DIÁRIO OFICIAL DA UNIÃO

Publicado em: 28/07/2022 | Edição: 142 | Seção: 1 | Página: 141

Órgão: Ministério do Turismo/Fundação Cultural Palmares

PORTARIA FCP Nº 159, DE 26 DE JULHO DE 2022

Dispõe sobre as diretrizes básicas da tecnologia da informação e institui a Política de Segurança da Informação - POSIN no âmbito da Fundação Cultural Palmares- FCP.

O PRESIDENTE SUBSTITUTO DA FUNDAÇÃO CULTURAL PALMARES, no uso das atribuições que lhe foram conferidas pelo art. 18, III, do Anexo I, do Decreto nº 6.853, de 15 de maio de 2009 e observadas as determinações contidas no Decreto nº 9.637, de 26 de dezembro de 2018 e Portaria Mtur nº 108, de 22 de maio de 2013, e o que consta dos autos do processo nº 01420.100625/2022-14, resolve:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Seção I

Objeto e campo de aplicação

Art. 1º Fica instituída a Política de Segurança da Informação - POSIN que objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações custodiadas e de propriedade da Fundação Cultural Palmares, de modo a preservar os seus ativos e sua imagem institucional.

Art. 2º A POSIN trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da FCP, em todo o seu ciclo de vida criação, manuseio, divulgação, armazenamento, transporte e descarte, visando a continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3º Os objetivos e diretrizes estabelecidos nesta POSIN serão desenvolvidos para toda a FCP, incluindo nesta política, os colaboradores, servidores, estagiários, terceirizados, prestadores de serviços, e aplicam aos ambientes, sistemas, pessoas e processos, tanto em meio digital quanto nos meios analógicos de processamento, comunicação e armazenamento de informações.

Art. 4º A alta direção da FCP deve manter postura exemplar em relação à segurança da informação e comunicação, bem como propiciar os recursos necessários para divulgações, capacitações, sensibilização e cumprimentos das normas e procedimentos.

Art. 5º São objetivos da Política de Segurança da Informação - POSIN da FCP:

I - estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

II - apoiar a implantação das iniciativas relativas à Segurança da Informação e Comunicações; e

III - possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

Art. 6º Integram também a POSIN as normas, metodologias e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Seção II

Conceitos e Definições

Art. 7º Para os efeitos desta POSIN e, considerando o Glossário de Segurança da Informação, estabelecido pela Portaria GSI/PR nº 93, de 26 de setembro de 2019, entende-se por:

I - ativo - qualquer coisa que tenha valor para a organização;

II - autenticidade - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade

III - confidencialidade - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IV - disponibilidade - propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

V - gestão de riscos - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança quanto à realização de seus objetivos;

VI - gestão de segurança da informação - ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VII - gestor de segurança da informação - responsável pelas ações de segurança da informação, no âmbito do órgão ou entidade da Administração Pública Federal

VIII - incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IX - incidente - evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

X - informação - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XI - informação classificada - informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

XII - integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIII - perfil de acesso - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XIV - plano de continuidade de negócios - documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

XV - quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

XVI - risco (de segurança da informação) - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização

XVII - Segurança da Informação -SI - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVIII - sensibilização - atividade que tem por objetivo atingir uma predisposição dos participantes para uma mudança de atitude sobre a segurança da informação, de tal forma que eles possam perceber em sua rotina pessoal e profissional ações que devem ser corrigidas. É uma etapa inicial da educação em segurança da informação; e

XIX - usuário - pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade

Seção III

Princípios da Política de Segurança da Informação

Art. 8º São princípios da Política de Segurança da Informação -POSIN da FCP:

I - toda informação coletada, gerada, utilizada, em trânsito e armazenada por todos usuários deverá ser tratada como parte do patrimônio da FCP, devendo ser assegurada sua confidencialidade, integridade e disponibilidade, bem como a proteção de dados pessoais e conformidade legal;

II - todos os recursos de informação da FCP devem ser projetados para que seu uso seja consciente e responsável. Os recursos tecnológicos da instituição devem ser utilizados para a consecução de seus objetivos finalísticos;

