/home.html>

2 - Exin . Disponível em: <https://www.exin.com/data-protection-security/exin-privacy-and-data-protection/exin-privacy-and-data-protection-essentials-based-on-lgpd/#:~:text=EXIN%20Privacy%20%26%20Data%20Protection%20Essentials%20based%20on%20LGPD%20%C3%A9%20uma,mat%C3%A9ria%20de%20prote%C3%A7%C3%A3o%20de%20dados.>

3- O que é LLM? | Large Language Model. Disponível em: <https://canaltech.com.br/inteligencia-artificial/o-que-e-llm-large-language-model/>

Dez cuidados básicos de segurança

1. USE SENHAS DIFERENTES

Use senhas diferentes para contas diferentes. Jamais utilize a senha da SEFAZ-RJ em outro site ou serviço.

2. USE ANTIVÍRUS NO COMPUTADOR DE CASA

Instale e mantenha atualizado software de antivírus nos seus computadores pessoais.

3. CUIDADO COM E-MAIL RECEBIDOS

Não abra anexos nem clique em links de e-mails de remetentes desconhecidos. Não baixe arquivos recebidos por mensagens instantâneas.

4. NÃO UTILIZE WI-FI PÚBLICO

Não utilize redes de Wi-Fi públicas, pois são portas de entrada fáceis para ataques e roubo de senhas.

5. CUIDADO COM SEUS DADOS PESSOAIS

Cuidado com dados pessoais. Não compartilhe dados ou documentos pessoais em redes sociais, sites na internet, ou com empresas inseguras.

6. JAMAIS COMPARTILHE SUA SENHA

A senha é pessoal e intransferível, e não deve ser armazenada em mídia digital em formato texto puro.

7. PROTEJA DISPOSITIVOS MÓVEIS

Mantenha dispositivos móveis protegidos com senha ou biometria.

8. NÃO USE SOFTWARE PIRATEADO NO COMPUTADOR DE CASA

Nao usar software pirata ou “crackeado” em casa. Os softwares piratas tem altíssima probabilidade de conter malware.

9. AO SAIR, BLOQUEIA A TELA

Não deixe sua tela destravada - Ao se afastar do seu computador, trave a tela apertando Window+L. No celular, configure bloqueio automático.

10. MANTENHA SEUS SOFTWARES ATUALIZADOS

Mantenha todos os softwares dos seus computadores pessoais atualizados. Software desatualizado contém vulnerabilidades que **possibilitam invasões remotas.**

Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda

RESOLUÇÃO SEFAZ Nº 599 DE 28 DE DEZEMBRO DE 2023

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) NO ÂMBITO DA SECRETARIA DE ESTADO DE FAZENDA (SEFAZ-RJ).

O SECRETÁRIO DE ESTADO DE FAZENDA DO RIO DE JANEIRO, no uso das atribuições legais, de acordo com o inciso I do Parágrafo único do art. 148 da Constituição do Estado do Rio de Janeiro, tendo em vista o disposto no Decreto Nº 31.896/2002 e o disposto no Processo n.º SEI-040227/000356/2023,

CONSIDERANDO:

- a ABNT NBR ISO/IEC 27001:2022, a ABNT NBR ISO/IEC 27002:2022, a ABNT NBR ISO/IEC 27005:2023 e a NIST SP 800-53, atinentes à segurança da informação;
- a necessidade de estabelecer diretrizes e padrões para viabilizar um ambiente tecnológico controlado e seguro;
- as diretrizes emanadas pelo órgão central de tecnologia de informação e comunicação do Governo do Estado (Instrução Normativa PRODERJ/PRE nº 02 de 28 de abril de 2022);
- a proteção dos pilares da segurança da informação: integridade, disponibilidade e confidencialidade;
- a imperatividade de assegurar a autenticidade dos dados e informações dos diversos sistemas e serviços de TIC;
- a necessidade de atualização da Política de Segurança da Informação da SEFAZ-RJ editada em 2018;
- o disposto no Marco Civil da Internet (art. 3º, V, da Lei nº 12.965, de 23 de abril de 2014); e
- a Lei Geral de Proteção de Dados Pessoais (art. 23 da Lei nº 13.709, de 14 de agosto de 2018).

RESOLVE:

TÍTULO I - DAS DISPOSIÇÕES PRELIMINARES

CAPÍTULO I – DA APLICAÇÃO

Art. 1º Fica instituída, nos termos desta Resolução, a Política de Segurança da Informação da Secretaria de Estado de Fazenda do Rio de Janeiro.

Parágrafo único. Os comandos desta norma se aplicam a servidores, prestadores de serviço, estagiários e a todos que se relacionem, direta ou indiretamente, com a SEFAZ-RJ.

Art. 2º Para os fins deste ato, considera-se:

I. ambiente corporativo: espaço, físico e virtual, no qual estão inseridos os ativos de tecnologia e de informação da organização, tais como dispositivos, redes, sistemas, *hardware*, *software*, dados, informações, pessoas, processos físicos, papéis, documentos, dentre outros;

II. ameaça: evento negativo que pode levar a resultado indesejado, como dano ou perda de um ativo de informação (*International Information System Security Certification Consortium - ISC²*);

III. ativo intangível: todo elemento que possui valor para a instituição e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, tais como reputação, imagem, marca e conhecimento;

IV. ativo: algo que possua valor para a organização, incluindo pessoas, propriedades e informações (ISC²);

V. ativos de tecnologia da informação e comunicação (TIC): todo objeto, tangível ou intangível, que um órgão ou entidade pública ou privada pode controlar e que tem potencial ou real valor para o atingimento de seus objetivos. Assim, consideram-se ativos de TIC os equipamentos, os materiais, os programas de computador, as informações, as licenças de *software* e os contratos que constituem a infraestrutura tecnológica de suporte às atividades de TIC do órgão ou entidade (Art. 2º, V, da Resolução SEFAZ Nº 509 de 31 de março de 2023);

