impa

Instituto de
Matemática
Pura e Aplicada

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Política de Segurança da Informação

Gerência de Tecnologia da Informação

Versão 1.2/2020

Estrada Dona Castorina, 110 Jardim Botânico - CEP 22460-320 Rio de Janeiro, RJ - Brasil Phone: +55 21 2529-5000
www.impa.br

SUMÁRIO

Introdução

Este documento consiste na Política de Segurança da Informação – PSI do Instituto de Matemática Pura e Aplicada – IMPA, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. No entanto destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da instituição.

A governança no compartilhamento de dados na administração pública federal, autárquica e fundacional segue as diretrizes estabelecidas no Decreto no 10.046, de 9 de outubro de 2019, e precisa ser compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicações e do disposto pela Lei no 13.709, de 14 de agosto de 2018 - **Lei Geral de Proteção de Dados Pessoais** (LGPD).

A **Lei Geral de Proteção de Dados Pessoais** (LGPD – Lei n° 13.709/2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois "agentes de tratamento", o Controlador e o Operador:

- O **Controlador** é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

- O **Operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Considera-se "tratamento de dados" qualquer atividade que utilize um **dado pessoal** na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A LGPD manteve o conceito de **dado pessoal** trazido pela Lei 12.527/2011 e evoluiu sobre o conceito de informação sensível: **"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"** (Art. 5o, II). Cabe destacar que todos os tipos de atributos constituem dados pessoais, pois são relativos a titular pessoa física identificado ou identificável.

Com isso, essa Política de Segurança da Informação, vem informar a todos os usuários de que deve haver um **comprometimento** com as informações internas, bem como o bom uso dos sistemas e recursos computacionais disponibilizados pelo IMPA.

Objetivos

A segurança da informação se baseia em três pilares: **confidencialidade**, **integridade** e **disponibilidade**.

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Esta Política de Segurança da Informação será implementada no IMPA por meio de normas e procedimentos específicos, obrigatórios para todos os usuários, independentemente do nível hierárquico ou função, bem como de vinculo empregatício ou de prestação de serviço.

É dever de todos zelar pela Segurança da Informação e Comunicações.

Diretrizes da Gerência de TI

1. Resguardar a proteção dos dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas;
2. Realizar a adequada classificação das informações e garantir a continuidade do processamento das mesmas, conforme os critérios e princípios indicados nos normativos internos vigentes sobre o tema;
3. Garantir que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;
4. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou tratados os dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a dados internos e confidenciais, por meio, dentre outros aspectos:
    a. da manutenção de softwares antivírus e firewall instalados e atualizados;
    b. da manutenção dos programas de computador instalados no ambiente;
5. Adotar procedimentos e controles para reduzir a vulnerabilidade da instituição a incidentes e atender aos objetivos de segurança cibernética, dentre eles: a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos vigentes.

Recomendações Gerais

O uso correto e responsável dos recursos de TI é de responsabilidade de todos os usuários do Instituto, inclusive aos externos, alunos, servidores, funcionários e prestadores de serviço, que utilizam esses recursos e a infraestrutura disponível. As informações pertencentes ao IMPA devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

Recomendações para o uso seguro dos recursos de TI

O envolvimento do usuário é importante no processo da segurança dos recursos de TI, pois é na adequada utilização destes recursos, como instrumento de trabalho, que se inicia a formação de uma sólida cultura de segurança da informação.

Desta forma, recomenda-se aos usuários a adoção das seguintes práticas:

1. **Obrigatoriamente**, utilizar senhas que contenham, pelo menos, dez caracteres, evitando o uso de nomes, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com o usuário ou palavras constantes em dicionários. Recomendamos fortemente, utilizar senhas compostas de letras, números e símbolos;
2. Alterar periodicamente suas senhas ou quando ocorrerem vazamento de dados em sites que possua cadastro;
3. Certificar a procedência dos links, sites e a utilização de conexões seguras (criptografadas) ao realizar transações via web;
4. Verificar se o certificado do site ao qual se deseja acessar, esta integro e corresponde realmente aquele site, observando ainda, se o mesmo está dentro do prazo de validade;
5. Certificar que o endereço apresentado no navegador corresponde ao site que realmente se quer acessar, antes de realizar qualquer ação ou transação;
6. Digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino;
7. Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus;
8. Utilizar somente programas de computador licenciados. A instalação de programas e sistemas homologados é atribuição da Gerência de TI;
9. Criar, transmitir, distribuir, disponibilizar e armazenar documentos, desde que respeite às leis e regulamentações, notadamente àqueles referentes aos crimes informáticos, ética, decência, pornografia envolvendo crianças, honra e imagem de pessoas ou empresas, vida privada e intimidade;
10. Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitada a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos no âmbito da Administração Pública Federal, exigindo-se autorização para aqueles protegidos pelos direitos autorais, inclusive músicas, textos, documentos digitalizados e qualquer conteúdo encontrado em revistas, livros ou quaisquer outras fontes protegidas por direitos autorais.

