

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. INTRODUÇÃO	4
2. OBJETIVO	4
3. ABRANGÊNCIA.....	5
4. DIRETRIZES GERAIS	6
4.1. INTERPRETAÇÃO	6
4.1.1. TERMINOLOGIA E DEFINIÇÕES	6
4.1.2. RESTRIÇÃO DE INTERPRETAÇÃO.....	6
4.2. PROPRIEDADE	7
4.2.1. PROPRIEDADE E DIREITO DE USO EXCLUSIVOS:	7
4.2.2. RECURSOS DE TIC PARA ATIVIDADES OPERACIONAIS:.....	7
4.2.3. USO RESTRITO A ATIVIDADES PROFISSIONAIS:.....	7
4.2.4. UTILIZAÇÃO DE MARCAS E IDENTIDADE VISUAL:.....	7
4.2.5. MENÇÃO À MARCAGEM CONTEXTOS PROFISSIONAIS:.....	7
4.2.6. ATIVIDADES PROFISSIONAIS:.....	8
4.3. CLASSIFICAÇÃO DA INFORMAÇÃO	8
4.3.1. RESPEITO A CLASSIFICAÇÃO DA INFORMAÇÃO:.....	8
4.3.2. SIGILO PROFISSIONAL E CONTRATUAL:	8
4.3.3. DADOS PESSOAIS:	8
4.3.4. MECANISMOS DE CRIPTOGRAFIA:.....	8
4.4. CONTROLE PARA ACESSO DE COLABORADORES.....	9
4.4.1. IDENTIDADE DIGITAL INDIVIDUAL:	9
4.4.2. IDENTIFICAÇÃO NAS DEPENDÊNCIAS FÍSICAS:.....	9
4.4.3. SEGURANÇA FÍSICA DE ÁREAS CRÍTICAS:	9
4.4.4. PROTEÇÃO DE ATIVOS CRÍTICOS:.....	10
4.5. INTERNET PARA COLABORADORES.....	10
4.5.1. PROPÓSITO DA CONECTIVIDADE:	10
4.5.2. ACESSO INDIVIDUAL E RESPONSABILIDADE:	10
4.6. CORREIO ELETRÔNICO PARA COLABORADORES.....	11

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.6.1. USO PROFISSIONAL:.....	11
4.6.2. ACESSO EM DISPOSITIVOS MÓVEIS:	11
4.6.3. USO DE CORREIO ELETRÔNICO PARTICULAR:.....	11
4.7. REDE SEM FIO (WI-FI) PARA COLABORADORES	11
4.7.1. USO ADMINISTRATIVO:.....	11
4.7.2. ACESSO AUTORIZADO:.....	11
4.8. ARMAZENAMENTO DE INFORMAÇÕES PARA COLABORADORES	12
4.8.1. LOCAL APROPRIADO PARA ARMAZENAMENTO:.....	12
4.8.2. ARMAZENAMENTO DIGITAL NOS SERVIDORES CORPORATIVOS: ...	12
4.8.3. SOLICITAÇÃO DE REMOÇÃO DE CONTEÚDOS:.....	12
4.9. Mídias Sociais para Colaboradores.....	13
4.9.1. Comportamento Seguro nas Mídias Sociais:	13
4.9.2. Participação Institucional Responsável:	13
4.10. Conteúdo Audiovisual para Colaboradores	13
4.10.1. Restrições ao Registro e Compartilhamento:	13
4.10.2. Restrições ao Registro por Colaboradores:.....	13
4.10.3. Restrições ao Conteúdo por Colaboradores:.....	14
4.11. Uso Responsável de Aplicativos de Comunicação para Colaboradores.....	14
4.11.1. Ambiente de Trabalho:	14
4.12. Monitoramento para Colaboradores	14
4.12.1. Registro e Monitoramento:	14
4.12.2. Finalidade do Armazenamento de Dados:	14
4.12.3. Colaboração em Casos de Incidentes:	15
4.13. Contratos para Colaboradores	15
4.13.1. Acesso e Porte de Dispositivos:	15
4.13.2. Desligamento ou Rescisão:.....	15
4.14. Segurança da Informação para Colaboradores	16
4.14.1. Repasse e Transmissão de Informações:.....	16
4.14.2. Cautela na Utilização de Recursos Online:.....	16
4.14.3. Salvaguarda e Restauração de Arquivos Digitais:	16
4.14.4. Descarte Seguro de Informações Confidenciais:	16
4.14.5. Proteção em Caso de Desastres:.....	16