VI. autenticação de multifator (MFA): autenticação usando dois ou mais dentre os seguintes fatores: algo que você sabe; algo que você possui; e algo que você é;

VII. avaliação de riscos: o processo de identificação de riscos para operações organizacionais, incluindo missão, funções, imagem, reputação, ativos organizacionais, indivíduos, e outras organizações, resultantes da operação de um sistema de informação (ISC²);

VIII. conformidade: designa o dever de cumprir, de estar em conformidade e fazer cumprir regulamentos internos e externos impostos às atividades de uma organização;

IX. continuidade do negócio: capacidade de a organização continuar com as operações essenciais durante a ocorrência de um incidente de segurança (ISC²);

X. controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal (ISO/IEC 27002);

XI. controle de acesso baseado em papéis (RBAC): utiliza papéis ou grupos. Em vez de associar permissões diretamente a usuários, contas de acesso são ligadas a papéis, de tal forma que administradores possam associar privilégios aos papéis. As boas práticas internacionais correlacionam os papéis com as funções desempenhadas na organização. Segundo o NIST, cada usuário receberia uma coleção de autorizações de acesso com base em uma suposição explícita ou implícita de uma determinada função

(NIST 800-53);

XII. controle de segurança: salvaguardas ou contramedidas prescritas para sistemas ou organizações de informação projetadas para proteger a confidencialidade, integridade e disponibilidade das informações que são processadas, armazenadas e transmitidas por esses sistemas ou organizações, bem como para satisfazer um conjunto de requisitos de segurança definidos (NIST 800-53);

XIII. dados: parte elementar da estrutura do conhecimento, computável, não produzindo, isoladamente, conclusões inteligíveis ao destinatário;

XIV. dispositivo de identificação digital: recurso tecnológico que possibilita identificar e autenticar o usuário em ambientes lógicos e físicos, tais como *software* autenticador, certificado digital, *token* e leitor biométrico;

XV. dispositivos móveis: equipamentos que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como por exemplo, pen *drives*, celulares, *smartphones*, *notebooks* ou *netbooks*, *tablets*, equipamentos reprodutores de MP3, câmeras de fotografia ou filmagem, ou qualquer dispositivo que permita conexão à internet, portabilidade ou armazenagem de dados;

XVI. evento de segurança da informação: uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação (ISO/IEC 27001);

XVII. gestor de sistema: responsável na área de negócio pelo sistema, desde a sua concepção até a sua desativação (Art. 2º, XV da Resolução SEFAZ Nº 509 de 31 de março de 2023);

XVIII. gestor de usuário: responsável pela gestão do vínculo de uma pessoa física ou jurídica com a SEFAZ-RJ do qual resulte a concessão de login de rede ou qualquer outro tipo de credencial de acesso ao ambiente corporativo.

XIX. grupo: maneira de tornar o gerenciamento de acesso mais eficiente. A configuração de permissões baseadas em atribuição no nível do grupo permite que todos os usuários de um grupo tenham o mesmo acesso a quaisquer eventos e permissões atribuídos ao grupo;

XX. incidente de segurança da informação: um evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (ISO/IEC 27001);

XXI. informação: conjunto de dados que podem ser utilizados para produção e transmissão de conhecimento;

XXII. log: registro de atividades que permite a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação;

XXIII. matriz de controle de acesso: uma tabela que correlaciona sujeitos, objetos e privilégios

atribuídos;

XXIV. mídias sociais: plataformas baseadas em internet, nas quais ocorre a interação entre pessoas físicas ou jurídicas e a produção, troca ou compartilhamento de informações;

XXV. papel: no contexto de RBAC se refere a um grupo de pessoas que compartilham determinadas características comuns, a exemplo de: departamento, localização, senioridade, responsabilidades de trabalho;

XXVI. permissão: propriedade de um objeto. Estabelece quais usuários têm permissão para usar o objeto e o que eles têm permissão para fazer (exemplo: ler, modificar, executar);

XXVII. privilégio: propriedade de um agente, como um usuário. Permite que o agente faça coisas que normalmente não são permitidas, a exemplo de: acessar um objeto que ele normalmente não tem permissão; executar funções de manutenção, como reiniciar o computador;

XXVIII. recursos de tecnologia de informação e comunicação (recursos de TIC): recursos físicos e lógicos utilizados para criar, armazenar, processar, manusear, transportar, compartilhar e descartar a informação, podendo-se destacar: microcomputadores, *notebooks, smartphones, tablets, pendrives,* mídias, impressoras, *scanners, softwares,* entre outros;

XXIX. risco: mensuração do quanto que uma entidade está ameaçada por uma circunstância ou evento potencial, considerados os impactos adversos que surgiriam se a circunstância ou evento ocorresse e a probabilidade de ocorrência (NIST 800-53);

XXX. segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ISO/IEC 27001);

XXXI. serviços corporativos: são serviços oferecidos aos usuários dos recursos de TIC, por meios próprios da SEFAZ-RJ ou por intermédio de contratos com terceiros;

XXXII. sujeitos: usuários, grupos ou papéis;

XXXIII. usuário: funcionário, servidor, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venha a ter relacionamento, direta ou indiretamente, com a SEFAZ-RJ;

XXXIV. usuário externo: pessoa ou instituição sem vínculo com a SEFAZ-RJ;

XXXV. violação: qualquer atividade que desrespeite as diretrizes estabelecidas nesta Política ou em quaisquer das demais normas que a complemente; e

