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

Documento assinado eletronicamente por **Leonardo Lobo Pires**, **Secretário de Estado**, em 28/12/2023, às 17:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **66075127** e o código CRC **15D9BA1C**.

Referência: Processo nº SEI-040227/000356/2023 SEI nº 66075127