Boletim de Serviço Eletrônico em 06/05/2021

FUNDAÇÃO ALEXANDRE DE GUSMÃO

PORTARIA Nº 36, DE 06 DE MAIO DE 2021

Institui a Política de Segurança da Informação (PSI) da Fundação Alexandre de Gusmão.

O PRESIDENTE DA FUNDAÇÃO ALEXANDRE DE GUSMÃO, no uso das atribuições que lhe foram conferidas pelo art. 16 do anexo I do Decreto nº 10.099, de 6 de novembro de 2019, e em atendimento ao disposto na Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, R E S O LV E :

Art.1º Instituir a Política de Segurança da Informação (PSI), constante do Anexo I, no âmbito da FUNAG.

Art.2º Esta portaria entra em vigor na data de sua publicação.

ROBERTO GOIDANICH

Documento assinado eletronicamente por **Roberto Goidanich**, **Presidente**, em 06/05/2021, às 15:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.funag.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0044783** e o código CRC **25A1717A**.

ANEXO I

(Portaria nº 36, de 06 de maio de 2021)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I

ESCOPO E ABRANGÊNCIA

1. O presente documento trata da Política de Segurança da Informação (PSI) da Fundação Alexandre de Gusmão (FUNAG), com base no Decreto nº 10.332, de 28 de abril de 2020, e na Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), estabelecendo diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação, no campo da tecnologia da informação.

2. O objetivo da PSI é definir os padrões mínimos obrigatórios para o devido uso e proteção das informações criadas, recebidas, armazenadas, processadas e transmitidas, estabelecendo as atribuições e responsabilidades dos atores envolvidos, com vistas à promoção da segurança da informação no âmbito da FUNAG.

3. A PSI abrange os servidores, os estagiários e os colaboradores que, direta ou indiretamente, utilizam ou são responsáveis pelos sistemas informatizados ou pela infraestrutura ou por informações decorrentes da implementação das atividades meio/apoio ou finalísticas da Fundação, os quais serão tratados como usuários.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

4. A presente Política tem como base os conceitos e definições contidos no Glossário de Segurança da Informação, aprovado pela Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República, disponível no *link* https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de- 2019-219115663.

CAPÍTULO III

PRINCÍPIOS

5. As ações desenvolvidas no âmbito da PSI da FUNAG serão norteadas pelos seguintes princípios: responsabilidade, ética, auditabilidade, celeridade, proporcionalidade, integração e irretratabilidade.

CAPÍTULO IV

DIRETRIZES GERAIS

6. A PSI tem como diretrizes gerais: I - tratamento da informação; II - segurança física e do ambiente; III - gestão de incidentes em segurança da informação; IV - gestão de ativos; V - gestão do uso dos recursos operacionais e de comunicações (e-mail, acesso à Internet, mídias sociais, computação em nuvem, dentre outros); VI - controles de acessos pelos usuários; e VII - gestão de riscos, continuidade, auditoria e conformidade dos recursos de tecnologia da informação.

SEÇÃO I

TRATAMENTO DA INFORMAÇÃO

7. O tratamento das informações coletadas e armazenadas pela FUNAG obedecerá a Política de Classificação da Informação (PCI) e a Política de Proteção de Dados Pessoais (PPDP).

SEÇÃO II

SEGURANÇA FÍSICA E DO AMBIENTE

8. Com vistas a segurança física e do ambiente de tecnologia da informação da FUNAG, todos os abrangidos pela PSI deverão seguir as orientações abaixo:

8.1. os controles de acesso físico serão realizados de modo a restringir o acesso a equipamentos, documentos e suprimentos do ambiente tecnológico, bem como a proteção dos recursos computacionais, permitindo acesso apenas às pessoas autorizadas pela equipe de tecnologia da Fundação;

8.2. os recursos computacionais críticos deverão ser mantidos em ambientes reservados, monitorados e com acesso físico controlado, permitido o acesso apenas por pessoas autorizadas pela equipe de tecnologia da informação da Fundação;

8.3. a concessão, a alteração e o cancelamento de acesso ao parque tecnológico da Fundação serão objeto de análise e aprovação pela equipe de tecnologia da informação da Fundação; e

8.4. a equipe de tecnologia da informação da FUNAG, periodicamente, revisará os acessos aos ambientes tecnológicos reservados, restringindo-os, se necessário.

