SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE - FURG
SECRETARIA EXECUTIVA DOS CONSELHOS
CONSELHO UNIVERSITÁRIO

# RESOLUÇÃO CONSUN/FURG Nº 5, DE 20 DE MAIO DE 2022

Dispõe sobre a Política de Segurança da Informação da FURG.

O REITOR DA UNIVERSIDADE FEDERAL DO RIO GRANDE- FURG, na qualidade de Presidente do CONSELHO UNIVERSITÁRIO, considerando a Ata de nº 472 deste Conselho, de reunião realizada em 20 de maio de 2022, e o Processo nº 23116.001077/2022-19**,**

**RESOLVE:**

Art. 1° Instituir a Política de Segurança da Informação da Universidade Federal do Rio Grande - FURG (PSI/FURG), contendo as diretrizes, objetivos e estruturas voltadas à segurança da informação, pautadas nos princípios de autenticidade, confidencialidade, disponibilidade, integridade e conformidade.

Parágrafo Único. Integram, também, a presente Política, normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização. Aplicam-se ainda os conceitos do Anexo I com base nas referências legais e normativas do Anexo II, e o Termo de Responsabilidade e Sigilo do Anexo III.

## CAPÍTULO I
## DOS PRINCÍPIOS

Art. 2° A Política de Segurança da Informação (PSI) deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, com destaque para:

I - Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade com as devidas autorizações;

II - 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 autorizada nem credenciada;

III - Disponibilidade: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário;

IV - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental. Uma vez garantida a autenticidade e a integridade, a irretratabilidade (não repúdio) garante que o autor não possa negar a autoria da informação;

V - Conformidade: é a garantia do cumprimento das legislações, normas e

procedimentos relacionados à segurança da informação, privacidade e proteção a dados pessoais.

## CAPÍTULO II
## DOS OBJETIVOS

Art. 3° O objetivo desta política é estabelecer diretrizes, processos e responsabilidades no que diz respeito à gestão, tratamento, controle e proteção dos ativos de informação e processamento, servindo de norma à administração na implementação da segurança da informação da FURG, buscando assegurar os princípios desta política.

## CAPÍTULO III
## DAS DIRETRIZES

Art. 4° As diretrizes da segurança da informação devem considerar, prioritariamente, os requisitos legais, os princípios, bem como os objetivos estratégicos do Plano de Desenvolvimento Institucional da FURG.

Art. 5° A PSI deve garantir a segurança da informação tanto aos sistemas no ambiente de computação quanto aos meios convencionais de processamento, comunicação e armazenamento independente do suporte.

Art. 6° A FURG deve dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo que está sendo protegido e de acordo com a identificação de riscos potenciais à atividade fim da Universidade.

Art. 7° Toda e qualquer informação gerada, adquirida, processada ou armazenada pela FURG é um ativo e deve ser protegida.

Art. 8° Sobre a Propriedade Intelectual:
I - Os ativos de informação produzidos no âmbito da FURG por usuários internos, colaboradores e prestadores de serviço, no exercício de suas funções, são patrimônio intelectual da FURG;
II - É vedada a utilização de informações produzidas para uso exclusivo da FURG em quaisquer outros projetos ou atividades de uso diverso do estabelecido pela instituição, salvo com autorização específica pelos gestores dos ativos de informação, nos processos e documentos de sua competência; e
III - Todos os usuários devem atentar-se a legislação vigente no país sobre direitos autorais, propriedade industrial e a política institucional de inovação e tecnociência solidária e normas relacionadas.

Art. 9° A estrutura de gestão da segurança da informação deve promover e manter um “Programa Contínuo de Capacitação em Segurança da Informação” que permita a seus colaboradores: reconhecer ataques; executar as melhores práticas de autenticação e tratamento de dados; evitar exposição não intencional de dados; reconhecer e notificar incidentes de segurança da informação; identificar e notificar a falta de atualização de segurança nos ativos corporativos; saber sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras.