XXXVI. vulnerabilidade: fraqueza que pode ser explorada (ISC²).

CAPÍTULO II - DOS OBJETIVOS

Art. 3º Esta Política de Segurança da Informação tem por objetivos:

I. estabelecer os princípios e as diretrizes estratégicas de um modelo de gestão da segurança da informação, por meio da implantação de controles para uso seguro, ético e legal dos ativos de TIC da SEFAZ-RJ;

II. declarar formalmente o compromisso da Instituição com a proteção dos ativos de TIC de sua propriedade ou sob sua guarda, devendo ser cumprida por todos os seus usuários;

III. promover e motivar a criação de uma cultura de segurança da informação, abrangendo todos os usuários da SEFAZ-RJ na execução de suas atividades profissionais, bem como seus processos de trabalho, buscando o envolvimento de toda a Instituição, do nível operacional ao estratégico;

IV. zelar pelos pilares da segurança da informação:

a) autenticidade: garantia de que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

b) confidencialidade: garantia de que as informações sejam acessadas e reveladas somente a indivíduos, entidades e processos devidamente autorizados;

c) disponibilidade: garantia de que as informações e os recursos de TIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

d) integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas;

e) legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com a legislação em vigor; e

f) não repúdio: garantia de que o emissor ou pessoa que tenha executado determinada transação de forma eletrônica não possa, posteriormente, negar sua autoria.

CAPÍTULO III - DOS PRINCÍPIOS

Art. 4º São princípios da gestão da segurança da informação no âmbito da SEFAZ-RJ:

I. legalidade/conformidade: cumprimento da legislação vigente e dos instrumentos regulamentares relacionados às atividades profissionais e aos objetivos institucionais e éticos da SEFAZ-RJ e da Administração Pública Estadual;

II. defesa em profundidade: estratégia de segurança de informação que busca integrar pessoas, tecnologia e recursos instituindo múltiplos, redundantes e independentes níveis de proteção, considerando o valor dos ativos de TIC para a organização;

III. hierarquia de controles administrativos: estabelecimento de políticas, normas e procedimentos para o gerenciamento, planejamento, controle e avaliação das atividades de segurança da informação relacionados à TIC;

IV. simplicidade: favorecimento da implementação de salvaguardas e controles de segurança

simples ao invés de complexos;

V. proteção dos ativos intangíveis: preservação aos ativos intangíveis da SEFAZ-RJ em relação aos diversos tipos de ameaça como acesso, divulgação, compartilhamento ou modificação não autorizados;

VI. cultura de segurança da informação: incorporação, por todos os usuários, da segurança da informação como um elemento essencial em seus hábitos e atitudes dentro e fora da organização;

VII. privilégio mínimo: concessão aos usuários apenas das permissões estritamente necessárias para a execução das atividades profissionais designadas;

VIII. celeridade: oferecimento de ações rápidas em resposta a incidentes e falhas, visando reduzir os impactos gerados por incidentes de segurança; e

IX. responsabilidade: definição clara das responsabilidades primárias e finais pela proteção de cada ativo de TIC e pelo cumprimento de processos de segurança.

TÍTULO II - DAS DIRETRIZES

CAPÍTULO I - DO TRATAMENTO DAS INFORMAÇÕES

Art. 5º Os tratamentos de dados definidos no art. 5º, X, da Lei nº 13.709, de 14 de agosto de 2018 deverão ser realizados em conformidade com os comandos da Lei Geral de Proteção de Dados, sem prejuízo da observância aos demais normativos pertinentes.

§1º A base legal que autoriza o uso das informações no âmbito da SEFAZ-RJ será:

I. o cumprimento de obrigação legal ou regulatória;

II. o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; ou

III. outra hipótese aplicável regulada pela Lei nº 13.709, de 14 de agosto de 2018.

§2º Nas hipóteses que envolvam transferência de sigilo fiscal, a disponibilização de informações será objeto de normatização específica.

§3º Além do disposto no caput, deverão ser observadas a legislação pertinente e as boas práticas de segurança internacionais.

Art. 6º As informações devem ser classificadas considerando aspectos legais, grau de sigilo requerido, tempo de guarda e retenção, e observando o seguinte:

I. adoção de tecnologias atuais que viabilizem a classificação das informações de forma descentralizada, colaborativa, assertiva e oportuna, respeitando os dispositivos da Lei nº 13.709, de 14 de agosto de 2018

atinentes à salvaguarda de dados pessoais;

II. as melhores práticas de segurança da informação, consentâneas com a legislação vigente, que visam garantir a privacidade e proteção dos dados;

III. metodologia de classificação e de tratamento da informação quanto ao grau de sigilo regulada por legislação específica, levando em conta, também, as diretrizes da legislação para tratamento de dados sensíveis e dados pessoais.

Art. 7º O tratamento das informações deve atender aos seguintes requisitos:

I. corresponsabilidade de cada usuário pela segurança dos ativos de TIC, inclusive informações que tiver acesso em função de suas atividades na SEFAZ-RJ, especialmente em relação àqueles que estejam sob a sua tutela;

II. vedação ao usuário de revelar, transferir, publicar, compartilhar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da SEFAZ-RJ, inclusive informações relacionadas às suas rotinas de trabalho, dados de contribuintes, fornecedores e prestadores de serviços ou demais detalhes operacionais, salvo quando na execução de atividades institucionais, observando-se, nesse caso, os critérios de classificação e tratamento da informação e o sigilo fiscal;

III. controles de segurança aplicáveis no gerenciamento da informação que levem em consideração todo o seu ciclo de vida, o qual compreende sua criação, registro, classificação, acesso, manuseio, modificação, reprodução, distribuição, compartilhamento, publicação, transmissão, armazenamento, arquivamento e destruição;

IV. nível de segurança compatível com o grau de exigência, a natureza e a criticidade dos serviços públicos e dos dados utilizados, conforme art. 21, IX, da Lei nº 14.129, de 29 de março de 2021;

V. transmissão, armazenamento e recebimento de mensagens, conteúdos, arquivos, *software* ou informações institucionais, de propriedade ou sob responsabilidade da SEFAZ-RJ realizada por intermédio de serviços corporativos oferecidos, exceto quando houver necessidade de comunicação com pessoa externa ou previsão diversa em legislação específica.