III - deverão ser criados e instituídos controles apropriados, mapeamento de ativos, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que da FCP julgar necessário, com vistas à redução dos riscos dos seus ativos de informação;

IV - os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais (privilégios diferenciados associados a cada perfil), acessar arquivos e dados de outros usuários. Tal operação só será permitida quando necessária para a execução de atividades sob sua responsabilidade;

V - autorização definida pelos gestores: definir acessos e cancelar acessos aos recursos e aos locais restritos com base na solicitação do gestor de cada Unidade Organizacional, que também é responsável pelos ativos disponibilizados para uso;

VI - a segregação da administração e a execução de funções conflitantes ou áreas de responsabilidade críticas deverão ser implementadas para que ninguém detenha controle de um processo na sua totalidade, visando a reduzir os riscos de mau uso, acidental ou deliberado, dos ativos da FCP, salvo em condições devidamente justificadas;

VII - todo o acesso a redes e sistemas do órgão deverá ser feito por meio de credencial de acesso único, pessoal e intransferível, qualificando o titular como responsável por todas as atividades desenvolvidas por meio dela;

VIII - o acesso e o uso dos ativos devem ser controlados e limitados de acordo com as funcionalidades necessárias para o cumprimento das atividades dos usuários, no estrito interesse institucional, para cumprimento de finalidades profissionais, lícitas, éticas e devidamente autorizadas. Qualquer outra forma de acesso e uso necessitará de prévia autorização do proprietário do ativo de informação;

X - a FCP pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocadas sob suas instalações;

X - cada usuário é responsável pela segurança das informações na instituição, principalmente das informações que estão sob sua responsabilidade;

XI - todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema e justificados, acordados, documentados, implantados e testados durante a fase de execução;

XII - a gestão da segurança da informação será realizada pelo Comitê de Tecnologia da Informação;

XIII - deverá constar em todos os contratos celebrados, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação, bem como o atendimento à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018), a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades da FCP, inclusive provenientes de organismos internacionais;

XIV - nos contratos de prestação de serviços firmados pelo órgão deverá estar previsto que as empresas e profissionais prestadores de serviço devem entregar declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição, devendo ser realizada revisão de procedimentos, implementação de soluções tecnológicas e atualização documental para atender aos requisitos de controle e governança previstos nos arts. 43 e 50 da LGPD (gestão de riscos por contratos e códigos de conduta);

XV - somente será permitido o uso de ativos homologados e autorizados pela FCP, desde que sejam identificados de forma individual, inventariados, protegidos e tenham um proprietário responsável. Os ativos devem ter documentação atualizada, riscos mapeados, capacidade, manutenção e contingência adequadas e sua operação deve estar de acordo com essa Política de Segurança da Informação - POSIN , cláusulas contratuais e legislação em vigor;

XVI - os dados pessoais e a privacidade deverão ser protegidos de acessos não autorizados e de situações acidentais ou ilícitos de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequada ou ilícito que possa afetar a privacidade do titular;

XVII - a conscientização contínua deverá ser promovida com o objetivo de instruir, informar e capacitar os usuários sobre questões relacionadas à segurança da informação na execução de suas atividades, bem como sobre o cumprimento de suas responsabilidades relacionadas aos ativos com o objetivo de minimizar riscos;

XVIII - as diretrizes, normas e procedimento da POSIN deverão ser definidas, aprovadas pelo Comitê de Tecnologia da Informação, publicadas e comunicadas para todos os usuários e partes externas relevantes;

XIX - a identificação de quebra ou fragilidade na segurança da informação deverá ser comunicada a Divisão de Tecnologia da Informação - DTI; e

XX - a disponibilidade, o uso, o acesso e a proteção dos ativos que suportam os serviços e processos críticos deverão ser assegurados por meio de ações de administração de crise, prevenção e recuperação, com a implementação de estratégia de continuidade de negócios com o objetivo de mitigar possíveis interrupções causadas por desastres ou falhas.

Parágrafo único. A Política de Segurança da Informação -POSIN, prevista nesta Portaria, será implementada por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vínculo empregatício ou de prestação de serviço.