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.14.6. Educação Continuada em Segurança da Informação:.....	17
5. PAPEIS E RESPONSABILIDADES	17
5.1. TODOS- DIRETRIZES PARA COLABORADORES NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	17
5.1.1. CONHECIMENTO E DISSEMINAÇÃO DAS REGRAS:	17
5.1.2. PRESERVAÇÃO DE ATIVOS:.....	17
5.1.3. PRESERVAÇÃO DE RECURSOS INSTITUCIONAIS:.....	17
5.1.4. ZELO PELO PATRIMÔNIO:	17
5.1.5. EVITAR EXPOSIÇÃO DESNECESSÁRIA:	17
5.1.6. PREVENÇÃO DE INCIDENTES:.....	18
5.1.7. CUMPRIMENTO E ATUALIZAÇÃO:.....	18
5.1.8. PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO:.....	18
5.1.9. COMBATE AO BULLYING:	18
5.1.10. REPORTE DE INCIDENTES:	18
5.2. Gestores e Coordenadores	18
5.2.1. Orientação Constante:.....	18
5.2.2. RESPONSABILIDADE DELEGADA:	19
5.2.3. CUMPRIMENTO DA POLÍTICA.....	19
5.2.4. INVESTIGAÇÃO DE INCIDENTES:	19
5.2.5. PARTICIPAÇÃO NO COMITÊ DE SEGURANÇA:	19
5.3. COLABORADORES	19
5.3.1. PRESERVAÇÃO DA VIDA PARTICULAR:.....	19
5.3.2. COMUNICAÇÃO RESPEITOSA:.....	19
5.3.3. USO CONSCIENTE DE MÍDIAS SOCIAIS:	20
6. DISPOSIÇÕES FINAIS.....	20
7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:.....	20
8. APÊNDICE – SIGLAS, TERMOS E DEFINIÇÕES	21

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

1. INTRODUÇÃO

A Faculdade, com uma sede denominada Matriz e suas duas filiais, reconhece a importância crítica da segurança da informação e da infraestrutura de rede para o êxito de suas operações. Nesse contexto, a implementação de uma Política de Segurança da Rede é fundamental para atender às crescentes necessidades de comunicação e conectividade entre esses locais geograficamente dispersos.

Em resumo, este projeto de Política de Segurança da Rede tem como objetivo garantir eficiência operacional, segurança robusta e escalabilidade, atendendo às necessidades específicas de cada localidade da Faculdade. A integração de tecnologias locais e em nuvem, combinada com um monitoramento contínuo, contribui para uma infraestrutura de rede resiliente e adaptável, pronta para enfrentar os desafios dinâmicos do ambiente acadêmico atual.

2. OBJETIVO

A Política de Segurança da Faculdade tem como objetivo principal estabelecer diretrizes e práticas que assegurem a confidencialidade, integridade, disponibilidade e autenticidade das informações e sistemas críticos da organização. Esta política visa garantir uma proteção eficaz contra ameaças cibernéticas, preservando a continuidade operacional, promovendo a conformidade com regulamentações vigentes e cultivando uma cultura de segurança entre todos os colaboradores.

Para alcançar esses objetivos, a política se concentra nos seguintes pontos:

Proteção dos Ativos de Informação: Salvar ativos de informação, incluindo dados sensíveis e sistemas críticos, por meio da implementação de controles de acesso, criptografia e outras medidas de segurança apropriadas.

Gestão de Acessos: Garantir que o acesso aos recursos de tecnologia da informação seja concedido de maneira criteriosa, com base nos princípios de necessidade mínima e atribuição de privilégios conforme as responsabilidades dos colaboradores.

Monitoramento e Detecção de Ameaças: Implementar sistemas de monitoramento contínuo, para identificar precocemente atividades suspeitas, ataques cibernéticos e outras ameaças à segurança da rede.

Políticas de Uso Aceitável: Estabelecer regras claras e diretrizes para o uso apropriado dos recursos de tecnologia da informação, promovendo a conscientização dos colaboradores sobre boas práticas de segurança.

Gestão de Incidentes: Desenvolver e manter um plano abrangente de gestão de incidentes, definindo procedimentos para uma resposta rápida e eficaz a eventos de

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

segurança, minimizando o impacto e prevenindo recorrências.