Art. 8º As unidades integrantes da SEFAZ-RJ deverão atuar de ofício de modo a cumprir as exigências da Lei nº 13.709, de 14 de agosto de 2018.

Art. 9º Cabe ao Gestor de Sistema definido pela Resolução SEFAZ Nº 509 de 31 de março de 2023 informar as hipóteses em que no exercício de suas competências ocorre o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, nos termos do art. 23, I da Lei nº 13.709, de 14 de agosto de 2018.

CAPÍTULO II – DO USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 10. Os recursos de TIC da SEFAZ-RJ são destinados ao cumprimento das atividades institucionais e o uso não apropriado destes pode pôr em risco a segurança da organização.

Parágrafo Único. A inobservância do disposto no *caput* poderá gerar responsabilização administrativa.

Art. 11. É proibido acessar, baixar, transmitir, utilizar, instalar, armazenar, divulgar ou repassar qualquer arquivo, material, conteúdo, ou recurso ilícito ou com finalidade ilícita.

Parágrafo Único. A Assessoria de Segurança de Informação da SUBTIC poderá, em razão do estrito cumprimento de suas atribuições, manipular os arquivos descritos no caput.

Art. 12. É vedada a inserção de informação confidencial, proprietária ou sensível da SEFAZ-RJ em ferramenta de inteligência artificial não homologada para uso pela SUBTIC.

Art. 13. Os dispositivos de TIC particulares conectados à rede da SEFAZ-RJ poderão ser inspecionados pela área competente, caso necessário.

§ 1º A responsabilidade pelo conteúdo armazenado nos recursos de TIC particulares é do usuário.

§ 2º Em nenhuma hipótese a SEFAZ-RJ se responsabilizará por danos em dispositivos pessoais, ainda que utilizados em conexão com o ambiente corporativo.

Art. 14. Os processos de manutenção, instalação, configuração, desinstalação, substituição e remanejamento de recursos de TIC da SEFAZ-RJ serão realizados exclusivamente pela SUBTIC, a qual poderá autorizar a realização dessas atividades mediante solicitação justificada.

Art. 15. As senhas são de uso pessoal e intransferível, devendo respeitar os padrões mínimos de segurança recomendados pelas boas práticas internacionais.

Art. 16. A utilização de autenticação multifator é obrigatória para acesso à rede ou a quaisquer ativos de TIC do ambiente corporativo da SEFAZ-RJ em que se faça necessária a autenticação de usuário, inclusive ambientes corporativos em nuvem.

CAPÍTULO III – DO MONITORAMENTO

Art. 17. Os ativos de TIC da SEFAZ-RJ serão continuamente monitorados.

§ 1º Os registros de uso (*logs*) em geral, os *e-mails,* os registros de acessos a sítios de internet, o histórico de navegação, o endereçamento IP, as condições aceitas e quaisquer outras informações de uso dos ativos de TIC devem ser armazenados de forma segura, por prazo estabelecido em norma específica.

§ 2º É vedada qualquer tentativa de alteração de registros de logs.

§ 3º Os registros de monitoramento serão classificados como restritos e só poderão ser acessados

por profissionais autorizados pela SUBTIC.

§ 4º Compete à SUBTIC adequar todos os ativos de TIC de maneira a viabilizar o monitoramento descrito no *caput.*

§ 5º Os gestores dos sistemas definirão os requisitos de *logs* que permitam auditoria de uso, sem prejuízo da competência da SUBTIC prevista no § 4º.

CAPÍTULO IV – DA GESTÃO DE IDENTIDADES E ACESSOS

Art. 18. A SEFAZ-RJ implementará gestão de identidades e acessos com promoção de equilíbrio entre segurança da informação e experiência do usuário, suportando os processos de negócio, atuando em conformidade com a legislação e aplicando controles apropriados contra fraude.

Art. 19. A gestão de identidades e acessos atenderá os seguintes requisitos:

I. adoção preferencial de controle de acesso baseado em perfis ou papéis (RBAC);

II. respeito ao princípio do privilégio mínimo; e

III. uso excepcional e precário de autorizações de acesso individuais.

Art. 20. Denomina-se Gestor de Usuário, no contexto de segurança da informação, o responsável pela gestão do vínculo de uma pessoa física ou jurídica com a SEFAZ-RJ do qual resulte a concessão de login de rede ou qualquer outro tipo de credencial de acesso ao ambiente corporativo.

Art. 21. Compete ao Gestor de Usuário:

I. gerir o vínculo da pessoa física ou jurídica com a SEFAZ-RJ, autorizando e revogando o ingresso no ambiente corporativo;

II. garantir a autenticidade do usuário recebedor de *login* de rede ou credencial de acesso; e

III. assegurar a assinatura do Termo de Sigilo e Confidencialidade pelo usuário.

Parágrafo Único. O gestor mencionado no *caput* corresponderá:

I. ao fiscal administrativo de contrato, nos casos de usuários que sejam prestadores de serviços vinculados à entidade contratada;

II. ao titular da unidade da SEFAZ-RJ responsável pela assinatura de convênio com pessoa jurídica que estabeleça a possibilidade de acesso ao ambiente corporativo; e

III. ao titular da Superintendência de Recursos Humanos da SEFAZ-RJ, em se tratando de usuários que sejam servidores, estagiários e nos demais casos.