São consideradas **atividades ilegais**:

- Introduzir códigos maliciosos nos sistemas de TI;
- Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas, etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
- Tentar interferir desautorizada mente em um serviço, sobrecarrega-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;
- Alterar registro de evento dos sistemas de TI;

- Obter acesso não autorizado ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
- Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
- Fornecer informações a terceiros, sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização de autoridade competente;
- Fornecer dados classificados de acordo com a legislação vigente, sem autorização de autoridade competente;
- Uso de recursos computacionais para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;
- Uso não condizente a atividades de ensino e pesquisa;

Tratamento da Informação

Documentos imprescindíveis para as atividades dos usuários da instituição deverão ser salvos em drives de rede, tais como os compartilhamentos das gerências e coordenações ou nos serviços institucionais na nuvem, Cubo (OwnCloud) e/ou Google Drive.

Todos os arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Arquivos pessoais e/ou não pertinentes às atividades institucionais do IMPA (fotos, músicas, vídeos, etc..) **não deverão** ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário.

Normas de classificação de informações, acesso à informação, uso e descarte de ativos de informação, dentre outros temas afins, serão fixadas em estrita aderência às leis e normas atinentes à Administração Pública Federal – considerando as competências regimentais.

Controle de acessos

Todo acesso à infraestrutura de Tecnologia de Informação e Comunicação do IMPA, se dá através de uma **identificação única e indivual**, ou seja, login e senha, que são criados na momento da sua vinculação ao IMPA, seja como servidor, funcionário, aluno ou pesquisador visitante. É através dessa identificação que se tornam “usuários” e tem acessos liberados, conforme explicado abaixo:

Automáticos: Será dado a todos os usuários, automaticamente, o acesso aos serviços básicos como correio eletrônico, aplicações de produtividade e sistemas institucionais. Estas facilidades básicas poderão variar de acordo com os cargos e serão determinadas pelas Gerências e Coordenações. Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por uma solicitação especial feita ao proprietário da informação envolvida.

Por solicitação: As solicitações para novas identificações de usuários e alterações de privilégios devem ser feitas pelos canais disponíveis de Apoio aos Usuários e aprovadas pela sua chefia imediata.

Uso de equipamentos particulares na rede do IMPA

O IMPA possui uma rede sem fio – Wi-Fi com cobertura total nas suas instalações, tanto para uso interno, quanto para uso público em geral, seja por visitantes ou participantes de eventos. Apesar de ser uma rede acessível somente nas suas instalações, não podemos deixar de considerar os requisitos de segurança da informação, por isso se estabelecem algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis, como por exemplo, notebooks, smartphones e pendrives.

Fica autorizado, de forma automática, o acesso a todos os usuários que possuam um e-mail corporativo, ou seja, "@impa.br", através da rede sem fio "IMPA-internal". Os demais usuários deverão solicitar o acesso ao Wi-Fi como convidados, através da rede sem fio "IMPA-guest", usando o Portal de Wi-Fi para recebimento do *token* de acesso. Também é possível utilizar a rede sem fio "EduRoam", caso a instituição do usuário seja participante dessa rede de serviço, seja para usuários do IMPA ou de outras instituições.

Todas as recomendações de uso dos recursos computacionais se aplicam, adicionalmente a:

- É de responsabilidade do proprietário usar somente sistemas operacionais e aplicativos legalizados no seu equipamento;
- Não podem ser executados aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
- A equipe de TI do IMPA não realiza, em hipótese alguma, manutenção, instalação, seja de software ou harware, em equipamentos particulares. O único atendimento técnico autorizado são aqueles referentes à conexão ao Portal de Wi-Fi. No entanto, todos os equipamentos particulares conectados à rede e/ou sistemas do IMPA se submetem automaticamente a esta política.
- Caso seja detectado uso indevido da rede sem fio, tais como uso de aplicativos *peer-to-peer*, farejadores de tráfego (*sniffers*) ou que possam trazer prejuízos à infraestrutura ou à imagem do IMPA, não serão permitidos. Caso o equipamento não obedeça aos requisitos dessa política de segurança, o acesso não será concedido ou revogado;
- É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário, no seu notebook, smartphone, disco externo ou pendrive. Todos os arquivos que pertençam ao IMPA não podem ser armazenados nos equipamentos pessoais, sem a prévia autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento corporativo destinado para tal ou nos serviços institucionais na nuvem, Cubo (OwnCloud) e/ou Google Drive.

Responsabilidades

São responsabilidades gerais de todos os usuários quando utilizando os serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais do IMPA:

- Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;
- Seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do instituto;

- Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais do IMPA, em alinhamento ao seu **Código de Ética e Conduta**.
- Manter-se atualizado em relação a esta Política de Segurança da Informação e às normas e procedimentos relacionados, buscando informação junto à Gerência de TI sempre que não estiver absolutamente seguro quanto à utilização dos recursos computacionais institucionais.