Art. 10 Para fins da segurança da informação esta Política deve orientar a institucionalização dos seguintes processos:

I. da Classificação e Tratamento da Informação;
II. da Gestão de Ativos e Recursos de TI;
III. da Gestão de Controle de Acesso;
IV. do Backup de Dados e Informações;
V. da Gestão de Riscos de Segurança da Informação;
VI. da Gestão de Incidentes de Segurança da Informação;
VII. da Gestão de Continuidade de Negócios;
VIII. da Gestão de Mudanças.

## CAPÍTULO IV
## DA ABRANGÊNCIA

Art. 11 Servidores, estudantes, colaboradores e quaisquer pessoas que tenham acesso aos dados, sistemas, sites, aplicativos e informações geradas, adquiridas, processadas ou armazenadas pela FURG, em função de suas atividades, atribuições ou relações de trabalho, sujeitam-se às diretrizes, normas e procedimentos de segurança da informação da Política de que trata este documento, e são responsáveis por garantir a segurança dos dados e informações a que tenham acesso.

## CAPÍTULO V
## DA ESTRUTURA DE GOVERNANÇA

Art. 12 A estrutura de gestão da segurança da informação compreende:- A Alta Administração;
I - O Gestor de Segurança da Informação;
II - O Comitê Gestor de Segurança da Informação (CGSI);
III - A Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR);
IV - O Comitê de Governança Digital (CGDig);
V - O Centro de Gestão de Tecnologia da Informação (CGTI);
VI - Os Gestores das Unidades Acadêmicas e Administrativas (Diretores e Coordenadores) dos campis da FURG;
VII - O Custodiante da Informação;
VIII - O Usuário dos Ativos de Informação, Sistemas e Serviços da FURG;
IX - A Coordenação de Arquivo Geral;
X - O Comitê Gestor de Proteção de Dados Pessoais (CGPD);
XI - A Comissão Permanente de Avaliação de Documentos (CPAD/FURG);
XII - A Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS/FURG).

## CAPÍTULO VI
## DAS COMPETÊNCIAS

Art. 13 Compete à Alta Administração da FURG prover a orientação e o apoio necessários às ações de segurança da informação, de acordo com os objetivos estratégicos da instituição e com as leis e regulamentos vigentes, tendo como responsabilidades:
I - designar o Gestor de Segurança da Informação;
II - instituir o Comitê Gestor de Segurança da Informação (CGSI);

III - prover a disponibilidade de recursos orçamentários para garantir as ações de implementação desta Política.

Art. 14 Compete ao Gestor de Segurança da Informação:
I - assessorar a Alta Administração na implementação da PSI;
II - coordenar o Comitê Gestor de Segurança da Informação;
III - representar o Comitê Gestor de Segurança da Informação em eventos oficiais;
IV - apresentar à Alta Administração as necessidades de recursos para as ações de segurança da informação;
V - responder junto ao Comitê Gestor de Segurança da Informação às diligências relativas à segurança da informação, promovidas por meio de auditoria interna ou externa;
VI - orientar a comunidade universitária em relação a institucionalização dos processos de segurança da informação;
VII - encaminhar a PSI para análise do Comitê de Governança Digital, sempre que necessário.

Art. 15 Compete ao Comitê Gestor de Segurança da Informação (CGSI), órgão colegiado de natureza deliberativa e de caráter permanente, as seguintes atribuições:
I - assessorar o Gestor de Segurança da Informação e as Unidades da FURG em matérias relativas à segurança da informação na FURG;
II - formular, revisar e monitorar diretrizes, normas e mecanismos institucionais que visem o cumprimento e implementação da PSI;
III - avaliar regularmente a aplicação da PSI em consonância com os comitês e comissões que estabelecem a estrutura de gestão desta Política;
IV - revisar periodicamente a PSI;
V - analisar os pedidos de elaboração ou revisão de normas relativas à segurança da informação;
VI - indicar a composição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);
VII - atuar em conjunto com a ETIR nos assuntos relativos à segurança da informação;
VIII - propor ações permanentes de divulgação, treinamento, educação e conscientização sobre políticas, normas e procedimentos que promovam a segurança da informação.