SEÇÃO III

GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

9. Para a gestão e respostas aos incidentes que possam comprometer a segurança da informação no âmbito da FUNAG, deverão ser observados os seguintes procedimentos:

9.1. o gestor de segurança da informação, que é o responsável pela área de tecnologia da informação, deverá ser informado, formalmente, pela equipe de tecnologia da informação da FUNAG, quando for identificada qualquer ameaça que possa resultar em eventual incidente de segurança:

9.1.1. a área técnica de tecnologia da informação, por meio dos recursos de detecção na rede, monitorará o tráfego de dados nos servidores de tecnologia da informação;

9.1.2. a equipe de tecnologia da informação, após identificado o alerta, analisará o problema e encaminhará formalmente o caso ao gestor de segurança da informação;

9.1.3. qualquer evento, mesmo que suspeito, deve ser analisado e validado rapidamente pela área de tecnologia da informação. Uma vez confirmada a ocorrência de um incidente, a análise do escopo deverá ser executada. Esta análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes.

9.2. a equipe de tecnologia da informação e o gestor de segurança da informação deverão considerar como notificações de um evento de segurança da informação:

9.2.1. violação da disponibilidade, confidencialidade ou integridade da informação;

9.2.2. inconformidade das políticas ou procedimentos;

9.2.3. alterações de sistemas sem controle;

9.2.4. funcionamento indevido de *software* ou *hardware* críticos; e

9.2.5. violação de acesso lógico.

9.3. qualquer usuário do ambiente tecnológico da FUNAG é responsável por relatar de imediato à área de tecnologia da informação todo tipo de evento e fragilidade que possam causar danos à segurança da informação.

9.4. a equipe de segurança da informação da FUNAG, no tocante ao tratamento do incidente de segurança da informação, deverá:

9.4.1. preservar, na medida do possível, todas as evidências para que seja identificado o problema e a possível causa;

9.4.2. verificar se existem planos de ação relacionados ao incidente e adotá-los quando necessário;

9.4.3. agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;

9.4.4. utilizar atividades de recuperação tais como: a restauração de *backup*s de sistemas, a instalação de *patches*, a alteração de senhas e a revisão da segurança do perímetro da rede da FUNAG;

9.4.5. registrar as ações envolvidas nas respostas aos incidentes para futuras análises, compondo banco de conhecimento para resposta em incidentes semelhantes; e

9.4.6. realizar, a cada três meses, uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las.

10. No combate a *software* malicioso, no âmbito da FUNAG, deverão ser observados os seguintes procedimentos:

10.1. os servidores de tecnologia da informação, físicos e virtuais, as estações de trabalho, os dispositivos móveis e os dispositivos de segurança da informação deverão estar protegidos com sistemas de proteção contra *softwares* maliciosos e atualizados periodicamente, conforme disponibilização de versão do fabricante;

10.2. os controles de detecção, prevenção e combate a *softwares* maliciosos serão objeto de rotinas da área de tecnologia de informação e orientações a serem encaminhadas aos usuários;

10.3. o usuário deve estar atento quanto ao funcionamento e atualização do *software* antivírus e, quando houver divergência, acionar a equipe de tecnologia da informação para as devidas providências;

10.4. apenas a equipe de tecnologia da informação poderá realizar a instalação de *softwares* no ambiente tecnológico. Em caso de necessidade específica de alguma das áreas da Fundação, o titular da unidade deverá encaminhar pedido formal à equipe de tecnologia da informação para análise e autorização; e

10.5. os sistemas de proteção contra *softwares* maliciosos devem ser instalados pela equipe de tecnologia da informação da FUNAG, com controles que não permitam alteração de sua configuração ou remoção da ferramenta, por usuários não autorizados.