Art. 22. O acesso a todo e qualquer ativo de TIC ocorrerá, preferencialmente, por meio de perfil de acesso padronizado, concedido mediante procedimentos automatizados.

Parágrafo Único. Na ausência de efetivação de acesso na forma do caput, este será concedido excepcional e precariamente de forma individual, desde que atendidos os requisitos do art. 24.

Art. 23. O processo de concessão de acesso individual a sistemas de informação, a bancos de dados corporativos ou a outros ativos de TIC que contenham informações é composto de três etapas:

I. autorização;

II. definição dos meios de acesso à informação; e

III. configuração do ativo.

Parágrafo Único. O processo previsto neste artigo deverá ser observado diante de qualquer grau de sigilo da informação, sempre em conformidade com a legislação.

Art. 24. Compete ao subsecretário hierarquicamente superior no setor que necessite da informação autorizar o acesso individual, considerando:

I. a real necessidade;

II. a confidencialidade da informação; e

III. o tipo de acesso (leitura, alteração, deleção) a ser autorizado.

§ 1º No caso de órgãos colegiados, a competência para autorização será do presidente ou da respectiva autoridade máxima.

§ 2º Inexistindo subsecretaria hierarquicamente superior ao setor do usuário que necessite da informação e não correspondendo à hipótese do § 1º deste artigo, competirá à Subsecretaria Geral da Fazenda decidir acerca da autorização.

§ 3º A autorização concedida deverá conter termo de validade, não podendo superar 12 (doze) meses.

Art. 25. A SUBTIC definirá os meios de acesso à informação, no que tange a seus aspectos técnicos, levando em consideração a necessidade do requisitante e vedada a concessão de acesso direto ao banco de dados para usuários externos.

§ 1º Para a efetivação do disposto no caput, os meios mais seguros, eficientes e amigáveis aos usuários deverão ser buscados.

§ 2º A concessão de acesso direto a bancos de dados a usuários do ambiente corporativo da SEFAZ somente será realizada nas hipóteses de inexistência de outro meio viável, devendo ser revogada tão logo sobrevenha alternativa.

Art. 26. Após autorização e definição do meio de acesso, a realização da configuração das credenciais de acesso referentes à solicitação ficará a cargo do gestor do ativo de TIC, o qual corresponderá:

I. ao gestor do sistema, em se tratando de sistemas corporativos, transacionais ou analíticos, nos termos da Resolução SEFAZ Nº 509 de 31 de março de 2023;

II. ao responsável designado para a concessão das credenciais no setor atinente à Governança de Dados da SUBTIC, em se tratando de acesso a dados diretamente em bancos de dados corporativos; ou

III. ao Service Desk, para os demais ativos de TIC.

CAPÍTULO V – DA AUDITORIA E CONFORMIDADE

Art. 27. Auditorias de verificação de conformidade em segurança da informação poderão ser realizadas periodicamente pela SUBTIC visando à adequação e ao aprimoramento dos controles de segurança aos objetivos estabelecidos por esta Política e pelas demais normas e procedimentos de segurança da informação.

§ 1º A periodicidade das auditorias poderá ser definida em função dos riscos associados aos recursos de TIC e da sensibilidade das informações.

§ 2º Os procedimentos e autorizações de auditoria serão classificados como restritos.

Art. 28. A SEFAZ-RJ poderá auditar e realizar inspeções nos ativos de TIC próprios ou naqueles que interajam com seus ambientes lógicos ou físicos.

CAPÍTULO VI – DOS SISTEMAS DE INFORMAÇÃO

Art. 29. O desenvolvimento, a aquisição e a manutenção de sistemas, produtos e serviços de TIC devem atender aos requisitos de segurança definidos pela SUBTIC.

Parágrafo Único. O processo de atribuição de credenciais para usuários externos em sistemas será objeto de regulamentação própria que contemplará critérios mínimos atinentes à segurança da informação.

Art. 30. Os *softwares* adquiridos de terceiros e aqueles que estejam de posse da SEFAZ-RJ não podem ser copiados, salvo se houver previsão nos termos de licenciamento de *software* e desde que previamente autorizado.

Art. 31. Desde a concepção de uma solução tecnológica e durante todo o seu processo de desenvolvimento, a segurança da informação deve ser pautada considerando que as vulnerabilidades podem decorrer de tecnologia, processos e pessoas.

Art. 32. No processo de desenvolvimento de Sistemas de Informação deverão ser adotadas metodologias, técnicas e testes de segurança e validação de *software* que visem à entrega de soluções com código seguro, confiáveis e com base em práticas que minimizem os riscos relacionados a vulnerabilidades técnicas.

Art. 33. A SUBTIC deverá garantir a manutenção da atualização tecnológica e de segurança dos servidores, *frameworks*, componentes e demais sistemas de suporte enquanto estes sistemas estiverem ativos e em uso.

