Ministério da Cultura
Fundação Biblioteca Nacional

PORTARIA FBN Nº 089 DE 09 DE NOVEMBRO DE 2023.

O Presidente da FUNDAÇÃO BIBLIOTECA NACIONAL, no uso das Atribuições legais que lhe confere o Estatuto da Entidade, aprovado pelo Decreto n° 11.233, de 10 de outubro de 2022, publicado no Diário Oficial da União em 11 de outubro de 2022,

DECIDE:

Art.1º Aprovar o Plano de Segurança Orgânica - PSO da Fundação Biblioteca Nacional.

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

Marco Lucchesi
Presidente

Documento assinado eletronicamente por **Marco Americo Lucchesi**, **Presidente**, em 09/11/2023, às 16:58, conforme horário oficial de Brasília, com fundamento na MP nº - 2.200-2 de 24/08/2001, que institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

A autenticidade deste documento pode ser conferida no site https://sei.bn.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0126927** e o código CRC **1A42489E**.

ANEXO I

APRESENTAÇÃO

Com a finalidade de cumprir o objetivo estratégico de fortalecer a Segurança Institucional da Fundação Biblioteca Nacional. A Fundação Biblioteca Nacional resolveu priorizar a criação do Plano de Segurança Orgânica.

FINALIDADE

Estabelecer diretrizes e regras aplicáveis à Segurança Orgânica, visando proteger as instalações da instituição, os processos de negócio, os empregados e demais pessoas que atuam no âmbito da Fundação Biblioteca Nacional, bem como o sigilo das informações para garantir a continuidade dos negócios da instituição.

CONCEITOS

Política de Segurança

documento elaborado com base nos princípios da administração da FBN, no qual são estabelecidas as diretrizes, critérios e suportes administrativos aptos à implementação da Segurança da Informação, bem como sua estrutura e competências;

Segurança da Informação

ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

A segurança da informação abrange:

I. a segurança cibernética;

II. a defesa cibernética;
III. a segurança física;
IV. a proteção de dados organizacionais;
V. as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por pessoa física ou determinado sistema, órgão ou entidade;

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e não credenciado;

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Gestor de Segurança Orgânica: responsável pelas ações de Segurança da Informação;

Computer Security Incident Response Team - CSIRT: equipe de tratamento e respostas aos incidentes em redes computacionais com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança em computadores.

DIRETRIZES

A FBN manterá em sua estrutura organizacional, permanentemente, unidades nos níveis estratégico, tático e operacional responsáveis pelas ações e manutenções de segurança a longo, médio e curto prazo;

As demais áreas da FBN deverão elaborar procedimentos complementares às diretrizes instituídas pelos órgãos responsáveis pela segurança na FBN, quando se fizer necessário;

A Assessoria de Segurança Orgânica deve estabelecer diretrizes para disciplinar o controle do acesso físico e lógico na FBN, objetivando:

I. Proteger as instalações e as informações com ações preventivas;

II. Buscar sempre a segurança dos empregados e demais pessoas em casos de ações que venham a ameaçar a FBN;
III. Manter contingência dos ativos de serviço e de logística, contra tipos de risco, sinistro ou intrusão, mesmo na presença de condições ambientais adversas e/ou de agentes maliciosos.

Toda informação criada, adquirida ou custodiada pela FBN possui valor, portanto deve ser protegida conforme as diretrizes de segurança dispostas nos normativos da instituição e demais regulamentações em vigor;

Deverá ser instituído na estrutura da FBN o Comitê de Segurança da Informação, que será responsável por assessorar a implantação e gestão desta Política;

A FBN deverá dispor do Comitê, para dar tratamento e respostas a incidentes em redes computacionais;

Deverão ser preservadas as informações pessoais, proprietárias e os segredos comerciais, garantindo a disponibilidade, integridade, confidencialidade e autenticidade das informações;

Todos os sistemas de informação da FBN são passíveis de monitoramento de segurança a qualquer momento, devendo ser observado os limites impostos pela legislação em vigor;

As hipóteses de monitoramento de segurança da informação deverão ser motivadas e autorizadas pelo Assessor de Segurança Orgânica;

Constitui infração a esta Política qualquer ato que exponha a FBN a danos financeiros, efetivos ou potenciais à sua imagem, à segurança da informação, de recursos materiais ou humanos para propósitos não autorizados por lei.