SEÇÃO IV

GESTÃO DE ATIVOS

11. Os ativos de tecnologia da informação são todos os componentes de tecnologia da FUNAG, sejam eles virtuais ou físicos. Para a gestão desses ativos deverão ser observadas as seguintes

orientações:

11.1. os ativos de tecnologia da informação da FUNAG são de uso exclusivo para a realização de atividades institucionais;

11.2. nos processos de gestão dos ativos, devem ser considerados os ciclos de vida, que compreendem o planejamento, a aquisição, a implantação, o gerenciamento e o descarte;

11.2.1. o planejamento da aquisição de um ativo deverá estar alinhado com o Plano Anual de Compras da FUNAG. O planejamento de aquisições em TI envolve a revisão dos ativos que estão em uso na Fundação e a análise dos custos de compra e instalação;

11.2.2. a aquisição de ativos considerará os padrões técnicos, definidos no Termo de Referência;

11.2.3. no processo de implantação de ativos adquiridos, deverão ser realizadas as instalações e as configurações, levando em conta os critérios de segurança estabelecidos nesta PSI;

11.2.4. o gerenciamento do ativo inclui as ações de monitoramento, manutenção e atualização;

11.2.5. o descarte de um ativo deverá ser realizado quando o bem perde sua utilidade e torna-se antieconômico, alterando a sua classificação para material ocioso, antieconômico ou irrecuperável.

11.3. os ativos físicos ou de *software* da FUNAG devem ser preferencialmente padronizados e disponibilizados conforme perfil do usuário; e

11.4. os ativos físicos portáteis (*notebooks* e outros), sempre que possível, deverão permanecer nas instalações da FUNAG para evitar exposição e risco de furto ou roubo, podendo ficar sob a responsabilidade de servidores, autorizados previamente, por meio da assinatura de termos de responsabilidade.

SEÇÃO V

GESTÃO DO USO DOS RECURSOS OPERACIONAIS E DE COMUNICAÇÕES

12. A gestão do uso de recursos operacionais e de comunicação abrange a utilização da Internet, do correio eletrônico e das mídias sociais no âmbito da FUNAG.

SUBSEÇÃO I

INTERNET

13. O uso da Internet no âmbito da FUNAG deverá seguir as orientações básicas abaixo:

13.1. a Internet deve ser utilizada para as atividades relacionadas ao trabalho;

13.2. o acesso a recursos específicos da Internet será disponibilizado de acordo com as necessidades correspondentes ao perfil funcional de cada usuário; e

13.3. os *softwares* com as características *peer-to-peer*, o acesso a serviços de transferência de arquivos, bem como o uso de repositórios digitais devem ser solicitados formalmente à equipe de tecnologia da informação da FUNAG para análise e autorização.

14. O acesso à Internet de pessoas sem vínculo com a FUNAG deverá ser controlado e monitorado, quer seja em meio móvel (*wi-fi*) ou fixo:

14.1. a concessão de acesso à rede de visitantes deve estar associada à conscientização das diretrizes desta PSI.

SUBSEÇÃO II

CORREIO ELETRÔNICO

15. Apenas os usuários da FUNAG poderão ser credenciados a fazer uso do correio eletrônico institucional no âmbito da FUNAG, devendo ser seguidas as orientações abaixo:

15.1. o serviço de correio eletrônico adotado como institucional pela FUNAG deve ser conhecido e divulgado para todos os usuários, inclusive externos;

15.2. o correio eletrônico institucional deve ser priorizado e considerado como meio formal de comunicação eletrônica da FUNAG, em detrimento de qualquer outro disponível;

15.3. cada usuário deverá possuir sua própria conta de correio eletrônico e, caso haja necessidade de utilização de apenas um endereço para um grupo de usuários, essa solicitação deverá ser formalizada à CAFI;

15.4. todas as mensagens que forem enviadas pelos usuários da FUNAG devem estar em conformidade com os procedimentos de conduta ética e de segurança da informação, de forma que não será permitido o envio de mensagens ilegais, fraudulentas, difamatórias ou caluniosas;

15.5. a utilização incorreta do correio eletrônico institucional pode comprometer a segurança, o desempenho e a disponibilidade de acesso a sistemas e funcionalidades de tecnologia da informação disponibilizadas pela FUNAG, sendo que as mensagens não relacionadas às atividades institucionais desempenhadas na FUNAG não devem ser enviadas, respondidas ou encaminhadas;