CAPÍTULO VII – DA SUBSECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 34. Sem prejuízo das outras atribuições contidas nesta norma, SUBTIC terá por responsabilidade:

I. definir os requisitos de segurança da informação e os controles adequados para a proteção das informações e recursos de TIC da Instituição;

II. estabelecer parâmetros de segurança adequados para a disponibilização de serviços, de sistemas e da infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais da SEFAZ-RJ;

III. gerenciar a estrutura de segurança dos recursos de TIC para que os objetivos estabelecidos na Política e demais normas e procedimentos em vigor sejam alcançados;

IV. executar as atividades técnicas e operacionais visando atender às orientações desta Política e prestar o suporte necessário ao esclarecimento de dúvidas dos usuários;

V. disponibilizar e prover a manutenção das ferramentas necessárias para viabilizar a implementação das diretrizes descritas nesta Política, em todo o ambiente computacional da SEFAZ-RJ;

VI. identificar e avaliar os riscos relacionados aos ativos intangíveis, recursos de TIC, dados e informações e promover melhorias nos controles existentes;

VII. implementar e atualizar os controles de segurança para a proteção das informações e dos recursos de TIC da SEFAZ-RJ e apoiar as demais áreas em suas necessidades relacionadas à segurança da informação;

VIII. gerenciar os incidentes de segurança da informação, desenvolvendo capacidades para sua detecção, tratamento e prevenção;

IX. prover mecanismos para detecção e remoção de códigos maliciosos e combate a atividades anormais;

X. analisar e avaliar casos de violações e demais eventos negativos relativos à segurança da informação na SEFAZ-RJ, inclusive quando envolver a internet e as mídias sociais;

XI. realizar programas de segurança ofensiva, visando a detectar fragilidades ou falhas de segurança nos ambientes físicos e lógicos;

XII. prover mecanismos de autenticação e registro que determinem a titularidade de todos os acessos a recursos de TIC;

XIII. realizar programas de conscientização em segurança da informação com envolvimento dos usuários e suas chefias, estimulando o cumprimento da Política e aprimorando a cultura em segurança da informação;

XIV. orientar os usuários a respeito das responsabilidades e dos procedimentos de segurança acerca dos recursos de TIC que lhes forem disponibilizados; e

XV. monitorar os dados e informações da SEFAZ-RJ em trânsito ou armazenados em recursos de TIC institucionais ou particulares.

Art. 35. Observada a competência do Comitê de Governança da Segurança da Informação, a SUBTIC poderá disciplinar por intermédio de Portaria:

I. o uso aceitável de recursos de TIC da SEFAZ-RJ;

II. os requisitos e condições para utilização de dispositivos particulares em conexão à rede corporativa;

III. observado o disposto no parágrafo único deste artigo, a segurança física do ambiente, englobando o regramento acerca dos mecanismos de proteção às instalações físicas e às áreas de processamento das informações;

IV. a política de senhas;

V. o uso de assinatura eletrônica;

VI. os meios de acesso à informação;

VII. outros temas pertinentes relacionados com a segurança da informação.

Parágrafo Único. A norma correspondente ao inciso III deste artigo deverá ser editada em conjunto com a Subsecretaria de Administração.

TÍTULO III - DAS DISPOSIÇÕES FINAIS

Art. 36. Esta Resolução deverá ser observada quando da assinatura de contratos, convênios, ajustes, acordos de cooperação, termos de colaboração, termos de fomento, ou qualquer outro instrumento formalizado pela SEFAZ-RJ.

Art. 37. A SUBTIC poderá regulamentar temas específicos objeto desta política mediante edição de Portaria.

Art. 38. Revoga-se a Resolução SEFAZ nº 244 de 18 de abril de 2018 - Política de Segurança da Informação, bem como seus anexos: Política de Segurança da Informação - Norma: 001-N1: Diretrizes Gerais; Norma 002-N1: Acesso à Internet; Norma 003-N1: Acesso à informação; Norma 004-N1: Uso do Correio Eletrônico; e Norma 005-N1: Gestão de *Backup.*

Art. 39. Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro, 28 de dezembro de 2023

LEONARDO LOBO PIRES
Secretário de Estado de Fazenda

Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda

RESOLUÇÃO SEFAZ N.º 649 DE 10 DE MAIO DE 2024

INSTITUI A POLÍTICA DE USO DO CORREIO ELETRÔNICO CORPORATIVO NA SEFAZ-RJ, DEFININDO DIRETRIZES PARA SEGURANÇA E PRIVACIDADE DAS INFORMAÇÕES EM CONFORMIDADE COM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

O SECRETÁRIO DE ESTADO DE FAZENDA, no uso de suas atribuições constitucionais e legais, de acordo com o inciso I do Parágrafo único do art. 148 da Constituição do Estado do Rio de Janeiro, tendo em vista o disposto no Decreto nº 31.896/2002, e ainda o que consta no Processo nº SEI-040005/000035/2024; e

CONSIDERANDO:

- A necessidade de estabelecer diretrizes claras para o uso do serviço de correio eletrônico corporativo (*e-mail*), visando a melhoria da comunicação interna e externa, a segurança dos dados, e a promoção da integridade e transparência nas comunicações da Secretaria de Estado de Fazenda (SEFAZ-RJ);
- A importância de alinhar as práticas da SEFAZ-RJ aos padrões internacionais de segurança da informação e procedimentos internos; e
- A Política de Segurança da Informação (PSI) instituída pela Resolução SEFAZ n° 599 de 28 de dezembro de 2023.

RESOLVE:

CAPÍTULO I - DA POLÍTICA DE USO

Art. 1º Fica instituída a Política de Uso do Serviço de Correio Eletrônico Corporativo aplicável a todos os usuários no âmbito da SEFAZ-RJ.

Art. 2º Para os fins deste ato, considera-se:

I- Caixa postal corporativa: área de armazenamento contendo as mensagens do *e-mail* corporativo;

II- Caixa postal individual: espécie do gênero caixa postal corporativa que seja atribuída a uma única pessoa física;

III- Caixa postal institucional ou coletiva: espécie do gênero caixa postal corporativa atribuída a uma unidade organizacional da SEFAZ-RJ, podendo ser acessado por múltiplos usuários.