Atualizações e Patching: Assegurar que todos os sistemas e softwares sejam regularmente atualizados e que as vulnerabilidades sejam corrigidas de maneira oportuna, reduzindo assim o risco de exploração.

Conformidade com Regulamentações: Manter conformidade com leis, regulamentos e padrões aplicáveis relacionados à segurança da informação, garantindo transparência e responsabilidade da instituição.

Educação e Treinamento em Segurança: Fomentar uma cultura de segurança por meio de programas regulares de treinamento e conscientização, capacitando os colaboradores a reconhecer e mitigar ameaças potenciais.

3. ABRANGÊNCIA

A abrangência inclui, mas não se limita a:

Colaboradores: Todos os funcionários, terceirizados, estagiários e qualquer outra entidade que tenha acesso aos sistemas de informação e recursos da Faculdade.

Instalações: Todas as instalações físicas da Faculdade, incluindo escritórios administrativos e centros de processamento de dados.

Sistemas de Informação: Todos os sistemas, servidores, bancos de dados, aplicativos e plataformas tecnológicas utilizadas para processar, armazenar e transmitir informações.

Redes de Comunicação: A infraestrutura de rede, incluindo equipamentos de rede, roteadores, switches, firewalls e outros dispositivos utilizados para facilitar a comunicação entre as instalações.

Dispositivos de Usuários Finais: Todos os dispositivos de propriedade da Faculdade ou utilizados por colaboradores para acessar os sistemas da organização, como computadores, laptops, tablets e smartphones.

Serviços em Nuvem: Todos os serviços em nuvem utilizados pela Faculdade, que estão integrados à infraestrutura de rede.

Processos de Negócios: Todos os processos operacionais, incluindo aqueles relacionados à produção, logística, recursos humanos, finanças e outras áreas funcionais, que

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

dependem de sistemas de informação e infraestrutura de rede.

4. DIRETRIZES GERAIS

4.1. INTERPRETAÇÃO

4.1.1. TERMINOLOGIA E DEFINIÇÕES

Para uma interpretação uniforme desta Política de Segurança da Faculdade (PSF), são adotadas as siglas, termos e definições especificadas no Apêndice A deste documento.

4.1.2. RESTRIÇÃO DE INTERPRETAÇÃO

Esta PSF deve ser interpretada de forma restritiva. Em situações excepcionais ou não contempladas por suas disposições, a realização de atividades específicas somente é permitida mediante prévia e expressa autorização da gestão superior da Faculdade.

4.1.2.1. EXCEÇÕES E AUTORIZAÇÕES PONTUAIS

Qualquer caso excepcional ou permissão diferenciada será concedido de forma pontual, aplicável exclusivamente ao solicitante, dentro dos limites e motivos que fundamentaram a solicitação. A aprovação destas exceções é uma prerrogativa da Faculdade e ocorrerá por mera liberalidade, com duração limitada. A Faculdade reserva-se o direito de revogar tal autorização a qualquer momento, sem necessidade de aviso prévio, caso julgue necessário.

Estas diretrizes visam garantir uma interpretação consistente da PSF, ao mesmo tempo em que proporcionam flexibilidade controlada para lidar com circunstâncias excepcionais que possam surgir durante a implementação e execução das medidas de segurança.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.2. PROPRIEDADE

4.2.1. PROPRIEDADE E DIREITO DE USO EXCLUSIVOS:

Todas as informações geradas, acessadas, recebidas, manuseadas ou armazenadas pela Faculdade, assim como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis, são de propriedade exclusiva de cada unidade.

4.2.2. RECURSOS DE TIC PARA ATIVIDADES OPERACIONAIS:

Os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela Faculdade para o desenvolvimento de atividades operacionais, em todas as suas localidades, são de propriedade de cada unidade ou estão a ela cedidos. Permanecem sob sua guarda e posse, devendo ser utilizados exclusivamente para o cumprimento da finalidade a que se propõem.

4.2.3. USO RESTRITO A ATIVIDADES PROFISSIONAIS:

Todos os ativos tangíveis e intangíveis da Faculdade só podem ser utilizados para o cumprimento das atividades profissionais, limitados à função do colaborador.

4.2.4. UTILIZAÇÃO DE MARCAS E IDENTIDADE VISUAL:

A utilização das marcas, identidade visual e demais sinais distintivos da Faculdade, atuais e futuros, em qualquer veículo de comunicação, incluindo internet e mídias sociais, só pode ocorrer para atender a atividades profissionais, mediante prévia e expressa autorização.