CAPÍTULO II

DIRETRIZES GERAIS

Seção I

Do Tratamento da Informação

Art. 9º O tratamento da informação na FCP deverá observar diretrizes específicas e procedimentos próprios e deverão ser fixados em norma complementar, considerando como diretrizes gerais as normas de classificação de informações, o acesso à informação, o uso e descarte de ativos de informação, e o tratamento de dados pessoais, dentre outros temas afins, que serão fixados em estrita observância às leis e normas atinentes à Administração Pública Federal, considerando as competências regimentais.

Seção II

Da Segurança Física e do Ambiente

Art. 10. A FCP deverá observar diretrizes específicas e procedimentos próprios de segurança física e do ambiente que deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - o acesso físico ao ambiente deverá ser monitorado e controlado;

II - agentes públicos e prestadores de serviços deverão ser identificados por meio do uso de crachá.

III - o acesso de visitantes as dependências do órgão deverá ser autorizado por servidor;

IV - agentes públicos e prestadores de serviços desligados deverão ser excluídos da relação de pessoas autorizadas para acessar as dependências; e

V - os arquivos físicos, assim como os digitais, deverão ser protegidos e estabelecidos em locais de acesso restrito e devidamente trancados em sala ou armário específico com o controle de acesso sob responsabilidade do gestor responsável pelos ativos.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 11. No tratamento de incidentes em redes computacionais, a Divisão de Tecnologia da Informação, responsável pelo tratamento e resposta aos incidentes, deverá considerar, a elaboração de um documento com relatos do incidente, no mínimo, as seguintes diretrizes:

I - todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;

II - o tratamento da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor; e

III - a ocorrência de incidentes de segurança em redes de computadores da FCP deverá ser comunicada ao Comitê de Tecnologia da Informação, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública federal, bem como a geração de estatísticas.

Seção IV

Da Gestão de Ativos

Art. 12. A gestão de ativos visa a estabelecer medidas de segurança pelo valor do ativo e em função dos riscos de impacto nos negócios, atividades e objetivos institucionais, com vistas à proteção de dados pessoais, à privacidade e à conformidade legal, implantando planos de contingência e de continuidade para os serviços e sistemas.

Seção V

Da Gestão do Uso dos Recursos Operacionais e de Comunicações

Subseção I

Do Correio Eletrônico

Art. 13. As diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico (e-mail) deverão ser fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - o serviço de correio eletrônico será oferecido como um recurso institucional para apoiar os seus usuários no cumprimento das atividades; e

II - o correio eletrônico deverá ser utilizado somente para fins corporativos e relacionados às atividades do usuário no âmbito da FCP, sendo vedado o uso para fins pessoais.

Subseção II

Do Uso e Acesso à Internet

Art. 14. As diretrizes específicas e procedimentos próprios de controles de uso e acesso à Internet serão fixadas em norma complementar, considerando as seguintes diretrizes gerais:

I - toda informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a FCP, de acordo com norma legal vigente, reserva-se no direito de monitorar e registrar os acessos à rede de computadores; e

II - os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da FCP, que pode analisar e, se necessário, bloquear qualquer arquivo, sítio, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privativas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação - POSIN.

Subseção III

Do Serviço de Backup

Art. 15. Os procedimentos próprios ao serviço de backup deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - o serviço de backup deve ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente;

II - a solução de backup deverá ser mantida sempre atualizada, considerando suas diversas características tais como atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros;

III - a administração das mídias de backup deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter a sua segurança e integridade;

IV - as mídias de backups deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres;

V - os backups críticos exigem uma regra de retenção especial; e

VI - a execução de rotinas de backup e de recuperação deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

Subseção IV

Do Uso Institucional das Redes Sociais

Art. 16. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações da FCP será regida por normas internas especificas e deverá estar em consonância com esta POSIN e com os objetivos estratégicos da FCP.

Art. 17. Os perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por equipes compostas exclusivamente por servidores públicos ocupantes de cargo efetivo.

Subseção V

Da Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Art. 18. As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação deverão observar os padrões, critérios e controles de segurança dispostos em normas e na legislação específica.