IV- *E-mail*: Correio Eletrônico;

V- Endereço de *e-mail* corporativo: aquele pertencente ao domínio @fazenda.rj.gov.br;

VI- Endereço de *e-mail* individual: utilizado por uma pessoa física para enviar e receber mensagens

do domínio @fazenda.rj.gov.br

VII- Endereço de *e-mail* institucional: utilizado por um conjunto de usuários para receber e enviar mensagens referentes a uma unidade organizacional da SEFAZ-RJ e pertencente ao domínio @fazenda.rj.gov.br;

VIII- PSI: Política de Segurança da Informação da SEFAZ, instituída pela Resolução SEFAZ nº 599, de 2023;

IX- Serviço de *e-mail* corporativo: sistema de mensagens utilizado para criar, encaminhar, responder, transmitir, arquivar, manter, copiar, ler ou imprimir informações, com o propósito de estabelecer comunicações, relacionadas com as funções institucionais da SEFAZ-RJ, entre redes de computadores, entre pessoas e entre grupo de pessoas; e

X- Usuário: conforme PSI, inclui funcionários, servidores, estagiários, prestadores de serviço, terceirizados, conveniados, credenciados, fornecedores ou qualquer indivíduo ou organização com relação direta ou indireta com a SEFAZ-RJ.

CAPÍTULO II – DAS DIRETRIZES GERAIS

Art. 3º A Política de Uso do Serviço de Correio Eletrônico Corporativo visa estabelecer diretrizes para o uso seguro e adequado do *e-mail* corporativo da SEFAZ-RJ, protegendo a privacidade e segurança das informações

Art. 4º O serviço de e-mail corporativo deve ser utilizado exclusivamente para fins profissionais, vedada sua utilização para finalidades pessoais ou disseminação de conteúdos não relacionados às atribuições da SEFAZ-RJ.

Parágrafo Único - É proibido o uso do *e-mail* corporativo para enviar ou receber conteúdos que infrinjam leis, violem direitos autorais, sejam de natureza sexual explícita, discriminatória, constituam assédio ou contrariem os princípios éticos e morais da SEFAZ-RJ..

Art. 5º O usuário é responsável pelo conteúdo de mensagens que enviar por meio do *e-mail* corporativo.

Art. 6º Todas as mensagens enviadas por meio do serviço de *e-mail* corporativo devem possibilitar que o destinatário identifique o servidor remetente.

Parágrafo único: As mensagens enviadas a partir de caixas postais individuais presumem-se identificadas a partir do campo remetente.

Art. 7º As assinaturas insertas no corpo de texto das mensagens de *e-mails* corporativos deverão seguir o padrão oficial.

CAPÍTULO III – DAS CAIXAS POSTAIS INDIVIDUAIS

Art. 8º As caixas postais individuais são de uso pessoal e intransferível, sendo proibido o acesso

por terceiros, salvo nas hipóteses previstas na PSI.

Art. 9º As mensagens originadas de caixas individuais estão diretamente vinculadas a um usuário, que se presumirá autor das mensagens.

Art. 10º. O formato dos endereços de e-mail individuais seguirá padrão definido pela Subsecretaria de Tecnologia da Informação e Comunicação (SUBTIC).

CAPÍTULO IV – DAS CAIXAS POSTAIS INSTITUCIONAIS OU COLETIVAS

Art. 11 A gestão das caixas postais institucionais ou coletivas, incluindo criação, alteração, exclusão e gerenciamento de acesso, é responsabilidade do titular da unidade organizacional correspondente e dependem de pedido expresso e motivado.

Art. 12 Todas as mensagens eletrônicas originadas de *e-mails* institucionais ou coletivos devem identificar claramente o servidor autor, contendo no corpo da mensagem seu nome completo e identificador funcional (ID Funcional), proibindo-se o anonimato.

Art. 13 No caso de mensagens eletrônicas originadas de *e-mail* institucional de autoria de prestadores de serviço, terceirizados, conveniados, ou qualquer outra hipótese de usuário que não seja servidor, a mensagem deverá conter nome completo do autor e nome da instituição que tenha o vínculo com a SEFAZ.

Art. 14 É de responsabilidade do titular da unidade organizacional correspondente ao *e-mail* institucional:

I – Gerenciar o acesso à caixa institucional correspondente, adicionando e removendo usuários conforme a necessidade;

II – Supervisionar o uso da caixa a fim de assegurar o cumprimento desta Política.

CAPÍTULO V – DO USO ADEQUADO

Art. 15 Define-se como uso adequado do *e-mail* corporativo a finalidade profissional, a observância da confidencialidade, o respeito no trato, a diligência na verificação da caixa de entrada e a não utilização para comunicações de caráter urgente, preferindo-se outros meios:

I. Finalidade Profissional: o *e-mail* deve ser utilizado exclusivamente para fins profissionais relacionados ao trabalho na SEFAZ-RJ.

II. Confidencialidade: devem ser sempre observadas as normas atinentes à Proteção de Dados.

III. Respeito: os usuários devem manter a urbanidade e o profissionalismo nas comunicações por *e-mail*, evitando linguagem ofensiva, difamatória ou imprópria.

IV. Diligência: a caixa de entrada deve ser verificada no mínimo diariamente pelos usuários ativos.

V. Não urgência: por sua natureza técnica, as mensagens de correio eletrônico não são adequadas para comunicar situações emergenciais ou urgentes, sendo preferível, nesses casos, a utilização alternativa ou concomitante de outros meios de comunicação tais como a forma pessoal, a telefonia por

voz ou a mensagem instantânea eletrônica.