4.2.5. MENÇÃO À MARCA EM CONTEXTOS PROFISSIONAIS:

Todos os colaboradores têm o direito de fazer menção à marca em contextos profissionais, citando o local onde trabalham. Contudo, a marca não deve ser utilizada para criar perfis em mídias sociais em nome da instituição e/ou para representá-la sem a devida autorização.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.2.6. ATIVIDADES PROFISSIONAIS:

Todos os recursos de TIC e informações devem ser utilizados de maneira prioritária para o desenvolvimento de atividades profissionais, promovendo a excelência nas operações e iniciativas relacionadas ao core business da Faculdade.

Esta seção visa preservar a propriedade intelectual e garantir que os recursos tecnológicos e informações sejam direcionados principalmente para atividades profissionais, fortalecendo assim a missão operacional da Faculdade.

4.3. CLASSIFICAÇÃO DA INFORMAÇÃO

4.3.1. RESPEITO A CLASSIFICAÇÃO DA INFORMAÇÃO:

Todos os colaboradores devem respeitar o nível de segurança indicado na classificação das informações. Em caso de dúvida, a informação deve ser tratada como de uso interno, sem divulgação externa, incluindo a internet e mídias sociais, sem autorização expressa.

4.3.2. SIGILO PROFISSIONAL E CONTRATUAL:

É fundamental que todo colaborador respeite o sigilo profissional e contratual, abstendo-se de revelar, transferir, compartilhar ou divulgar informações confidenciais, incluindo detalhes institucionais críticos, de outros colaboradores, fornecedores ou prestadores de serviços.

4.3.3. DADOS PESSOAIS:

Informações envolvendo dados pessoais de colaboradores devem ser tratadas como sigilosas, utilizadas com cautela e apenas por pessoas autorizadas.

4.3.4. MECANISMOS DE CRIPTOGRAFIA:

A equipe de Tecnologia da Informação (GTI) é responsável por homologar mecanismos de criptografia, cifragem ou codificação para o armazenamento e transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

no ambiente de conectividade.

Esta seção destaca a importância do respeito à classificação e sigilo de informações, reforçando as responsabilidades dos colaboradores na proteção de dados confidenciais da Faculdade.

4.4. CONTROLE PARA ACESSO DE COLABORADORES

4.4.1. IDENTIDADE DIGITAL INDIVIDUAL:

Cada colaborador recebe uma identidade digital individual e intransferível para acessar fisicamente e logicamente os ambientes e recursos de Tecnologia da Informação e Comunicação (TIC) da Faculdade.

4.4.1.1. MONITORAMENTO E CONTROLE DA IDENTIDADE DIGITAL:

A identidade digital é monitorada e controlada pela Faculdade.

4.4.1.2. RESPONSABILIDADE DO COLABORADOR

O colaborador é responsável pelo uso e sigilo de sua identidade digital. O compartilhamento, divulgação ou transferência não autorizados são estritamente proibidos.

4.4.2. IDENTIFICAÇÃO NAS DEPENDÊNCIAS FÍSICAS:

Quando a identidade é fornecida pela unidade, todos os colaboradores, prestadores de serviços e visitantes nas dependências físicas da Faculdade devem estar devidamente identificados, portando crachá individual de forma visível.

4.4.2.1. USO INDIVIDUAL DO CRACHÁ

O crachá de identificação é de uso individual e não pode ser compartilhado com outros colaboradores ou terceiros, nem ser utilizado fora das dependências da Faculdade. Tal transgressão pode ser punida de acordo com os artigos 299 (Falsidade Ideológica), 307 (Falsa Identidade) e 304 (Uso de Documento Falso) do Código Penal Brasileiro.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.4.3. SEGURANÇA FÍSICA DE ÁREAS CRÍTICAS:

A Faculdade deve estabelecer espaços físicos seguros para proteger áreas que criam, desenvolvem, processam ou armazenam informações críticas e ativos essenciais, como datacenters, sala de comunicações, salas de documentação crítica, entre outras.

4.4.4. PROTEÇÃO DE ATIVOS CRÍTICOS:

Ativos críticos para a Faculdade devem ser protegidos contra falhas de energia e outras interrupções, além de receber manutenção adequada para garantir sua contínua integridade e disponibilidade.

