Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia Baiano
Órgão de Assessoramento - Comitê de Governança Digital

PORTARIA 3/2024 - OA-CGD/IFBAIANO, de 24 de setembro de 2024

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL no uso de suas atribuições legais previstas no artigo 6º, no Regimento Interno do Comitê de Governança Digital, o Processo n.º 23327.251938.2024-94 e, considerando:

- a deliberação dos membros do CGD, em sua 2ª Reunião Ordinária, realizada em 16.09.2024.

RESOLVE:

Art. 1º Aprovar, a revisão da Política de Segurança da Informação do Instituto Federal Baiano.

Art. 2º Esta Portaria entra em vigor nesta data.

Marcelito Trindade Almeida
Presidente

Documento assinado eletronicamente por:

- **Marcelito Trindade Almeida**, **DIRETOR(A) EXECUTIVO(A) - CD3 - RET-DIREX**, em 24/09/2024 16:20:00.

Este documento foi emitido pelo SUAP em 24/09/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 606812
Código de Autenticação: dc38a3b537

Política de Segurança da Informação

2024 - 2028

Responsáveis: Assinaturas / Aprovações Eletrônicas

Atividade	**Nomes**
Elaboração	Comissão de elaboração
Revisões	Comissão de revisão
Aprovação	Comitê de Governança, Riscos e Controle
Homologação	Reitor

INSTITUTO FEDERAL
Baiano

Termos e Abreviações

IF Baiano	Instituto Federal de Educação, Ciência e Tecnologia Baiano
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
TI	Tecnologia da Informação
PSI	Política de Segurança da Informação
DGTI	Diretoria de Gestão da Tecnologia da Informação
CGD	Comitê de Governança Digital
RNP	Rede Nacional de Ensino e Pesquisa

INSTITUTO FEDERAL
Baiano

Sumário

1. Apresentação

A Política de Segurança da Informação do IF Baiano é uma declaração formal acerca do compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda. Esta política está alinhada ao planejamento estratégico do Instituto para promover uma cultura de segurança na instituição e garantir a integridade, confidencialidade e disponibilidade das informações.

2. Abrangência

Esta política se aplica aos(as) servidores(as), discentes, terceirizados(as), colaboradores(as) internos ou externos, estagiários(as), visitantes, prestadores(as) de serviços externos e a qualquer pessoa física ou jurídica que, de alguma forma, executem atividades vinculadas ao Instituto. As pessoas ou organizações que utilizem os meios físicos ou lógicos do IF Baiano devem ter conhecimento do seu teor e ser responsáveis por garantir a segurança das informações a que tenham acesso.

3. Objetivos

A política de segurança do IF Baiano tem por objetivo estabelecer as diretrizes estratégicas, normas, procedimentos e responsabilidades relativas à Segurança das Informações para proteção dos negócios do Instituto, assim como:

Proteger os dados pessoais: garantir a segurança e privacidade das informações pessoais das pessoas que estejam em sua abrangência e de outras partes interessadas, protegendo-as contra acesso não autorizado, uso indevido e divulgação não autorizada.

Garantir a integridade dos dados: assegurar que os dados armazenados e processados pelos sistemas de informação sejam precisos, completos e confiáveis, prevenindo alterações não autorizadas, corrupção ou perda de dados.

Assegurar a disponibilidade dos sistemas: garantir que os sistemas de informação estejam disponíveis e acessíveis quando necessário, minimizando interrupções e indisponibilidades que possam afetar o funcionamento das atividades educacionais.

Proteger contra ameaças cibernéticas: proteger os sistemas de informação contra uma variedade de ameaças cibernéticas, incluindo malware, phishing, ataques de negação de serviço e outras formas de ataques que visam comprometer a segurança e estabilidade dos sistemas.

Promover a conscientização e educação em segurança: educar e conscientizar sobre boas práticas de segurança da informação, aumentando sua capacidade de reconhecer e responder a ameaças de segurança de forma proativa.

Garantir conformidade regulatória: assegurar que as práticas de segurança da informação estejam em conformidade com as leis, regulamentos e padrões de segurança aplicáveis, garantindo que o Instituto esteja protegido contra possíveis penalidades legais e danos à reputação.

4. Definições

Segurança da Informação: conjunto de controles para proteção dos ativos da informação, por meio de atributos de confidencialidade, integridade e disponibilidade nos âmbitos de tecnologia, processos e pessoas.

Ativo: qualquer item ou elemento, físico ou não, que tenha valor para um indivíduo ou uma organização.

Ativos de Informação: representam quaisquer elementos ou itens da organização onde as informações são criadas, processadas, armazenadas, transmitidas ou descartadas.