Monitoramento

Para garantir a aplicação das recomendações mencionadas nesta Política de Segurança da Informação, além de fixar normas e procedimentos complementares sobre o tema, a Gerência de TI deve utilizar sistemas de monitoramento do uso das estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

Cabe a Gerência de TI, o direito de realizar, a qualquer tempo, inspeção física nos recursos computacionais, instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos locais de acesso, podendo desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

Embora a conexão direta e permanente da rede corporativa da instituição com a Internet ofereça um grande potencial de benefícios, é esperado o desenvolvimento de um comportamento eminentemente ético e profissional. Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, o IMPA, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à Internet.

Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor do quadro permanente. (perfis do IMPA no Facebook, Instagram e Twitter, por exemplo)

É de responsabilidade da Gerência de TI, somente tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação superior (Gerências ou Coordenações) ou por determinação da Diretoria.

Grupo de Resposta a Incidentes de Segurança

O IMPA possui um **Grupo de Resposta a Incidentes de Segurança (CSIRT@impa.br)**, para prevenção, tratamento e respostas a incidentes, atuando como um ponto central de contato, contando com os seguintes integrantes para combate às ocorrências:

- Roberto de Beauclair Seixas
- Rosa Ladeira
- Ricardo Gomes
- Daniel Lins de Albuquerque

Cabe ao Grupo de Resposta a Incidentes de Segurança do IMPA, a notificação do incidente ao CERT.br e também ao Centro de Atendimento a Incidentes de Segurança – CAIS, da Rede Nacional de

Ensino e Pesquisa – RNP, em casos que não ocorram exclusivamente na rede interna do IMPA. O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil, atuando como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

No tratamento de incidentes em redes computacionais, Grupo de Resposta a Incidentes de Segurança do IMPA, deverá considerar as seguintes diretrizes:

- Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;
- 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, naquilo que diz respeito ao estabelecimento de graus de sigilo;
- Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, o Grupo de Resposta a Incidentes de Segurança tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades competentes para a adoção dos procedimentos legais julgados necessários, observando os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade das atividades institucionais.

Considerações

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas à Direção do instituto ou a Comissão de Informática.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Diretoria e/ou da Gerência de Tecnologia da Informação, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

Esse documento deve receber revisões a cada dois anos ou sempre que ocorram modificações na legislação vigente, referentes à segurança dos sistemas de informação.

Referências de Legislação

A norma ISO/IEC 27000:2018, norma da Associação Brasileira de Normas Técnicas (ABNT), fornece a visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27001. Projetada para ser aplicável a todos os tipos e tamanho da organização de negócios, desde multinacionais até as pequenas e médias empresas, a nova versão, lançada em fevereiro é igualmente valiosa para agências governamentais ou organizações sem fins lucrativos.

A norma ISO/IEC 27001:2013 descreve os requisitos a serem adotados na elaboração de sistemas de gestão de segurança da informação.

A norma ISO/IEC 27002:2005 trata de técnicas de segurança em Tecnologia da Informação e funciona como um código de prática para a gestão da segurança da informação.

Resumo

Informação é patrimônio! Toda informação elaborada, adquirida, manuseada, armazenada, transportada e/ou descartada nos sistemas e/ou nas dependências do IMPA, deve ser utilizada exclusivamente para os interesses e atividades do IMPA.

Segurança da Informação: É o conjunto de ações e controles que tem como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos do IMPA.

- **Confidencialidade**: A informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;
- **Integridade**: Salvaguarda da exatidão da informação e dos métodos de processamento;
- **Disponibilidade**: As pessoas autorizadas devem obter acesso à informação, sempre que necessário;
- **Conformidade**: Processo de garantia do cumprimento de um requisito, podendo ter obrigações com aspectos legais e regulatórios relacionados à administração institucional, dentro de princípios éticos e de conduta estabelecidos pelo IMPA.

Incidente de Segurança da Informação: Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação acima.

Incidentes de Segurança precisam ser tratados: Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos do IMPA.

A responsabilidade e o comprometimento deve ser de todos: Todos os servidores, funcionários, alunos, colaboradores, estagiários, terceiros, fornecedores e parceiros, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos e informações de que sejam usuários ou com os quais tenham contato, assim como dos ambientes físicos e computacionais a que tenham acesso, independentemente das medidas de segurança implantadas.

O acesso à informação deve ser gerenciado: O acesso lógico, o controle de acesso físico e o uso da informação devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.

Uso e monitoramento: A equipe de TI monitora o acesso e a utilização de toda infraestrutura de TI, como dos ambientes, equipamentos e sistemas da informação, de forma que ações indesejáveis ou não autorizadas sejam detectadas.

Abordagem baseada em riscos: A segurança da informação é fundamentada em decisões baseadas em riscos como perda da vantagem produtiva, competitiva, conformidade, de responsabilidade civil, interrupções operacionais, danos à reputação e perdas financeiras.

Ambiente de segurança: A segurança da informação é estruturada com base na análise do comportamento humano, observando as crescentes necessidades de todas as partes interessadas, através da conscientização e maturidade dos usuários fortalecendo um dos elementos fundamentais para manter o nível apropriado de segurança.