Art. 16 Compete à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR):
I - analisar, tratar e responder aos incidentes, recebendo, filtrando, classificando e respondendo de forma reativa sempre que houver algum incidente de segurança em tecnologia da informação;
II - emitir alertas e advertências imediatas diante de um incidente de segurança ou vulnerabilidade descoberta;
III - orientar quanto às normas e procedimentos para que as soluções tecnológicas atendam a presente Política;
IV - elaborar o Plano de Gestão de Incidentes.

Art. 17 Compete ao Comitê de Governança Digital (CGDig), no que se refere à Segurança da Informação:
I - receber e analisar proposições referente a PSI encaminhadas pelo Gestor de Segurança da Informação;
II - indicar grupos de trabalhos relativos a segurança da informação sempre que demandado pelo Gestor de Segurança da Informação;
III - aprovar alterações na Política de Segurança da Informação;

IV - promover consultas públicas referente a temática de segurança da informação sempre que necessário ou demandado pelo Gestor de Segurança da Informação;
V - encaminhar a PSI para análise e aprovação do Conselho Universitário, sempre que necessário.

Art. 18 Compete ao Centro de Gestão de Tecnologia da Informação (CGTI), no que se refere à Segurança da Informação:
I. realizar suas atividades visando evitar que sejam inseridos novos riscos no ambiente de tecnologia da informação da FURG;
II. implementar e avaliar a eficácia dos controles de segurança da informação nas tecnologias utilizadas na FURG;
III. informar ao Gestor de Segurança da Informação e demais interessados os riscos residuais resultantes da avaliação dos controles de segurança da informação;
IV. definir e realizar análises de vulnerabilidades periódicas no ambiente de tecnologia da informação da FURG;
V. monitorar o ambiente de tecnologia, gerando indicadores e históricos de uso:
a) da capacidade instalada da rede e dos equipamentos;
b) tempo de resposta no acesso à Internet e aos sistemas críticos;
c) períodos de indisponibilidade no acesso à Internet e aos sistemas críticos;
VI. tomar as ações cabíveis em seu âmbito de atuação quando da identificação de incidentes de segurança;
VII. indicar à Alta Administração o Gestor de Segurança da Informação.

Art. 19 Compete aos Gestores das Unidades da FURG, no que se refere à segurança da informação:
I - comunicar os usuários e colaboradores sob sua supervisão as diretrizes da PSI;
II - indicar TAEs e demais gestores da unidade para participação em processos formativos referente a segurança da informação;
III - atender as orientações do Comitê Gestor de Segurança da Informação;
IV - participar de processos formativos relativos à segurança da informação promovidos pelo CGSI;
V - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;
VI - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação de sua Unidade;
VII - gerenciar o acesso às informações exclusivamente para pessoas devidamente autorizadas e conforme classificação de sigilo e legislação vigente.

Art. 20 Compete ao Custodiante da Informação, no que se refere à segurança da informação:
I - ter pleno conhecimento e seguir esta PSI;
II - responder por toda atividade executada com o uso de sua identificação;
III - notificar, com a maior brevidade possível incidentes de segurança da informação;
IV - cumprir todas as legislações inerentes a segurança da informação;
V - fazer uso correto dos dados pessoais do cidadão de forma a preservar a segurança e a privacidade dos dados utilizados;
VI - zelar pela segurança e bom funcionamento dos ativos da informação da FURG.

Art. 21 Compete ao Usuário dos Ativos de Informação, Sistemas e Serviços da FURG, no que se refere à segurança da informação:
I - responsabilizar-se pela precisão e veracidade dos dados informados;
II - comprometer-se em manter o sigilo de sua credencial de acesso, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido,

após o ato de compartilhamento;
III - respeitar a Política de Segurança da Informação e normas relacionadas;
IV - solicitar a remoção de acessos indevidos à sistemas e serviços quando constatada alguma inadequação;
V - utilizar os ativos e as informações somente para o desempenho das suas atividades institucionais;
VI - aceitar os Termos de Responsabilidade e os Termos de Uso dos Serviços Institucionais, atestando o conhecimento da existência da PSI da FURG;
VII - proteger os ativos da FURG, incluindo informação, evitando perda ou modificação de dados, *software* e *hardware*;
VIII - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade e legislação vigente;
IX - observar restrições em relação à manutenção e instalação de *software* e *hardware* conforme normas estabelecidas;
X - notificar, com a maior brevidade possível a ocorrência de incidentes de segurança da informação;
XI - ter consciência da responsabilização na reparação de danos indicada nos termos de responsabilidade e termos de uso.