15.6. o encaminhamento de mensagens em grande quantidade deve ser evitado. O encaminhamento de e-mails em massa para o público externo da FUNAG somente é possível ao Gabinete do Presidente e à Gerência de Projetos, por meio da utilização da ferramenta de *e-mail marketing* contratada pela Fundação;

15.7. os correios eletrônicos recebidos, contendo anexos de arquivos com código executável e outros normalmente utilizados para propagação de vírus devem ser automaticamente bloqueados por mecanismos no correio eletrônico do usuário; e

15.8. após o desligamento de servidor, colaborador ou estagiário, que seja usuário do correio eletrônico institucional, o chefe da área deverá demandar formalmente o bloqueio imediato da respectiva conta de correio eletrônico à equipe de tecnologia da informação da FUNAG.

SUBSEÇÃO III

REDES SOCIAIS

16. Os responsáveis pela inserção, acompanhamento e atualização de conteúdos nas redes socais deverão seguir as diretrizes abaixo sobre a utilização dos perfis institucionais da FUNAG:

16.1. a Gerência de Projetos, em conjunto com a chefia de Projetos de Eventos e Comunicação Digital, é a unidade responsável pela elaboração e inserção do conteúdo dos perfis institucionais da FUNAG nas redes sociais;

16.2. o conteúdo a ser inserido nas redes sociais deverá ser objeto de autorização do Presidente da FUNAG ou de seu substituto;

16.3. o Presidente da FUNAG, ou seu substituto, autorizará a criação e a exclusão de perfil institucional em redes sociais;

16.4. a Gerência de Projetos, em conjunto com a chefia de Projetos de Eventos e Comunicação Digital, responsável pelo gerenciamento do conteúdo dos perfis institucionais da FUNAG, estabelecerá rotinas e procedimentos com o intuito de minimizar os riscos, em cada rede social;

16.5. os responsáveis por manter os perfis institucionais da FUNAG em redes sociais deverão seguir o Manual de Uso de Redes Sociais publicado pela Secretaria Especial de Comunicação Social da Presidência da República, ou qualquer outro documento que venha substituí-lo.

17. Fica proibido o fornecimento ou a divulgação em redes sociais, sites de inscrições, grupos de discussão na Internet, dentre outros, de informações da FUNAG que não sejam autorizadas pelo Presidente da FUNAG ou seu substituto.

SEÇÃO VI

CONTROLES DE ACESSO

18. O controle de acesso dos usuários da FUNAG seguirá as seguintes diretrizes:

18.1. para cada ambiente tecnológico que seja necessária a inserção de usuários e senha, será criada conta de acesso por usuário;

18.2. não é permitido o reaproveitamento das contas de acesso para outros usuários;

18.3. não é permitido que os usuários compartilhem suas contas e senhas de acesso;

18.4. os usuários não podem realizar qualquer procedimento não autorizado em seus perfis ou nos perfis de grupo;

18.5. não é permitida a criação nem utilização de contas genéricas;

18.6. as chefias imediatas são responsáveis por requisitar as credenciais de acesso do usuário, definindo o perfil de acesso, quando for o caso, bem como informar imediatamente à área de tecnologia da FUNAG para que seja cancelado o acesso, senha e perfil de algum usuário, quando necessário;

18.7. qualquer bloqueio imediato aos sistemas administrados pela FUNAG e aos sistemas estruturantes do Governo Federal deve ser encaminhado formalmente à área de tecnologia da informação;

18.8. os acessos privilegiados, por questões de segurança, devem ser solicitados, formalmente, com as devidas justificativas à equipe de tecnologia da informação, que analisará e submeterá à autorização do Presidente da FUNAG ou seu substituto;

18.9. a cada 90 (noventa) dias, a área de tecnologia da informação fará o levantamento das contas de acesso na rede da FUNAG, realizando o bloqueio naquelas com mais de 60 (sessenta) dias de inatividade.