Art. 16 São vedados o anonimato, o acesso por terceiros à caixa postal individual, o envio de spam ou phishing, o uso malicioso ou ilegal, e o uso de *e-mails* de domínios não corporativos para fins profissionais:

I. Anonimato: é proibido deixar de se identificar em mensagem enviada por meio de caixa institucional, bem como valer-se de qualquer método para ocultar sua identidade ou de terceiros em uma mensagem enviada.

II. Uso do *e-mail* individual por terceiros: por ter caráter personalíssimo, é proibido acessar a caixa de e-mail individual de outros usuários, ressalvados os casos previstos pela PSI.

III. *Spam* ou *Phishing*: é proibido enviar mensagens não solicitadas (*spam*) ou tentar obter informações confidenciais por meio de técnicas de *phishing*, ressalvados os casos previstos pela PSI.

IV. Uso malicioso ou ilegal: é proibido o envio de vírus, *malware* ou de qualquer conteúdo malicioso por meio do serviço de *e-mail* corporativo, ressalvados os casos previstos pela PSI.

V. Uso de serviço de *e-mail* de domínios não corporativos: é proibido o uso de serviço de *e-mail* de domínios não corporativos para finalidades profissionais.

CAPÍTULO VI - DAS DISPOSIÇÕES FINAIS

Art. 17 Auditorias serão realizadas regularmente para verificar a aderência a esta política.

Art. 18 A inobservância das disposições aqui contidas sujeita o infrator às medidas disciplinares aplicáveis, conforme legislação estadual vigente.

Art. 19 Esta resolução entra em vigor na data de sua publicação.

LEONARDO LOBO PIRES
Secretário de Estado de Fazenda
ID 5097684-2

Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda

RESOLUÇÃO SEFAZ N.º 547 DE 12 DE JULHO DE 2023

ESTABELECE PROCEDIMENTOS DE BLOQUEIO DE ACESSO AOS SISTEMAS E AOS BANCOS DE DADOS CORPORATIVOS DA SECRETARIA DE ESTADO DE FAZENDA DO ESTADO DO RIO DE JANEIRO

O SECRETÁRIO DE ESTADO DE FAZENDA DO RIO DE JANEIRO, no uso de suas atribuições constitucionais e legais, e o que consta no Processo SEI-040227/000130/2022,

CONSIDERANDO:

- a ABNT NBR ISO 27002:2013, a ABNT NBR ISO/IEC 27001:2013 e a ABNT NBR ISO/IEC 27005:2019, atinentes à segurança da informação;

- a Instrução Normativa PRODERJ/PRE Nº 02 de 28 de abril de 2022;

- a necessidade de garantir o sigilo fiscal, a integridade, a confidencialidade e a disponibilidade das informações sob gestão da SEFAZ-RJ.

RESOLVE:

Art. 1º Estabelecer os procedimentos de bloqueio de acesso aos sistemas e aos bancos de dados corporativos da Secretaria de Estado de Fazenda do Estado do Rio de Janeiro nos casos previstos no art. 2º.

Art. 2º A Subsecretaria de Administração (SUBADM), através da Superintendência de Recursos Humanos (SUPRH), deverá efetuar o procedimento de bloqueio de acesso do usuário por meio de sistema informatizado nas seguintes hipóteses:

I – exoneração;

II – demissão ou destituição de função;

III – cessão;

IV – aposentadoria;

V – licenças e afastamentos superiores a 180 dias.

§1º O disposto no *caput* não se aplica aos casos de remoções internas realizadas no âmbito da SEFAZ-RJ.

§2º O bloqueio de acesso deverá ser realizado no menor tempo possível, respeitando o limite

máximo de 5 dias úteis, contados a partir da publicação do ato no Diário Oficial.

Art. 3º A Subsecretaria de Tecnologia da Informação e Comunicação (SUBTIC), através do *Service Desk*, deverá efetuar o procedimento de bloqueio de acesso do usuário nos casos de estagiários, menor estagiário da Fundação da Infância e Adolescência e de trabalhadores terceirizados que não dependam de ato de publicação no Diário Oficial para seu devido desligamento.

§1º Os chefes dos setores e responsáveis por trabalhadores terceirizados deverão solicitar o bloqueio do acesso aos sistemas previstos nesta resolução através de abertura de ordem de serviço junto ao *Service Desk.*

§2º Fica a SUBADM, por meio da SUPRH, responsável por enviar solicitação de bloqueio do acesso aos sistemas à SUBTIC, através de abertura de ordem de serviço junto ao *Service Desk*, no caso de desligamento de estagiários e de menor estagiário da Fundação da Infância e Adolescência.

Art. 4º Executado o procedimento de bloqueio, o usuário ficará, imediatamente e automaticamente, impedido de acessar todos os sistemas e bancos de dados corporativos da SEFAZ-RJ.

Art. 5º Caberá à Subsecretaria de Tecnologia da Informação e Comunicação a disponibilização e manutenção do mecanismo de bloqueio.

Art. 6º As regras de acesso aos sistemas serão disciplinadas em regulamentação específica acerca dos processos de tecnologia da informação e comunicação no âmbito da SEFAZ-RJ.

Art. 7º Caberá ao Comitê Gestor de Segurança da Informação – CGSI o tratamento dos casos omissos não previstos no artigo 2º.

Art. 8º Ficam a SUBTIC e a SUBADM autorizadas a editarem atos próprios visando a implementação e adequação do fluxo processual em consonância com o disposto na presente resolução.

Art. 9º Esta Resolução entra em vigor na data de sua publicação.

Rio de Janeiro, 12 de julho de 2023

BRUNO SCHETTINI
Secretário de Estado de Fazenda
Substituto

Secretaria de
Fazenda

GOVERNO DO ESTADO
RIO DE JANEIRO