O Plano de Segurança Orgânica permite que os padrões estabelecidos nos grupos de medidas de segurança sejam efetivamente alcançados em toda FBN, seja no planejamento, na gestão ou no gerenciamento da segurança institucional. Para tanto, faz-se necessário que os seus desdobramentos estejam alinhados com o planejamento estratégico, garantindo-se, assim, a integração dos níveis tático e operacional de cada unidade.

OBJETIVOS

I. Estabelecer normas de Segurança Institucional para a FBN Orientar os integrantes da FBN a respeito das normas de segurança;

II. Definir o planejamento e as ações necessárias à execução da atividade de Segurança Institucional no âmbito da FBN;
III. Estruturar a Segurança Institucional de forma sistêmica, abrangendo os conjuntos de medidas de segurança previstos neste Plano de Segurança Orgânica;
IV. Fomentar ações de prevenção e de proatividade para proteção e salvaguarda da FBN e de seus integrantes;
V. Planejar ações de auditoria, fiscalização e controle internos relacionados à
VI. Segurança Institucional;
VII. Contribuir para elaboração de projetos orçamentários e de capacitação de pessoal, relacionados à Segurança Institucional.

RESPONSABILIDADES

Compete ao Presidente da FBN

I. Zelar para que o Comitê de Segurança da Informação esteja em permanente funcionamento;
II. Promover a conscientização dos integrantes da Instituição quanto à importância da Segurança Orgânica;
III. Promover a integração dos diversos setores envolvidos na Segurança Orgânica, tais como comunicação social, gestão de pessoas, informática, engenharia e quaisquer outros cuja atividade tenha pertinência com o tema;
IV. Auxiliar o Gestor de Segurança Orgânica a dar publicidade oficial ao PSO da FBN, após homologação;
V. Disponibilizar os recursos humanos, materiais e financeiros necessários a atuação da atividade de Segurança Orgânica.

VI. Garantir a manutenção dos serviços terceirizados indispensáveis ao funcionamento seguro das unidades, atuando de forma conjunta com a Coordenação de Administração Geral visando novas contratações, aditamentos, entre outros;
VII. Designar o Assessor de Segurança Orgânica.

Compete à Diretoria Executiva

Garantir a disponibilidade de recursos necessários à institucionalização desta Política.

Compete ao Comitê de Segurança da Informação

Propor os normativos referentes a Segurança Orgânica, inclusive atualizações, quando necessário.

Compete ao Assessor de Segurança Orgânica

I. Instituir a ETIRC - Equipe de tratamento e respostas aos incidentes em redes computacionais
II. Elaborar os instrumentos normativos relativos à segurança da informação;
III. Promover ações de segurança a longo, médio e curto prazo;
IV. Supervisionar, fiscalizar e fazer cumprir o PSO na FBN;
V. Enviar o PSO para a direção da FBN, para fins de ciência, ponderação e posterior encaminhamento ao Presidente da FBN, a fim de conhecimento e consequente homologação e publicação;
VI. Orientar o Presidente da FBN para enviar o PSO a todos os envolvidos direta/indiretamente com a instituição para fins de ciência e cumprimento.

VII. Assessorar o Presidente da FBN na proposição e coordenação das medidas de segurança.
VIII. Solicitar auxílio aos Coordenadores da FBN, conforme o caso, nos incidentes de segurança.
IX. Com o auxílio das diversas Coordenadorias, elaborar e implementar o Plano de Segurança Orgânica
X. Assessorar na homologação e publicação do PSO.

Compete ao Departamento de Recursos Humanos – DRH

Incluir o tema segurança em programa de integração de novos empregados, bem como em programas internos de educação continuada.

Compete ao Coordenação de TI

I. Observar as diretrizes de segurança visando à proteção dos ativos de Tecnologia da Informação – TI da FBN;
II. Elaborar normativo para a utilização dos ativos de TI visando à disponibilidade do ambiente tecnológico da FBN para as atividades corporativas.

Compete a qualquer pessoa física ou jurídica que produza ou manipule informação da Fundação Biblioteca Nacional

I. Proteger as informações sob sua responsabilidade;
II. Zelar pelos bens sob sua custódia;
III. Comunicar imediatamente ao Departamento de Segurança qualquer ação ou omissão, intencional ou acidental que resulte no comprometimento da segurança da Instituição.