Esta seção destaca as diretrizes específicas para o controle de acesso, garantindo a segurança física e lógica dos colaboradores na Faculdade.

4.5. INTERNET PARA COLABORADORES

4.5.1. PROPÓSITO DA CONECTIVIDADE:

Os recursos de conectividade são fornecidos para fins administrativos, reconhecendo o acesso à internet como um direito essencial para o exercício da cidadania no Brasil. No entanto, os colaboradores devem utilizar a internet em conformidade com as leis vigentes, sendo responsáveis pelo cumprimento dessas normas.

4.5.2. ACESSO INDIVIDUAL E RESPONSABILIDADE:

O acesso à internet é concedido aos colaboradores por meio de identidade digital (login e senha) pessoal e intransferível. O titular é o único responsável por suas ações e/ou danos decorrentes do uso da internet.

Esta seção destaca as diretrizes específicas para o uso da internet por colaboradores na Faculdade, ressaltando a responsabilidade individual e a observância das leis em vigor.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.6. CORREIO ELETRÔNICO PARA COLABORADORES

4.6.1. USO PROFISSIONAL:

A utilização do correio eletrônico corporativo deve limitar-se à execução de atividades profissionais, seguindo as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

4.6.2. ACESSO EM DISPOSITIVOS MÓVEIS:

O correio eletrônico corporativo pode ser acessado em dispositivos móveis particulares. No entanto, o acesso fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, sendo uma prática de liberalidade e/ou conveniência sem requisição prévia da instituição.

4.6.3. USO DE CORREIO ELETRÔNICO PARTICULAR:

A utilização de correio eletrônico particular ou público é permitida apenas para transmissão ou recebimento de conteúdo ou informações particulares, desde que não prejudique as atividades profissionais ou acadêmicas, não cause impactos negativos para outros usuários, não viole a rede corporativa e acadêmica, e não infrinja normas da Faculdade.

4.7. REDE SEM FIO (WI-FI) PARA COLABORADORES

4.7.1. USO ADMINISTRATIVO:

A Faculdade, quando possível, disponibiliza uma rede sem fio (Wi-Fi) nos ambientes autorizados, limitada ao perímetro físico da instituição, destinada a finalidades administrativas.

4.7.2. ACESSO AUTORIZADO:

Acesso à rede sem fio (Wi-Fi) é concedido apenas a colaboradores expressamente autorizados, que devem comprometer-se a fazer uso seguro desse recurso.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.7.2.1. ACESSO PARA VISITANTES E FORNECEDORES:

Em casos excepcionais, visitantes e fornecedores podem ter acesso à rede sem fio mediante prévia autorização do gestor imediato, da equipe de Tecnologia da Informação (GTI) ou do Comitê de Resposta a Incidentes (CRC).

Esta seção estabelece diretrizes específicas para o uso da rede sem fio por colaboradores, alunos e terceiros na Faculdade, assegurando sua disponibilidade para finalidades administrativas e acadêmicas com controle de acesso autorizado.

4.8. ARMAZENAMENTO DE INFORMAÇÕES PARA COLABORADORES

4.8.1. LOCAL APROPRIADO PARA ARMAZENAMENTO:

Todos os colaboradores devem manter as informações da Faculdade armazenadas no local designado para esse fim.

4.8.2. ARMAZENAMENTO DIGITAL NOS SERVIDORES CORPORATIVOS:

As informações digitais da Faculdade devem ser armazenadas nos servidores da rede corporativa, que possuem controle de acesso e cópia de segurança. Informações físicas devem ser guardadas em locais seguros quando não estiverem em uso, especialmente aquelas relacionadas à identificação de colaboradores.

4.8.3. SOLICITAÇÃO DE REMOÇÃO DE CONTEÚDOS:

A Faculdade deve solicitar o apagamento e/ou a remoção de conteúdos em dispositivos móveis particulares, na internet, em mídias sociais e/ou em aplicativos, sempre que representarem riscos para colaboradores, contrariarem a legislação nacional vigente, prejudicarem o relacionamento ou possam causar danos à instituição.

Esta seção estabelece diretrizes específicas para o armazenamento seguro de informações por colaboradores na Faculdade, resguardando a integridade e a segurança dos dados.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.9. Mídias Sociais para Colaboradores

4.9.1. Comportamento Seguro nas Mídias Sociais:

Colaboradores devem adotar um comportamento seguro no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos pelas políticas da Faculdade.