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Análise de Riscos: uso sistemático de informações para identificar fontes e estimar o risco.

Ataque: ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro ou indisponível.

Vulnerabilidades: fraqueza em um ativo ou controle que pode ser explorada por uma ameaça.

Credenciais de Acesso: informações que pertencem a um usuário(a) e que são usadas para identificar e validar o acesso a qualquer recurso computacional.

Redes Sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

Usuário(a): pessoa que usa o serviço de TI.

Gestor(a): responsável por planejar e dirigir o trabalho de um grupo de indivíduos, monitorando e tomando medidas corretivas quando necessário.

Continuidade de Negócios: envolve planejar e responder a incidentes e interrupções, minimizando impactos e recuperando ativos críticos da informação para manter operações em níveis aceitáveis.

Custodiante do ativo de informação: pessoa física que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação, materializados ou não, que não lhe pertencem, mas que estão sob sua custódia.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): equipe responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança.

Política de Segurança da Informação: documento aprovado pela autoridade responsável pela instituição, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação.

Tecnologia da Informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

5. Referências

O IF Baiano está em conformidade com as leis e decretos federais relacionados à segurança da informação, a fim de manter constantemente atualizada sua Política de Segurança da Informação. Dentre os principais dispositivos legais e regulamentos federais aplicáveis, destacam-se:

Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação.

Resolução SE/GSI nº 1, de 11 de setembro de 2019, que aprova o Regimento Interno do Comitê Gestor de Segurança da Informação.

Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação.

Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética.

Instrução Normativa GSI/PR Nº 1, de 27 de Maio de 2020, dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

Instrução Normativa GSI/PR Nº 2, de 24 de Julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

Instrução Normativa GSI/PR Nº 3, de 28 de Maio de 2021, dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Instrução Normativa GSI/PR Nº 5, de 30 de Agosto de 2021, dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

Instrução Normativa GSI/PR 6, de 23 de Dezembro de 2021, estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

Instrução Normativa GSI/PR Nº 7, de 29 de novembro de 2022, altera a Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República; a Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021; e a Instrução Normativa nº 6, de 23 de dezembro de 2021, do Gabinete de Segurança Institucional da Presidência da República.

LEI Nº 13.709, de 14 de Agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

6. Princípios

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.

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

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.

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 devidamente autorizados.

Legalidade: garantia de que todas as ações de Segurança da Informação e Comunicação deverão obedecer aos princípios constitucionais, administrativos e à legislação vigente.

7. Diretrizes

7.1. Aspectos Gerais

- As informações produzidas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas relacionadas ao IF Baiano são consideradas patrimônio da Autarquia. Elas são classificadas e manipuladas de acordo com as normas e legislação específicas em vigor, garantindo a segurança ao longo de todo o seu ciclo de vida.
- Os contratos celebrados pelo IF Baiano com prestadores(as) de serviços devem conter cláusulas que determinem a observância da PSI e seus respectivos documentos, bem como a manutenção do sigilo de suas informações durante e após sua vigência.
- Os sistemas do IF Baiano possuem mecanismos de autenticação individual para garantir a segurança do acesso e é responsabilidade de todos os(as) usuários(as) comunicar incidentes de segurança à área responsável.

7.2. Seções da PSI

Classificação e tratamento das Informações

Os ativos de informação do IF Baiano devem ser classificados conforme sua confidencialidade, disponibilidade, integridade e requisitos legais. Após a classificação, devem ser gerenciados quanto ao acesso, armazenamento, cópias de segurança, movimentação e descarte.

As mídias removíveis ou impressas que contenham ativos de informação devem ser claramente classificadas e identificadas para garantir o tratamento adequado.

Segurança Física e do Ambiente

As instalações, equipamentos, redes e sistemas de computadores, exceto os destinados ao público externo, devem ter controles de acesso físico e/ou lógico para identificar usuários(as). A autenticação dos usuários(as) pode ser por senha, biometria ou outros métodos combinados, sendo a senha de uso pessoal e intransferível.

Deve-se estabelecer um perímetro de segurança física para permitir acesso apenas a pessoas autorizadas, com o uso obrigatório de identificação funcional. Os(as) usuários(as) são responsáveis por proteger os ativos de informação contra danos ou roubo, garantindo sua disponibilidade.

Informações classificadas como restritas devem ser armazenadas de forma segura, como em cofres ou armários com fechaduras. Equipamentos de armazenamento e processamento de informação só podem ser usados fora das dependências do Instituto com autorização prévia e proteção adequada contra furto ou perda.

Em caso de invalidação das credenciais de acesso de servidor(a), o acesso aos ativos de informação do Instituto seguirá as condições estabelecidas para visitantes.

Gestão de Incidentes em Segurança da Informação

A gestão de incidentes em segurança da informação tem como objetivo garantir um enfoque consistente e efetivo na administração dos incidentes de segurança, incluindo a comunicação sobre vulnerabilidades e eventos relacionados à segurança da informação. A ETIR é responsável por receber, filtrar, classificar e responder às solicitações e alertas, além de conduzir análises dos incidentes de segurança. Seu objetivo é extrair informações que possibilitem interromper a ação maliciosa e identificar tendências para prevenir futuros incidentes.

Gestão de Ativos

A Gestão de Ativos pretende grantir a identificação, proteção e otimização dos recursos fundamentais da instituição. Isso envolve a identificação de ativos físicos e de informação, a avaliação dos riscos associados, a implementação de medidas de proteção adequadas, o monitoramento contínuo e a otimização do uso dos recursos.

Gestão do Uso dos Recursos Operacionais e de Comunicações

- **E-mail**

O e-mail ou correio eletrônico é um serviço disponibilizado pelo IF Baiano como uma ferramenta institucional e acadêmica para aqueles que possuem vínculo com o

Instituto. Seu uso é pessoal e intransferível, para fins institucionais, de responsabilidade do usuário e está sujeito a auditorias.

Regulamento IF Baiano: Regulamento ao Acesso e Utilização do Correio Eletrônico Institucional

- **Acesso à Internet**

Os(as) usuários(as) têm o direito de acesso à Internet conforme as permissões de acesso estipuladas nas normas de segurança da instituição. Esse acesso deverá ser feito para fins diretos e complementares às atividades da Instituição, para o enriquecimento intelectual de seus usuários(as) ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de suas atividades.

Os acessos realizados nesse ambiente são monitorados pela equipe da DGTI, com o objetivo de garantir o cumprimento desta política.

Regulamento: Em parceria com RNP - Política de Uso Edurom

Regulamento: Em parceria com RNP - Política de Uso Rede Ipê

- **Redes Sociais**

O IF Baiano em seu âmbito geral que inclui a Reitoria e todos os campi só reconhece oficialmente as redes sociais listadas no portal institucional.

Qualquer outro perfil deverá ser desconsiderado e toda informação publicada nos meios de comunicação digitais oficiais do IF Baiano será de responsabilidade do(a) usuário(a) que realizou a publicação.

- **Computação em nuvem**

O IF Baiano dispõe, para os(as) servidores(as) e para os alunos, um espaço na nuvem para armazenamento de arquivos, editores de documentos online e hospedagem de e-mail institucional.

Para demais serviços oferecidos pelo IF Baiano que ainda não estão na nuvem, o Instituto irá dispor de norma própria e específica para cada um.

Regulamento IF Baiano: Política de Uso do Meu drive

Controle de Acesso

O acesso aos recursos de TI dentro da infraestrutura da instituição terá controles físicos e/ou lógicos com o objetivo de proteger equipamentos, sistemas, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada.

O acesso aos serviços de rede do IF Baiano que necessitem de autenticação só será permitido a usuários(as) cadastrados(as) conforme diretrizes homologadas pelo CGD.

Monitoramento

Informações que estão armazenadas ou circulam dentro dos limites físicos e lógicos do IF Baiano podem ser monitoradas. Esse monitoramento tem como objetivo garantir que não ocorra uso indevido das informações ou atividades não autorizadas que possam violar políticas, normas ou leis em vigor.

Gestão de Riscos

A Gestão de Riscos desempenha um papel essencial na PSI do IF Baiano, concentrando-se na identificação, avaliação e mitigação de ameaças potenciais que possam afetar a integridade, disponibilidade e confidencialidade dos ativos e operações da instituição. Por meio da Gestão de Riscos, o IF Baiano prontamente identifica os riscos associados às suas atividades e implementa estratégias para reduzir sua probabilidade de ocorrência e minimizar seu impacto caso se materializem.

O IF Baiano tem a gestão de riscos definida em norma complementar, seguindo diretrizes superiores e implantada na instituição. A metodologia de construção do processo de gestão de riscos, consta análise e avaliação de riscos, e define a periodicidade no levantamento de risco nos ativos de informação do IF Baiano, visando, sempre, fortalecer sua resiliência e capacidade de resposta a eventos

adversos, protegendo seus recursos e promovendo um ambiente seguro e confiável para sua comunidade acadêmica

Regulamento IF Baiano: Comitê de Governança, Riscos e Controle

Gestão de Continuidade

O processo de gestão de continuidade do negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

É de responsabilidade do gestor da unidade de négócio em solicitar a DGTI a condução e suporte dos processos de continuidade envolvendo sistemas, que devem ser implementado e testado periodicamente para garantir a continuidade dos serviços críticos do IF Baiano.

Auditoria e Conformidade

A Auditoria e Conformidade garante que os controles e procedimentos de segurança estejam em conformidade com os padrões, regulamentos e políticas internas e externas aplicáveis. Através de processos de auditoria regulares e abrangentes, o IF Baiano pode avaliar a eficácia de suas medidas de segurança, identificar eventuais lacunas ou não conformidades e implementar correções e melhorias necessárias. Isso inclui não apenas a avaliação da conformidade legal e regulamentar, mas também a aderência às melhores práticas da indústria e padrões de segurança reconhecidos internacionalmente. Além disso, a Auditoria e Conformidade desempenham um papel fundamental na garantia da integridade, confidencialidade e disponibilidade dos ativos e dados do IF Baiano, fornecendo uma garantia de que os recursos estão sendo gerenciados de acordo com os mais altos padrões de segurança e governança.

8. Competências

Comitê de Governança Digital

- promover a cultura de Segurança da Informação no âmbito da Instituição
- estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação.
- promover a divulgação da política e das normas internas de segurança da informação.
- incentivar novas tecnologias e seus eventuais impactos relacionados à segurança da informação.
- verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.
- 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.

Comitê de Governança, Riscos e Controle

- Acompanhar a implantação de novas tecnologias, no que diz respeito a possíveis riscos e impactos sobre a Segurança da Informação.
- acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.
- Acompanhar as investigações e avaliações dos dados decorrentes de quebras de segurança;
- Propor recursos necessários às ações de Segurança da Informação;

Diretoria de Gestão da Tecnologia da Informação

- Planejar, coordenar, executar e avaliar os projetos, procedimentos, normas e ações que possibilitem a operacionalização e manutenção desta política em articulação com as Pró-Reitorias, Direções Gerais e demais áreas de Tecnologia da Informação dos campi.

Gestores(as)

- Garantir que os(as) colaboradores(as) de sua equipe e os(as) prestadores(as) de serviços contratados sob sua gestão conheçam e cumpram as regras da PSI.
- Aderir às regras de proteção dos ativos de informação.
- Revisar periodicamente os acessos concedidos aos ativos de informação sob sua responsabilidade, informando a área responsável por controle de acesso sobre as revogações necessárias.
- Apoiar na investigação de incidentes de segurança da informação quando aos seus ativos estiverem no processo de investigação.
- Aprovar, desde que de acordo com as regras de confidencialidade e integridade, as solicitações de acesso a sistemas / informações dos(as) colaboradores(as) ou prestadores(as) de serviços sob sua responsabilidade.
- Solicitar os cancelamentos de acessos de colaboradores(as) ou prestadores(as) de serviços que não necessitem mais do acesso no exercício de suas atribuições.

Colaboradores(as) e usuários(as) da Informação

- Respeitar e seguir todas as políticas instituídas pelo IF Baiano, zelando pela proteção e preservação dos ativos de informação.
- Manter o sigilo das informações consideradas confidenciais e de uso restrito.
- Comunicar ao CGD qualquer desvio à PSI.
- Não compartilhar credenciais de acesso, sejam elas físicas ou digitais, como nomes de usuário(a) e senhas.

9. Penalidades

O Não cumprimento de qualquer um dos controles, regras e normas descritos na PSI e/ou seus anexos, é passível de ações disciplinares administrativas, acusações civis, penalidades criminais e/ou outras sanções, conforme estabelecido na legislação vigente.

10. Política de Atualização e Revisão

A PSI do IF Baiano, deve ser revisada e atualizada quando existirem demandas que justifiquem ou sempre que se fizer necessário, não devendo exceder o período máximo de 4 (quatro) anos a partir da data da sua publicação, de acordo com INSTRUÇÃO NORMATIVA Nº 1, DE 27 DE MAIO DE 2020 e, quando necessário, deve ser complementada por normas, metodologias e procedimentos.

11. Casos Omissos

Assuntos relacionados à Segurança da Informação no IF Baiano e não previstos neste documento devem ser encaminhados para aprovação pelo CGD.

Cópia de documento digital impresso por Viviane Menezes (1592062) em 25/09/2024 16:15.

Documento Digitalizado Público

Política de Segurança da Informação do Instituto Federal Baiano

Assunto: Política de Segurança da Informação do Instituto Federal Baiano
Assinado por: Robson Ramos
Tipo do Documento: Proposta
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Robson Cordeiro Ramos**, **DIRETOR(A) - CD3 - RET-DGTI**, em 12/08/2024 16:12:06.

Este documento foi armazenado no SUAP em 12/08/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 888580
Código de Autenticação: a8b522fccf