Subseção VI

Do Uso de Dispositivos Móveis

Art. 19. A unidade responsável pelos ativos de tecnologia deverá instituir normas e procedimentos específicos para o uso de dispositivos móveis que acessarem aos ativos de tecnologia da FCP, e atenderá às determinações desta POSIN.

Subseção VII

Dos Controles de Acesso

Art. 20. Ficam estabelecidas as diretrizes específicas e procedimentos próprios de controles de acesso lógico e físico deverão ser fixados em norma complementar, considerando as seguintes diretrizes gerais:

I - os usuários terão identificação única, pessoal e intransferível;

II - o controle de acesso deverá considerar e respeitar o princípio do menor privilégio, pelo qual cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades, para configurar as credenciais dos usuários aos ativos de informação da FCP por meio de sistema de acesso;

III - a criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário;

IV - contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;

V- o acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido em norma específica;

VI - as práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança; e

VII - da FCP poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da POSIN ou das normas e procedimentos específicos dela decorrentes.

Subseção VIII

Da Auditoria e Conformidade

Art. 21. Para garantir a aplicação das diretrizes mencionadas nesta norma, além de fixar normas e procedimentos complementares sobre o tema, da FCP poderá:

I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless (sem fio) e outros componentes da rede, de forma que a informação gerada por esses sistemas permitam a sua rastreabilidade, identificando usuários e respectivos acessos efetuados;

II - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gestor, seu superior ou por determinação do Comitê de Tecnologia da Informação;

III - realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

IV - instalar sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso; e

V - desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas, procedimentos e princípios vigentes.

CAPÍTULO III

DA ESTRUTURA PARA A GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 22. De forma a estruturar a gestão da segurança da informação, a FCP designará:

I - o Gestor de Segurança da Informação; e

II - o Comitê Gestor de Segurança da Informação e Comunicação - GSIC, com atuação por meio do Comitê de Tecnologia da Informação.

§ 1º O gestor de segurança da informação será designado dentre os servidores públicos ocupantes de cargo efetivo e militares de carreira, com formação ou capacitação técnica compatível com a legislação vigente.

§ 2º Caberá ao gestor de segurança da informação propor investimentos relacionados à segurança da informação com o objetivo de reduzir riscos, avaliar os incidentes de segurança, propor ações corretivas e definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação - POSIN e/ou das normas de segurança da informação complementares.

Seção I

Das competências da Gestão de Segurança da Informação

Art. 23. Compete ao gestor de segurança da informação:

I - coordenar a elaboração da Política de Segurança da Informação - POSIN e das normas internas de segurança da informação da FCP;

II - assessorar a alta administração na implementação da Política de Segurança da Informação - POSIN;

III - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV - promover a divulgação da política e das normas internas de segurança da informação da FCP a todos os servidores, usuários e prestadores de serviços que trabalham na FCP;

V - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VI - propor recursos necessários às ações de segurança da informação;

VII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

VIII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

IX - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Art. 24. São responsabilidades específicas do Gestor de Segurança da Informação:

I - deliberar sobre a implementação das ações de segurança da informação e utilização dos recursos da FCP;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Política de Segurança da Informação -POSIN e das normas internas de segurança da informação;

IV - propor alterações e revisar periodicamente a Política de Segurança da Informação - POSIN da FCP, em conformidade com a legislação existente sobre o tema; e

V - propor, aprovar, alterar e revisar normas complementares e procedimentos internos de segurança da informação, em conformidade com a legislação existente sobre o tema.

Seção II

Das competências Gerais

Art. 25. São responsabilidades de todos os usuários de serviços de rede, tais como internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais da FCP, com o objetivo de assegurar a segurança orgânica:

I - zelar pela segurança de suas credenciais de acesso aos serviços e espaços físicos e de seus respectivos dados;

II - seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais da FCP;

III - utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da FCP;

IV - manter-se atualizado, em relação a esta e outras normas e procedimentos relacionados, buscando informações junto ao Gestor de Segurança da Informação da FCP sempre que não estiver absolutamente seguro quanto à obtenção, uso e/ou descarte de informações;

V - entender os riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes; e

VI - ser responsável por todo prejuízo ou dano que vier a sofrer ou causar à FCP, em decorrência da não obediência às diretrizes e normas referidas na Política de Segurança da Informação - POSIN e nas normas e procedimentos específicos dela decorrentes.

Art. 26. São responsabilidades específicas dos dirigentes da FCP:

I - tomar as ações necessárias para cumprir com suas atribuições, bem como dirimir eventuais dúvidas dos seus subordinados;

II - manter os processos de sua área aderentes às políticas, normas e procedimentos específicos de segurança da informação e comunicações da FCP;

III - submeter ao Gestor de Segurança da Informação o que for pertinente para o desenvolvimento de políticas específicas para o bom cumprimento da POSIN; e

IV - solicitar o bloqueio de acesso de usuário(s) por motivo de desligamento da FCP, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos da autarquia.

Art. 27. São responsabilidades específicas da Divisão de Tecnologia da Informação da FCP:

I - zelar pela eficácia dos controles de segurança da informação e comunicações utilizados e informar aos gestores e demais interessados dos riscos residuais;

II - configurar os recursos informacionais e computacionais concedidos aos usuários com todos os controles necessários para o cumprimento dos requisitos de segurança estabelecidos pelos procedimentos, normas e políticas de segurança da informação;

III - gerar e manter trilhas de auditoria com nível de detalhe para rastrear possíveis falhas e fraudes;

IV - prover segurança para sistemas com acesso público;

V - zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada usuário;

VI - administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos considerados críticos para a FCP;

VII - definir as regras para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional e/ou dedicados à visitação externa, exigindo-se o seu cumprimento dentro da FCP;

VIII - realizar, quando solicitado por chamado, o backup de ativo de TIC ,nos casos de movimentações internas, antes do ativo ser disponibilizado para outro usuário;

IX - planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão de forma segura;

X - atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, que será o encarregado pelo uso da conta, devendo ser observado que a responsabilidade pela gestão das credenciais de usuários externos é do gestor do contrato de prestação de serviços ou do gestor do setor em que o usuário externo desempenha suas atividades;

XI - proteger os ativos de informação da FCP contra códigos maliciosos;

XII - garantir, quando demandado por solicitação dos gestores, via chamado, o bloqueio de acesso de usuários por motivo de desligamento da FCP, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguarda dos ativos da FCP;

XIII - garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede operem com o relógio sincronizado com os servidores de tempo oficiais do Governo Brasileiro; e

XIV - monitorar o ambiente de TIC, gerando dados indicadores e históricos de uso da capacidade da rede e de seus equipamentos, tais como: tempo de resposta no acesso à internet e aos sistemas críticos, períodos de indisponibilidade no acesso à internet e aos sistemas críticos, incidentes de segurança e atividade de todos os usuários durante os acessos às redes externas, inclusive internet, por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos.

CAPÍTULO IV

DAS PENALIDADES

Art. 28. As ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de segurança da informação serão devidamente apuradas, sendo cabíveis aos responsáveis as sanções administrativas, civis e penais.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 29. A política de segurança, as normas e os procedimentos complementares serão revisados periodicamente segundo os prazos estabelecidos pelo Gestor de Segurança da Informação ou sempre que algum fato ou evento relevante acontecer, não excedendo a 4 (quatro) anos.

Art. 30. Os documentos integrantes da estrutura normativa de gestão de segurança da informação deverão ser divulgados para todos os servidores, colaboradores, estagiários, aprendizes e prestadores de serviços da FCP quando de sua admissão, e também publicadas na Intranet corporativa, de maneira que seu conteúdo fique amplamente disponível a seus colaboradores a qualquer tempo.

Art. 31. Os casos omissos e as dúvidas na aplicação da Política de Segurança da Informação - POSIN e suas normas complementares serão resolvidas pelo Divisão de Tecnologia da Informação.

Art. 32. Fica revogada a Portaria nº 207, de 23 de dezembro de 2009.

Art. 33. Esta Portaria entra em vigor em 1º de setembro de 2022.

MARCO ANTONIO EVANGELISTA DA SILVA