19. Os usuários da FUNAG deverão seguir as orientações abaixo sobre o uso de senhas de acesso a sistemas no âmbito da FUNAG:

19.1. o usuário é o responsável pelo uso de suas credenciais de acesso. A senha é a principal ferramenta de autenticação, devendo ser individual, intransferível e mantida em segredo;

19.2. as senhas não devem ser trafegadas em mensagens de correio eletrônico, aplicativos de mensagens instantâneas, redes sociais ou outros formulários de uso de comunicação eletrônica;

19.3. as solicitações de recuperação de senhas, caso não haja recurso de recuperação de senha no sistema, devem ser solicitadas à equipe de tecnologia da informação da FUNAG;

19.4. os padrões de senha exigidos para acesso aos sistemas, aos serviços e aos dispositivos do ambiente tecnológico da FUNAG devem seguir as recomendações abaixo:

19.4.1. ter pelo menos seis caracteres;

19.4.2. ter caracteres alfanuméricos;

19.4.3. possuir funcionalidades de criptografia capaz de mascarar as senhas na tela, armazenadas e trafegadas, pelo sistema ou aplicação.

20. As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente.

21. Nos casos em que o sistema tecnológico utilizado permita, os registros de atividades com a respectiva identificação dos responsáveis pela requisição, aprovação, concessão, comprovação e revogação de acesso devem ser armazenados para fins de análise de segurança da informação e auditoria interna.

22. O acesso do público externo ao ambiente de tecnologia da informação da FUNAG deverá ser objeto de encaminhamento de requisição formal, com as devidas justificativas, para a área de tecnologia da informação com vistas a análise e autorização se pertinente.

SEÇÃO VII

GESTÃO DE RISCOS, CONTINUIDADE E AUDITORIA

23. A chefia da equipe de tecnologia da informação da FUNAG adotará ações referentes à gestão de riscos de tecnologia da informação, visando identificar os ativos de tecnologia relevantes e determinar ações de gestão apropriadas.

24. A equipe de tecnologia da informação adotará todos os procedimentos necessários para dar continuidade às atividades desempenhadas pela área, com vistas a garantir que os sistemas e o parque tecnológico da FUNAG estejam em pleno funcionamento.

25. Todo evento de segurança da informação deverá ser registrado, a fim de permitir a auditoria e a detecção de incidentes de segurança. Os controles de segurança de tecnologia implementados deverão ser testados para verificar sua efetividade e conformidade com esta política.

26. Toda interação do usuário e do visitante com os recursos tecnológicos da FUNAG deverá ser registrada, a fim de permitir possíveis auditorias.

CAPÍTULO V

COMPETÊNCIAS

27. O Comitê de Segurança da Informação, que participa da elaboração da presente PSI e das normas internas de segurança da informação, preservadas as demais atribuições definidas na Portaria FUNAG nº 51, de 29 de junho de 2020, tem as seguintes competências:

27.1. assessorar a implementação das ações de segurança da informação;

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

27.3. propor alterações à PSI e às normas internas de segurança da informação;

27.4. deliberar sobre normas internas de segurança da informação; e

27.5. outras atribuições que lhe forem cometidas pelo Presidente da FUNAG.

28. Ao Gestor de Segurança da Informação compete:

28.1. incentivar e promover a cultura da segurança da informação no âmbito da Fundação;

28.2. propor normas e procedimentos relativos à segurança da informação ao Comitê de Segurança da Informação;

28.3. coordenar as investigações dos danos decorrentes de quebras de segurança; e

28.4. comunicar todo incidente de segurança da informação à alta administração da Fundação, para que sejam tomadas a providências quanto ao encaminhamento do incidente ao Gabinete de Segurança Institucional da Presidência da República.

29. À equipe de tecnologia da informação da FUNAG compete:

29.1. executar ações de segurança da informação;

29.2. informar qualquer suspeita de quebra de segurança ao gestor de segurança da informação.

CAPÍTULO VI

PENALIDADES

30. As ações que violem esta PSI ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de segurança da informação serão devidamente apuradas pelo Gestor de Segurança da Informação e poderão ser aplicadas aos responsáveis sanções administrativas, penais e civis de acordo com a análise do fato.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

31. Esta PSI deverá ser revisada sempre que se fizer necessário, não devendo exceder o período máximo de quatro anos.

32. Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação.