MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
Conselho Superior

RESOLUÇÃO 33/2021 - CONSUP/RE/IFAP

Aprova a Política de Segurança da Informação, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP.

A PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ, no uso de suas atribuições legais e regimentais, considerando o que consta no processo nº 23228.000625/2021-45, e as deliberações na 48º Reunião Ordinária do Conselho Superior do Ifap,

RESOLVE:

Art.1º Aprovar a Política de Segurança da Informação, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP.

Art. 2º Esta resolução entrar em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por:

- Marialva do Socorro Ramalho de Oliveira de Almeida, REITOR - CD0001 - RE, em 17/08/2021 17:19:29.

Este documento foi emitido pelo SUAP em 16/08/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifap.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 18975
Código de Autenticação: 6ded19678a

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

Política de Segurança da Informação - POSIN

Origem

Diretoria de Tecnologia da Informação

Coordenação de Segurança da Informação

Referência Normativa

Lei nº 8.112/90 (Regime jurídico dos servidores civis da União).

Decreto nº 9.637/18 (Política Nacional de Segurança da Informação).

IN DSIC-GSIPR nº 1 de maio de 2020 (Estruturação da gestão da POSIN).

Portaria GSI/PR nº 93 de 2019 (Glossário de Segurança da Informação).

ABNT NBR ISSO/IEC 27001:2013.

ABNT NBR ISO/IEC 27002:2013.

NBR 16665:2019 - Cabeamento Estruturado.

Resolução IFAP n° 008/2020 (Plano de Gestão de Risco do IFAP).

Campo de Aplicação

Esta Política de Segurança da Informação – POSIN, se aplica em todo o âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP.

Objetivo

Definir diretrizes, responsabilidades, competências e apoio a alta direção na implementação da gestão de segurança da informação do Instituto Federal de Educação, Ciência e Tecnologia do Amapá - IFAP, buscando assegurar a disponibilidade, autenticidade, integridade e confidencialidade das informações.

Fundamento Legal

Conforme o Decreto no 9.637, de 26 de dezembro de 2018, que institui a PNSI (Política Nacional de Segurança da Informação) e Instrução Normativa DSIC-GSIPR nº 1 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.

Escopo

A Política de Segurança da Informação proposta neste documento é aplicável a todos os bens e serviços de Tecnologia de Informação disponibilizados pelo Instituto, bem como aos servidores, terceirizados, discentes ou qualquer pessoa que de alguma forma esteja em uso dos serviços oferecidos de maneira eletrônica.

Conceitos e Definições

Comitê de Segurança da Informação - CSI: grupo de pessoas que tem a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do Instituto Federal de Ciência e Tecnologia do Amapá;

Diretoria de Tecnologia da Informação - DITI: órgão executivo pertencente à Reitoria, que planeja, dirige, avalia e executa a Política de Tecnologia da Informação em todo o Instituto, em articulação com as Pró-Reitorias, Diretorias Sistêmicas e as Direções Gerais dos Campi;

Coordenação de Segurança da Informação – COSEGI: responsável pelo gerenciamento da segurança dos serviços fornecidos através da rede de dados do IFAP.

Recursos de Tecnologia da Informação e Comunicação: equipamentos, instalações e recursos de informação direta ou indiretamente administrados pela DITI, mantidos ou operados em qualquer dependência do Instituto, tais como:

- Equipamentos de informática e de telecomunicações de qualquer espécie;
- Infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie;
- Laboratórios de informática de qualquer espécie;
- Recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados ou transmitidos por meio da infraestrutura computacional do IFAP.

Usuário: qualquer pessoa física ou jurídica com vínculo ou em condição autorizada que utiliza de alguma forma, recursos de tecnologia da informação e comunicação do IFAP. Os usuários poderão ser cadastrados ou não no domínio e serão classificados, para fins de acesso aos recursos, de acordo com suas atribuições respeitando o princípio do mínimo necessário para a execução de suas atribuições;

Unidade de Ensino: os campi, campi avançados, polos permanentes ou temporários e outras estruturas administrativas com atividades pedagógicas que demandem o uso das Tecnologias da Informação.

Os conceitos e definições adotados a seguir estão regulamentados pela portaria GSI/PR nº 93, de 26 de setembro de 2019, que define o Glossário de Segurança da Informação.

Gestor de Segurança da Informação: responsável pelas ações de SI no âmbito do órgão ou entidade da Administração Pública Federal;

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

Estratégia de Continuidade de Negócios: abordagem de um órgão ou entidade que garante a recuperação dos ativos da informação e a continuidade das atividades críticas ao se confrontar com um desastre, uma interrupção ou com outro incidente maior;

Evento de Segurança: qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;

Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

Gestão De Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

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

Serviços de Tecnologia da Informação: provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação;

Política de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);

POSIC: acrônimo de Política de Segurança da Informação e Comunicações. Foi substituído pelo acrônimo POSIN pela Portaria GSI/PR nº 93 de 2019 (Glossário de Segurança da informação aplicado à Administração Pública Federal).

POSIN: acrônimo de Política de Segurança da Informação.

Estrutura da Gestão de Segurança da Informação

Comitê de Segurança da Informação

Fica instituído o Comitê de Segurança da Informação com poderes normativos e deliberativos, presidido pelo Coordenador de Segurança da Informação – COSEGI. Regimento próprio versará sobre a composição e funcionamento.

Gestor de Segurança da Informação

Responsável pelas ações que envolvem a Segurança da Informação no âmbito do Instituto Federal de Ciência e Tecnologia do Amapá. Ocupado pelo Coordenador de Segurança da Informação – COSEGI.

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas à incidente de segurança em redes de computadores. Terá sua composição da seguinte forma:

- Departamento de Governança de TIC – DEGOTIC;
- Coordenador da COSI;
- Coordenador da COSEGI;
- Coordenador da CORI;
- Coordenadores, Supervisores ou chefes de unidades de Tecnologia da Informação dos campi.

Caso seja julgado pertinente, qualquer membro da equipe poderá indicar pessoa diversa para apoio às medidas de tratamento e resposta ao incidente se aceito pelos demais.

Em caso de impedimento do titular, o respectivo substituto ocupará a cadeira junto à equipe.

Princípios

O Instituto Federal de Ciência e Tecnologia do Amapá é regido pelos seguintes princípios da Segurança da Informação.

Confidencialidade: É a propriedade da informação que garante que os dados não estarão disponíveis a indivíduos, entidades ou processos sem autorização.

Integridade: Princípio que garante que o conteúdo da mensagem não será alterado por quem não tiver autorização.

Disponibilidade: Garante que a informação estará acessível para indivíduos, entidades ou processos autorizados na forma e pelo tempo acordado.

Autenticidade: Visa confirmar que os dados são de fato provenientes de determinada fonte, assegurando que foram criados, expedidos, alterados ou destruídos por certo indivíduo, entidade ou processo.

Irretratabilidade ou Não repúdio: Após a garantia da autenticidade o indivíduo, entidade ou processo não possa negar a autoria de uma ação específica.

Legalidade: O uso da tecnologia da informação e comunicação será baseado em todos os preceitos legais devendo seguir o ordenamento jurídico vigente na República Federativa do Brasil e por conseguinte as regulamentações internas do IFAP.

Diretrizes Gerais

Tratamento da Informação

Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da Instituição de tal forma a garantir integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.

O descarte de informações sensíveis deverá ser realizado através de meios não reversíveis.

Cópias de segurança das informações deverão ser tomadas com base na norma de gerenciamento de cópias de segurança da informação aprovadas na Instrução Normativa nº 06 de 2018.

As cópias de segurança deverão ser testadas, validadas e armazenadas de tal forma a evitar a perda da informação por alguma eventualidade ou problemas na restauração dos dados.

Segurança Física e do Ambiente

Deve ser composto por um sistema de pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas ou de procedência ambiental.

Ativos deverão ser protegidos por um perímetro mínimo necessário estipulado pelo responsável levando em consideração os eventuais prejuízos financeiros e aos serviços de TI dependentes do ativo.

O suprimento de energia elétrica assim como toda a malha de cabos devem seguir no que for possível a NBR 16665:2019 (cabeamento estruturado) devendo ser justificado a não conformidade por escrito com a anuência do responsável da unidade juntamente com suas implicações.

Gestão de Incidentes em Segurança da Informação

Tem como principal objetivo restaurar a operação normal do serviço o mais rápido possível, minimizando os prejuízos à operação do negócio e garantindo assim o melhor nível de serviço e disponibilidade.

Considera-se Incidente de Segurança qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores conforme portaria Nº 93/2019 do Gabinete de Segurança Institucional da Presidência da República.

Deve-se registrar todo o ciclo de vida do incidente com o objetivo de compreendê-lo e solucioná-lo evitando o retrabalho posterior para o mesmo incidente. O registro deve haver ao mesmo:

- Registro do incidente;
- Classificação com referência a categoria e prioridade do incidente;
- Diagnóstico e análise;
- Registro da solução definitiva ou solução de contorno com comunicação ao interessado;
- Fechamento.

Se for o caso, o registro do escalonamento funcional ou hierárquico do incidente também deve ser registrado.

Todos os incidentes devem ser registrados e geridos preferencialmente no Sistema Unificado de Administração Pública – SUAP gerido e disponibilizado pela DITI.

Gestão de Ativos

Objetiva cuidar de todos os componentes de tecnologia tangíveis ou intangíveis referente ao oferecimento de serviços de tecnologia da informação de maneira satisfatória pela DITI ou unidades de ensino. Visando reduzir desperdícios de tempo e recursos.

É necessário que todos os ativos sejam inventariados e classificados de acordo com o nível exigido de segurança, além da indicação de seu responsável e sua respectiva anuência.

Regulamentação específica disporá sobre a classificação dos ativos em Tecnologia da Informação.

Gestão de uso dos recursos operacionais e de comunicação

Recursos operacionais e de comunicação

Todos os servidores, terceirizados e discentes que demonstrarem a necessidade de acesso aos recursos de Tecnologia da Informação do IFAP terão seu acesso franqueado de acordo com as diretrizes definidas para seu perfil, definidas por meio de requisitos técnicos e levando em consideração o princípio do menor privilégio.

O acesso aos recursos deverá ser munido de controles físicos e lógicos, com objetivo de proteger equipamentos, aplicativos e arquivos de dados contra perda, alteração ou divulgação não autorizada.

Usuários pertencentes ao grupo discentes deverão observar no que couber a Instrução Normativa nº 04/2016 que disciplina sobre a utilização da rede e Internet do Instituto.

Com exceção dos usuários discentes todos os demais deverão por meio de um termo de responsabilidade específico já normatizado na IN 05/2016 sem prejuízo a IN 04/2016 assumir compromisso no que se refere à:

- Declaração do conhecimento e aceitação dos termos desta política de segurança e de suas políticas e normas complementares, não podendo alegar desconhecimento;
- Declaração de estar ciente que os acessos realizados à Internet, assim como conteúdo das mensagens de correio eletrônico institucional são passíveis de auditoria;
- Manter a confidencialidade de sua senha, alterando a mesma sempre que existir qualquer indício de possível comprometimento, em intervalos regulares de tempo ou com base no número de acessos ou de períodos, a critério da DITI.

É de inteira responsabilidade do usuário a proteção das informações institucionais que estejam sob sua responsabilidade, utilizadas no âmbito do Instituto ou fora de suas dependências.

Uso de e-mail corporativo

O serviço de correio eletrônico do IFAP é oferecido como recurso de uso exclusivamente profissional para apoiar os usuários autorizados no cumprimento dos objetivos institucionais e serão passíveis de auditoria.

O serviço de correio eletrônico deverá garantir o sigilo, o não repúdio e a autenticidade. Os usuários devem zelar por suas credenciais de acesso e observar a Instrução Normativa pertinente que dispõe sobre o uso aceitável do e-mail institucional.

Controle de Acesso

Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

Qualquer privilégio concedido ao usuário de sistema deve ser autorizado pelo responsável imediato do ativo observando a princípio do menor privilégio para a execução de suas atividades.

Gestão de Risco

Entende-se como gestão de riscos o processo que visa à proteção dos serviços tecnológicos do IFAP, por meio do procedimento de mitigar, compartilhar, evitar e aceitar o risco, conforme seja estrategicamente mais viável. Sempre de acordo com o Plano de Gestão de Riscos aprovado na resolução n° 008/2020.

As normas e procedimentos para implantação e gerenciamento de riscos da Informação serão definidos em documento específico elaborado pela DITI através da Coordenação de Segurança da Informação – COSEGI tendo sua eficácia condicionada à aprovação do Comitê de Segurança da Informação e respeitando a Resolução 008/20.

Gestão de Continuidade

Será orientado pelo Programa de Gestão da Continuidade de Negócios (PGCN) sendo este um processo contínuo de gestão e governança suportado pela alta direção para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio de análises críticas, testes, treinamentos e manutenção. Em sua composição constarão minimamente o Plano de Gerenciamento de Incidentes - PGI, Plano de Continuidade de Negócios - PCN e o Plano de Recuperação de Negócios – PRN.

O Plano de Gerenciamento de Incidentes – PGI: processo a ser iniciado em caso de ocorrer um incidente. Busca definir pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

O Plano de Continuidade de Negócio – PCN: tem como objetivo manter em funcionamento os serviços e processos críticos do IFAP na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que venha a ocorrer.

Plano de Recuperação de Negócios – PRN: é a documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade;

O PGI, PCN e PRN do IFAP serão definidos pela COSEGI com base na análise de riscos e terá a aprovação do Comitê de Segurança da Informação.

Auditoria e Conformidade

Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos computacionais oriundos do IFAP.

Os procedimentos de auditoria e de monitoramento de uso dos recursos serão realizados periodicamente pela DITI, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

Havendo evidência de atividade que possa comprometer o desempenho ou a segurança dos recursos ou que infrinja a POSIN e normas complementares, será permitido à DITI auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso, podendo restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser imediatamente comunicado à chefia imediata do usuário, à direção geral do campus ou ao Gabinete da Reitoria a dependendo da gravidade.

Sendo considerada gravidade baixa a atividade que comprometa apenas a máquina do usuário, gravidade média a atividade que comprometa o desempenho da rede e gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços ou que coloque em risco a imagem da Instituição.

Será mantido pela ouvidoria do IFAP canal de comunicação para receber denúncias de infração a qualquer parte desta política de segurança através dos seguintes canais de comunicação:

- E-mail: ouvidoria@Ifap.edu.br ou;
- Site http://www.ouvidorias.gov.br/

Para mais informações acesse: http://ifap.edu.br/index.php/ouvidoria/apresentacao

Competências

Comitê de Segurança de Tecnologia da Informação

- Definir as diretrizes para gestão de riscos de TI;
- Elaborar, aprovar e revisar periodicamente a Política de Segurança da Informação - POSIN e normas relacionadas;
- Elaborar propostas de normas complementares e políticas de uso dos recursos de informação no que diz respeito à segurança,
- Aprovar e manter o Plano de Continuidade de Negócio – PCN,
- Definir os serviços de TI mais relevantes para o Instituto que deverão ser protegidos e monitorados de maneira prioritária;
- Decisões sobre questões de segurança da informação e gestão de riscos omissos na política de segurança da informação e normas relacionadas.

Pró-reitoria de Gestão de Pessoas – PROGEP

- Encaminhar os novos servidores para o conhecimento e assinatura do Termo de Responsabilidade junto a DITI ou coordenação do campus conforme norma para utilização de recursos de TI, IN 05/2016.
- Informar à Diretoria de Tecnologia da Informação - DITI sobre realocações no quadro funcional da Instituição com o intuito de que seja alterado o perfil do usuário de acordo com suas novas atribuições em módulos que não dispõe de administração pelo seu responsável.

Demais Gestores

- Zelar pelo cumprimento da Política de Segurança da Informação - POSIN.

Usuários

- Conhecer a POSIN, seguindo as suas diretrizes e normas complementares,
- Adotar comportamento seguro, assumindo atitude proativa e engajada no que diz respeito à proteção das informações do Instituto.

Qualquer usuário poderá sugerir alterações em normas ou procedimentos de segurança visando o aumento do nível de segurança endereçado ao Comitê de Segurança.

Gestor de Segurança da Informação

- Promover a cultura da Segurança da Informação cibernética;
- Propor recursos necessários às ações de segurança da informação e comunicações;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
- Propor normas relativas à segurança da informação e comunicações.

Penalidades

A quem descumprir a presente Política de Segurança da Informação, as normas e procedimentos estabelecidos pelo IFAP serão aplicadas as sanções e penalidades previstas na legislação em vigor, em especial o que consta:

- Lei no 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;
- Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto no 1.171/1994;
- Código Penal, através do Decreto-Lei no 2848/1940;
- Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

Disposições Gerais

Casos omissos, dúvidas ou sugestões surgidas na aplicação do disposto na Política de Segurança da Informação do IFAP devem ser direcionados ao Comitê de Segurança da Informação.

Atualização

Todos os instrumentos normativos gerados a partir da POSIN, incluindo a própria POSIN, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 04 (quatro) anos.

Eficácia

Revogam-se as disposições em contrário.

Esta Política de Segurança entra em vigor na data de sua publicação.