MEDIDAS DE SEGURANIA

A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação. Pode ser dividida em:

I. Segurança Orgânica;
II. Segurança Ativa.

Segurança Orgânica

A segurança orgânica é composta pelos seguintes grupos de medidas:

I. Segurança das áreas e instalações;
II. Segurança de materiais;
III. Segurança de recursos humanos;
IV. Segurança da informação, que se desdobra em:
    a. Segurança da informação nos meios de tecnologia da informação;
    b. Segurança da informação de pessoas;
    c. Segurança da informação na documentação; e
    d. Segurança da informação nas áreas e instalações.

Segurança das Áreas e Instalações

A segurança de áreas e instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade da FBN ou onde se realizem atividades de interesse da Instituição, bem como seus perímetros, com a finalidade de salvaguardá-las.

As medidas de segurança de áreas e instalações interagem com os demais grupos de medidas, integrando a segurança como um todo.

As aquisições, ocupação, uso, e os projetos de construção, adaptação e reforma de áreas e instalações de Unidades devem ser planejados e executados com a observância dos demais aspectos e diretrizes de segurança institucional, e com a integração dos demais setores da Instituição, de modo a reduzir as vulnerabilidades e riscos, e otimizar os meios de proteção. As áreas e instalações que abriguem informações sensíveis ou sigilosas e as consideradas vitais para o pleno funcionamento da Instituição serão objeto de especial proteção.

A execução da atividade de segurança desse grupo de medidas exige auditorias e fiscalização dos sistemas e serviços. Essas ações são implementadas para o efetivo cumprimento das normas de segurança.

A segurança de áreas e instalações é composta pelos seguintes sistemas:

Sistema Físico: Composto por vigilantes que executam diversos serviços de vigilância; Sistema Eletrônico: Composto por equipamentos eletrônicos de segurança, como sensores, circuito fechado de televisão (CFTV), alarmes, fechaduras eletrônicas, sistemas de registro, catracas, cancelas, sistema de controle de acesso etc;

Sistema de Barreiras: Envolve as diversas barreiras para segurança dos perímetros. Controle de Acesso

As seguintes normas e orientações de controle de acesso vinculam o público interno e externo a FBN:

I. O atendimento ao público externo é realizado de segunda a sexta-feira, conforme Regimento Interno;
II. Todo acesso às dependências da FBN deverá obedecer os procedimentos de segurança;
III. O ingresso nas dependências FBN fora do horário de expediente somente será permitido em situações excepcionais e com prévia autorização;
IV. É obrigatório o uso de crachá de identificação para o acesso às dependências da FBN e permanência em seu interior.
V. Os portadores de marca-passo não serão submetidos ao detector de metais, mas deverão apresentar documentação que identifique sua situação, submetendo-se a outros meios de vistoria;
VI. Os serviços de entregas serão feitos ao solicitante na recepção da Rua México. evitando assim o acesso frequente de pessoas estranhas FBN.
VII. É vedado o ingresso de animais nas dependências FBN, salvo o cão-guia que acompanha pessoa com deficiência visual;
VIII. É vedado o uso dos registros das cancelas e o uso das imagens do CFTV para controle de frequência de servidor;
IX. O acesso de visitantes deverá ser precedido de autorização do(a) responsável pela área que será visitada e identificação pessoal;
X. A circulação de visitantes é restrita ao setor e pavimento indicado no crachá;
XI. Os visitantes deverão seguir os procedimentos de segurança vigentes;
XII. Todos os veículos que utilizam os estacionamentos deverão usar credenciais de estacionamento, que deverão constar no cadastro de identificação;
XIII. O controle de acesso ao estacionamento deverá ser efetuado pela Segurança;
XIV. Deverá ser comunicada à segurança a perda ou extravio do CIF;
XV. Excepcionalmente, outros veículos poderão ter acesso à garagem, em função da condição de seus passageiros ou da característica da carga a ser manuseada. Nestes

casos, a permanência estará limitada ao tempo necessário para embarque/desembarque e será fiscalizada pelo serviço de vigilância;

XVI. Os profissionais da área de imprensa deverão cumprir as exigências de
XVII. identificação, cadastro e revista;
XVIII. Os deficientes físicos, as gestantes, as lactantes, as acompanhadas por crianças de colo e as pessoas com idade igual ou superior a 60 anos terão atendimento prioritário.