4.9.2. Participação Institucional Responsável:

A participação institucional do colaborador em mídias sociais, durante o horário de trabalho e a partir do ambiente da Faculdade, deve estar diretamente relacionada à sua função profissional e aos objetivos da Faculdade. O colaborador é responsável por qualquer ação ou omissão resultante de sua postura e comportamento nas mídias sociais.

4.10. Conteúdo Audiovisual para Colaboradores

4.10.1. Restrições ao Registro e Compartilhamento:

Não é permitido aos colaboradores tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da Faculdade, pátios, corredores, banheiros, vestiários ou qualquer outro local pertencente ao perímetro físico, sem prévia autorização.

4.10.1.1. Exceções para Eventos Públicos:

Exceções são permitidas para eventos administrativos, sociais e/ou esportivos, desde que previamente avisados e autorizados, e o conteúdo não exponha ao ridículo nem gere constrangimento aos envolvidos.

4.10.2. Restrições ao Registro por Colaboradores:

Colaboradores devem obter autorização prévia para captar ou reproduzir imagens, vídeos ou sons no ambiente da Faculdade. O registro deve ser utilizado apenas para fins profissionais, com proibição de compartilhamento público, exceto em situações previamente avisadas e autorizadas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.10.2.1. Exceções para Eventos Autorizados:

Exceções são permitidas para eventos administrativos, sociais e/ou esportivos, desde que previamente avisados e autorizados.

4.10.3. Restrições ao Conteúdo por Colaboradores:

Colaboradores não devem captar, reproduzir ou compartilhar imagens, vídeos ou sons que possam comprometer a segurança, sigilo das informações ou envolvam a imagem de outros colaboradores, visitantes, prestadores de serviço e fornecedores sem prévia autorização, exceto em situações previamente avisadas e autorizadas para eventos públicos.

4.11. Uso Responsável de Aplicativos de Comunicação para Colaboradores

4.11.1. Ambiente de Trabalho:

Colaboradores da Faculdade devem utilizar aplicativos de comunicação no ambiente de trabalho, seja dentro ou fora dele, por meio de recursos institucionais ou particulares, para compartilhar informações institucionais. Esse uso deve sempre respeitar o sigilo da informação, atender aos requisitos de segurança desta Política e cumprir as leis nacionais em vigor, evitando riscos desnecessários relacionados ao vazamento de informações ou que comprometam a instituição.

4.12. Monitoramento para Colaboradores

4.12.1. Registro e Monitoramento:

A Faculdade realiza o registro e armazenamento de atividades (logs) e monitora seus ambientes físicos e lógicos. Isso inclui a captura de imagens, áudio ou vídeo, visando a proteção do patrimônio, reputação e a segurança daqueles que se relacionam com a instituição.

4.12.2. Finalidade do Armazenamento de Dados:

O armazenamento dos dados monitorados tem finalidades administrativas e legais,

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

contribuindo para colaborar com as autoridades em investigações quando necessário.

4.12.3. Colaboração em Casos de Incidentes:

Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica dos colaboradores, a Faculdade tem a obrigação de fornecer informações ao órgão competente para apuração, quando necessário, contribuindo com a segurança e a integridade de sua equipe.

4.13. Contratos para Colaboradores

4.13.1. Acesso e Porte de Dispositivos:

O simples porte de dispositivos institucionais e o acesso aos recursos de TIC e/ou informações institucionais, mesmo de forma remota fora do horário normal de expediente, não implicam sobre jornada, sobreaviso ou plantão do colaborador. Essas ações podem ocorrer por ato de liberalidade ou conveniência do próprio colaborador, sem necessidade de expressa e prévia requisição da instituição.

4.13.2. Desligamento ou Rescisão:

Em casos de desligamento, rescisão contratual ou término do contrato, a equipe de Tecnologia da Informação (GTI) e o Centro de Relacionamento com o Colaborador (CRC) devem desativar todas as identidades digitais do colaborador em todos os sistemas e ambientes da Faculdade.

4.13.2.1. Exclusão de Informações no Desligamento:

No desligamento, o colaborador deve excluir todas as informações e contas da Faculdade disponíveis em seu dispositivo móvel particular, caso tenham sido cadastradas.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.14. Segurança da Informação para Colaboradores

4.14.1. Repasse e Transmissão de Informações:

Ao repassar informações da Faculdade o, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, os colaboradores devem agir com cautela. Isso inclui confirmar a identidade do solicitante e a real necessidade do compartilhamento da informação.