Segurança de Materiais

A segurança de materiais é um conjunto de medidas de segurança voltadas a proteger o patrimônio físico da Unidade, incluindo equipamentos, componentes, acessórios, mobiliários, veículos, matérias-primas e demais itens empregados nas atividades da Instituição. Tem por objetivo salvaguardar a produção, o recebimento, a distribuição, o manuseio, o armazenamento, o transporte, o descarte, a doação e o acondicionamento dos materiais e equipamentos de posse ou sob a responsabilidade da FBN.

Segurança de Recursos Humanos

A segurança de recursos humanos é um conjunto de medidas destinadas a proteger a integridade física dos integrantes da FBN, assim como de seus respectivos familiares, quando comprometida em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais. Pela natureza e circunstância do trabalho, é fundamental que os integrantes do FBN desenvolvam uma cultura de conscientização e sensibilização quanto às prováveis ameaças, estabelecendo procedimentos de proteção e preservação de sua integridade física e dos demais servidores.

Segurança da Informação

A segurança da informação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosas, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza a FBN ou proporcionar vantagem a atores antagônicos. Visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, informação ou conhecimento.

A segurança da informação, pela sua relevância e complexidade, desdobra-se nos seguintes subgrupos:

I. Segurança da informação nos meios de tecnologia da informação;
II. Segurança da informação de pessoas;
III. Segurança da informação na documentação; e
IV. Segurança da informação nas áreas e instalações.

Segurança da Informação nos meios de Tecnologia da Informação

A segurança da informação nos meios de tecnologia da informação compreende um conjunto de medidas voltado a salvaguardar as informações sensíveis ou sigilosas geradas, armazenadas e processadas por intermédio da informática, bem como a própria integridade dos sistemas utilizados pela Instituição, englobando as áreas de informática e de comunicações. Tais medidas deverão:

I. Privilegiar a utilização de tecnologias modernas e o uso de sistemas criptográficos na transmissão de dados e informações sensíveis ou sigilosos, inclusive nos meios de comunicação por telefonia;

II. Priorizar a utilização de certificação digital, em especial nos assuntos que necessitem de sigilo e validade jurídica, e o armazenamento de dados (backup), que promovam a segurança e disponibilidade da informação;
III. Conter funcionalidades que permitam o registro e rastreamento de logs de acesso e de ocorrências, para fins de auditoria e contrainteligência;
IV. Ser efetivada por cruzamento de verificação e com segregação de funções preferencialmente por estrutura não subordinada à área de tecnologia da informação e comunicações.

As seguintes ações podem ser utilizadas para o alcance da segurança:

I. A área de tecnologia da informação da Unidade regulamentará a utilização das redes e itens de segurança, disponibilizando aos usuários, de acordo com o seu nível de atividade, as respectivas permissões e orientações que lhe cabem;
II. Todo acesso e ações realizadas nos sistemas devem ser passíveis de auditoria;
III. As informações a respeito do monitoramento dos recursos de tecnologia da
IV. informação deverão ser disponibilizadas aos usuários por ocasião do login;
V. A instalação e remoção de software e hardware deverão ser realizadas por pessoa autorizada pela equipe de tecnologia da informação;
VI. As senhas deverão ser utilizadas de forma responsável, devendo o usuário ser orientado sobre a criação e renovação periódica das senhas, conforme política da FBN;
VII. Deverá ser realizado backup de acordo com as normas de Segurança da Informação;

Todos os usuários, ao afastarem-se temporariamente da estação de trabalho, deverão desconectar-se da rede ou, alternativamente, ativar rotina de proteção de tela com senha;

VIII. O uso da criptografia poderá ser implementado no tratamento de informações que requeiram alto grau de sigilo;

IX. O acesso aos recursos de tecnologia da informação poderá ser realizado a partir de ambiente externo às dependências da Unidade mediante a utilização de recursos e orientações de segurança e determinados pela área de Tecnologia da Informação;
X. A central telefônica deve ser instalada em local com acesso restrito, mediante porta com sistema de fechadura com chave;
XI. O quadro de telefonia e seu cabeamento devem estar protegidos;
XII. É vedado o uso dos recursos do correio eletrônico para a veiculação de mensagens de caráter político-partidário, ideológico, religioso, de discriminação social, publicitário, pessoal, comercial e de “correntes” de qualquer natureza, bem como divulgar dados ou informações sigilosas ou sensíveis, obtidas em razão do cargo, e, também, que possam comprometer a honra alheia;
XIII. Os recursos de informática e comunicações disponíveis para os usuários FBN; somente poderão ser utilizados em atividades estritamente relacionadas às funções institucionais.

Segurança da Informação de Pessoas

A segurança da informação de pessoas refere-se ao grupo de medidas voltadas a estabelecer comportamentos a serem adotados pelos integrantes do FBN com vistas a assegurar a proteção de informações sensíveis ou sigilosas, em especial:

I. Segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição;
II. Detecção, identificação, prevenção e gerenciamento de infiltrações, recrutamentos e outras ações adversas de obtenção indevida de informações;
III. Identificação precisa, atualizada e detalhada das pessoas em atuação na Unidade;
IV. Verificação e monitoramento de ações de prestadores de serviços à Instituição;

V. Utilização do Termo de Compromisso de Manutenção de Sigilo – TCMS, que deve ser subscrito por todos os integrantes da Instituição ou terceiros que, de algum modo, possam ter acesso as informações sensíveis ou sigilosas.

A segurança da informação de pessoas contempla também medidas de reeducação e promoção de uma cultura comportamental que visem a combater ataques de engenharia social contra a Instituição. O termo engenharia social é definido como a utilização de práticas manipulatórias com fins de contornar dispositivos de segurança ou de se obter informações sigilosas ou sensíveis, explorando a confiança das pessoas para obter vantagens pessoais.

Segurança da Informação na Documentação

A segurança da informação na documentação compreende o conjunto de medidas voltadas a proteger informações sensíveis ou sigilosas contidas na documentação que é arquivada ou tramita na Instituição. Tais medidas deverão ser adotadas em cada fase de produção, classificação, tramitação, difusão, arquivamento e destruição da documentação.

Os documentos deverão ser classificados de acordo com o grau de sigilo exigido por seu conteúdo, de forma a assegurar que recebam nível adequado de proteção. A Instituição deverá adotar os procedimentos que garantam uma gestão documental adequada para documentos ostensivos e sigilosos, inclusive com o estabelecimento dos respectivos protocolos de segurança.

Segurança da Informação nas Áreas e Instalações

A Segurança da informação nas áreas e instalações compreende um conjunto de medidas voltadas a proteger informações sensíveis armazenadas ou em trâmite no espaço físico sob a responsabilidade da FBN ou no espaço físico onde estejam sendo realizadas atividades de interesse institucional. Esse grupo de medidas engloba ações para estabelecer o fluxo do público interno e externo, controlando o acesso referente às informações de layout de salas e gabinetes, localização de áreas sigilosas ou sensíveis, localização de setores de atendimento ao público e outras.

Segurança Ativa

A segurança ativa é o conjunto de ações de caráter preventivo e proativo destinadas a identificar, avaliar, analisar e neutralizar ações adversas dirigidas a FBN e a seus integrantes. A Coordenadoria de Segurança Institucional deve realizar um Estudo de Contrainteligência que identifique as atuais deficiências no âmbito da segurança ativa e subsidie a implementação de novas medidas de segurança.

São medidas desenvolvidas pela segurança ativa:

I. Contra sabotagem: Compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações intencionais contra material, áreas ou instalações da Instituição que possam causar interrupção de suas atividades e/ou impacto físico direto e psicológico indireto sobre seus integrantes;
II. Contraespionagem: Compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de ações adversas e dissimuladas de busca de informações sensíveis ou sigilosas;
III. Contra Crime Organizado: Compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de ações adversas de qualquer natureza contra a Instituição e seus integrantes, oriundas de organizações criminosas;
IV. Contrapropaganda: Compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de abusos, desinformações e publicidade enganosa de qualquer natureza contra a Instituição.

MEDIDAS ADMINISTRATIVAS

O assessor de Política Orgânica será responsável em conjunto com a Comissão de Segurança Permanente da FBN, por reunir as condições necessárias para a execução do presente plano, providenciando os recursos humanos, financeiros e outras necessidades a serem apontadas para aimplementação e execução do PSO, submetendo-o a apreciação do Presidente da Comissão de Segurança Permanente e posterior encaminhamento ao Presidente da FBN, para deliberação e decisão que os casos apontarem.