4.14.2. Cautela na Utilização de Recursos Online:

Colaboradores devem exercer cautela ao acessar softwares, informações e conteúdos gratuitos na internet, como aplicativos, músicas, vídeos, trabalhos completos, livros digitais e e-mails com propostas suspeitas, devido ao risco de vetores de ataques criminosos.

4.14.3. Salvaguarda e Restauração de Arquivos Digitais:

A equipe de Tecnologia da Informação (GTI) e o Centro de Relacionamento com o Colaborador (CRC) devem manter um processo de salvaguarda e restauração dos arquivos digitais críticos para atender aos requisitos operacionais e legais, garantindo a continuidade do negócio em casos de falhas ou incidentes.

4.14.4. Descarte Seguro de Informações Confidenciais:

Informações confidenciais e recursos de TIC devem passar por procedimentos de destruição que impeçam sua recuperação e o acesso por pessoas não autorizadas quando descartados.

4.14.5. Proteção em Caso de Desastres:

GTI e CRC devem desenvolver estratégias e planos de ação para a proteção de informações e recursos de TIC críticos, garantindo a identificação e preservação adequadas dos serviços essenciais após a ocorrência de desastres.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

4.14.6. Educação Continuada em Segurança da Informação:

A Faculdade está comprometida em orientar constantemente seus colaboradores sobre o uso seguro das informações e da tecnologia, podendo realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança na instituição.

5. PAPEIS E RESPONSABILIDADES

5.1. TODOS- DIRETRIZES PARA COLABORADORES NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. CONHECIMENTO E DISSEMINAÇÃO DAS REGRAS:

Colaboradores devem conhecer e disseminar as regras e princípios da Política de Segurança da Informação.

5.1.2. PRESERVAÇÃO DE ATIVOS:

É responsabilidade dos colaboradores preservar e proteger os ativos tangíveis e intangíveis da PSF e mantidas contra ameaças, incluindo acesso, compartilhamento ou modificação não autorizados.

5.1.3. PRESERVAÇÃO DE RECURSOS INSTITUCIONAIS:

Colaboradores devem preservar e proteger os recursos institucionais, marca, reputação, conhecimento e propriedade intelectual da PSF e mantidas, especialmente suas informações e conteúdo.

5.1.4. ZELO PELO PATRIMÔNIO:

O zelo pela proteção do patrimônio da PSF e mantidas é fundamental, incluindo o uso responsável dos recursos físicos e lógicos fornecidos.

5.1.5. EVITAR EXPOSIÇÃO DESNECESSÁRIA:

Colaboradores devem evitar a exposição desnecessária de informações, projetos,

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

trabalhos e dependências da PSF e mantidas, incluindo mídias sociais e internet, agindo com responsabilidade no uso de recursos de TIC e informações.

5.1.6. PREVENÇÃO DE INCIDENTES:

A prevenção e redução de impactos gerados por incidentes de segurança da informação são responsabilidades dos colaboradores, garantindo confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

5.1.7. CUMPRIMENTO E ATUALIZAÇÃO:

Colaboradores devem cumprir e manter-se atualizados em relação a esta Política, Regimento Interno e demais Normas de Segurança da Informação da PSF e mantidas.

5.1.8. PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO:

É obrigação dos colaboradores proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela PSF e mantidas.

5.1.9. COMBATE AO BULLYING:

Colaboradores devem cumprir o dever de combater a intimidação sistemática (bullying), adotando medidas preventivas e reativas e conscientizando para coibir toda forma de violência na instituição.

5.1.10. REPORTE DE INCIDENTES:

Qualquer incidente que possa impactar na segurança das informações deve ser imediatamente reportado pelos colaboradores através do endereço incidentes@matriz.com.br.

5.2. Gestores e Coordenadores

5.2.1. Orientação Constante:

Gestores e coordenadores devem orientar constantemente suas equipes sobre o uso seguro de ativos tangíveis e intangíveis, e dos valores adotados pela PSF, instruindo-os a disseminar essa cultura entre os demais colaboradores.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

5.2.2. RESPONSABILIDADE DELEGADA:

Devem suportar todas as consequências das funções e atividades que delegarem a outros colaboradores.