As medidas administrativas que dizem respeito à segurança devem ser planejadas com envolvimento das coordenações: de administração, de comunicação, de gestão de pessoas, de engenharia, de tecnologia da informação dentre outras.

AUDITORIAS E CONTROLE INTERNO

A fim de acompanhar a observância das medidas de segurança preconizadas neste PSO e avaliar sua adequabilidade, deverão ser realizadas auditorias de segurança nos sistemas e serviços a seguir especificados:

I. Sistema de controle de acesso de pessoas, veículos e de patrimônio:
    a. nas portarias;
    b. nas garagens ou estacionamento;
    c. nas áreas e instalações sensíveis; e
    d. nos claviculários.
II. Sistemas de detecção de intrusão;
III. Sistema de CFTV;
IV. Sistema de prevenção e combate a incêndio.

PLANEJAMENTO DE CAPACITAÇÃO

A atividade de segurança institucional tem caráter essencial e permanente. Deve-se buscar a promoção de atividades para capacitação e aperfeiçoamento dos servidores públicos, para tanto, deve ser promovida a realização de cursos, seminários, palestras e atividades outras que contribuam para o desenvolvimento da segurança institucional na Biblioteca Nacional.

PLANEJAMENTO PARA EMERGÊNCIAS

Os planos de emergências estabelecem as diretrizes e ações a realizar em situações emergenciais que tenham potencial para repercussão que afete a segurança da instituição e de seus integrantes. Eles apresentam procedimentos de resposta as situações emergenciais, definem atribuições e estabelecem as condições de execução das ações previstas em situações complexas e que envolvam outras instituições, os planos devem ser integrados ao planejamento de emergência destas e prever ações em conjunto e interligadas.

PLANEJAMENTO DE CONTINGÊNCIA E CONTROLE DE DANOS

O Planejamento de Contingência visa minimizar ou neutralizar os impactos decorrentes de interrupções de atividades críticas e serviços essenciais da FBN, ocasionados por falhas, desastres, indisponibilidade significativa ou ação intencional de ator hostil em processos sensíveis, permitindo a continuidade das atividades e serviços em níveis aceitáveis. Esse planejamento contempla ações de prevenção e recuperação, além de medidas de avaliação do dano, que constituem o plano de contingência e o plano de controle de danos.

REVISÃO

Este Plano de Segurança Orgânica será submetido à revisão geral de seu conteúdo ao final do primeiro ano de sua vigência e periodicamente a cada dois anos após a primeira revisão. Nas situações em que ocorrerem alterações de legislação ou normas que exijam ajustes do PSO, poderão ser realizadas revisões específicas relacionadas ao assunto em pauta.

O mesmo se aplica às situações em que há ocorrência de mudança de sede ou de reformas que impliquem alterações nas normas de segurança.

FONTES DE CONSULTAS

_____

Casa da Moeda – Entrevista com o Sr.: Pedro Mattos (Superintendente de Segurança Institucional).

PSO TRT 13 Região

ABIN. Conceitos de Atividade de Inteligência. Disponível em: http://www.abin.gov.br/atividadeinteligencia/inteligenciaecontrainteligencia/.

BACALHAU, Marcos. Inteligência e Contrainteligência.

DUMONT, Danilo M. RIBEIRO, José A.; RODRIGUES, Luiz A. Inteligência pública na era do conhecimento.

HORTA, Rodrigo Otávio. A gestão da segurança institucional na gestão pública. MINISTÉRIO PÚBLICO DO TRABALHO. Segurança Institucional. Disponível em:

<http://portal.mpt.mp.br/wps/portal/portal_mpt/mpt/ompt/seguranca%20institucional/!ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8zi_QJNPN2dgg28Lcy8zA0czSwcPb0tAww8_Q31vfSj8CsAmmBU5Ovsm64fVZBYkqGbmZeWrx9RnJpeWpSYl5yokJlXXJJZUpoMty8zq7AwyIE_Kjk_ryS1okQ_IregRNUgXwFM4dJXkB2VVFnuqAgAQpdlxQ!!/>

Cruz Vermelha: https://www.marketingjob.com.br/wpcontent/uploads/2021/02/cruz- vermelha-manual-fique-seguro.pdf