5.2.3. CUMPRIMENTO DA POLÍTICA

Gestores e coordenadores têm a responsabilidade de assegurar o cumprimento desta Política e de outras regulamentações por parte dos colaboradores sob sua supervisão.

5.2.4. INVESTIGAÇÃO DE INCIDENTES:

Devem participar ativamente da investigação de incidentes de segurança relacionados às informações, ativos e aos colaboradores sob sua responsabilidade.

5.2.5. PARTICIPAÇÃO NO COMITÊ DE SEGURANÇA:

Gestores e coordenadores devem participar, sempre que convocados, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

5.3. COLABORADORES

5.3.1. PRESERVAÇÃO DA VIDA PARTICULAR:

Colaboradores devem ser cautelosos quanto ao excesso de exposição de sua vida particular, preservando informações como rotinas, trajetos e intimidades. É fundamental manter o sigilo profissional nas mídias sociais, contribuindo para a preservação da imagem e reputação da instituição.

5.3.2. COMUNICAÇÃO RESPEITOSA:

Durante a comunicação, seja presencial ou digital, é esperado que os colaboradores usem linguagem respeitosa e adequada. Evitar termos dúbios, interpretações duplas, exposição da intimidade, abuso de poder, perseguição, discriminação ou qualquer forma de assédio moral ou sexual, contribuindo para um ambiente condizente com o contexto estudantil, acadêmico e administrativo.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

5.3.3. USO CONSCIENTE DE MÍDIAS SOCIAIS:

No uso de mídias sociais, os colaboradores devem evitar excessos de exposição que possam representar riscos para sua própria imagem e reputação, assim como para a instituição. O equilíbrio na utilização dessas plataformas é essencial para manter um ambiente profissional adequado.

6. DISPOSIÇÕES FINAIS

Este documento deve ser interpretado em conformidade com as leis brasileiras, no idioma português, e em conjunto com outras normas da Faculdade.

Atitudes indevidas, ilícitas ou contrárias a esta Política e outras normas de segurança da informação serão consideradas violações, sujeitas a sanções conforme as políticas internas, contratos e normas da instituição.

A Política de Segurança da Informação (PSI) e demais normas estão disponíveis no Portal da Faculdade ou podem ser solicitadas através do e-mail seguranca@matriz.com.br em caso de indisponibilidade. Para esclarecimentos, dúvidas ou informações adicionais sobre esta Política ou outros procedimentos de segurança da informação, colaboradores podem contatar o e-mail: seguranca@matriz.com.br. Incidentes, infrações ou suspeitas devem ser comunicados imediatamente, pessoalmente ou através do endereço incidentes@matriz.com.br

7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:

Este documento complementa os Procedimentos, Códigos e Normas de Segurança da Informação da Faculdade e está alinhado com os seguintes padrões e normativas:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Código de prática para

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

controles de segurança da informação;

- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Gestão de riscos de segurança da informação;

8. APÊNDICE – SIGLAS, TERMOS E DEFINIÇÕES

PSF: Política de Segurança da Faculdade

GTI: Gerência de Tecnologia da Informação

CRC: Comitê de Resposta a Incidentes

TIC: Tecnologia da Informação e Comunicação

IDENTIDADE DIGITAL: Credencial única e intransferível para acesso aos ambientes e recursos de TIC.

CRACHÁ DE IDENTIFICAÇÃO: Dispositivo individual de identificação utilizado pelos colaboradores.

REDE SEM FIO (Wi-Fi): Infraestrutura para conectividade sem fio, restrita a ambientes autorizados.

LOGS: Registros de atividades, incluindo imagens, áudio ou vídeo, para monitoramento e proteção dos ativos.

SOBREJORNADA: Atividade além do expediente normal.

SIGILO PROFISSIONAL: Dever de não revelar informações confidenciais ou internas.

MÍDIAS SOCIAIS: Plataformas online para compartilhamento de informações, imagens e

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2024
	Versão: 1.1
Classificação: Interna	Última revisão: 01/06/2024

vídeos.

PLANTÃO: Atividade de prontidão fora do horário normal, requerendo requisição expressa da instituição.

INTIMIDAÇÃO SISTEMÁTICA (BULLYING): Comportamento repetitivo que visa intimidar ou prejudicar.

SOBREAVISO: Disponibilidade para ser chamado ao serviço, além do expediente normal.