Art. 22 Compete à Coordenação de Arquivo Geral, no que se refere à segurança da informação:
I - normatizar as atividades de gestão, preservação e acesso da informação no âmbito do Sistema de Arquivos da Universidade de Federal do Rio Grande - FURG (SIARQ/FURG);
II - garantir a produção, tramitação, preservação e utilização para manter a autenticidade, a confiabilidade e garantir o acesso contínuo em longo prazo aos documentos sob custódia, independente do suporte (SIARQ/FURG);
III - assegurar a classificação arquivística, a guarda, avaliação, transferência e recolhimento de documentos, observando os prazos de guarda e a destinação final, conforme previsto nas tabelas de temporalidade de documentos e normativos vigentes (SIARQ/FURG).

Art. 23 Compete ao Comitê Gestor de Proteção de Dados Pessoais (CGPD), as seguintes atribuições no que se refere à segurança da informação:
I - atuar como canal de comunicação entre a FURG e os titulares dos dados e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD);
II - sensibilizar e capacitar a comunidade universitária sobre a Lei Geral de Proteção de Dados Pessoais - LGPD;
III - recomendar o equacionamento das vulnerabilidades identificadas no diagnóstico de proteção de dados pessoais e na gestão de riscos, formulando princípios e diretrizes para a gestão de dados pessoais;
IV - desenvolver políticas internas de privacidade e proteção de dados pessoais;
V - monitorar os mecanismos de tratamento e proteção dos dados pessoais existentes e propor adequações à LGPD.

Art. 24 Compete à Comissão Permanente de Avaliação de Documentos (CPAD), as seguintes atribuições no que se refere à segurança da informação:
I - promover a divulgação e orientar a aplicação dos Códigos de Classificação de Documentos (CCD) e das Tabelas de Temporalidade e Destinação de Documentos (TTDD) relativos às atividades-meio e fim aprovadas pelo Arquivo Nacional, assim como promover sua atualização, quando necessário, revendo descritores, prazos de guarda e destinação final, encaminhando-os para aprovação do Arquivo Nacional;
II - conduzir o processo de avaliação dos documentos custodiados pela FURG,

tendo em vista preservar os documentos que possuem valor secundário (histórico, probatório, social ou de interesse institucional), e autorizar a eliminação dos documentos destituídos de tais valores, que já tenham cumprido os prazos legais;
III - elaborar, excepcionalmente, o Plano de Destinação de Documentos (PDD), quando os conjuntos documentais não constarem no CCD e na TTDD relativo às atividades-meio e/ou quando da inexistência de CCD e de TTDD relativos às atividades-fim, conforme orientação do Arquivo Nacional.

Art. 25 Compete à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), as seguintes atribuições no que se refere à segurança da informação:
**I** - assessorar quanto à classificação, reclassificação ou reavaliação de informações classificadas em qualquer grau de sigilo;
**II** - analisar os pedidos de acesso à informação e demais dados e documentos, quando solicitado, quanto à possibilidade de disponibilização das informações, assegurando a proteção das informações legalmente resguardadas.

## CAPÍTULO VII
## DOS PROCESSOS

Art. 26 A classificação da informação prevê que os dados e as informações sob custódia ou de propriedade da FURG devem ser classificados quanto aos aspectos de seu valor, requisitos legais e criticidade de forma a receber o nível de proteção adequado em atendimento à legislação vigente.

Art. 27 A Gestão de Ativos deve registrar, acompanhar e corrigir todos os ativos corporativos de TI (e.g. equipamentos de patrimônio da Universidade, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos da Internet das Coisas - *IoT* e servidores conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI da FURG, incluindo aqueles em ambientes de nuvem - *cloud computing*), com o objetivo de conhecer com precisão todos os ativos de *hardware* da organização que precisam ser monitorados e protegidos, e a identificar equipamentos não autorizados e/ou não gerenciados, os quais devem ser removidos ou corrigidos.

Art. 28 A Gestão de Controle de Acesso prevê a concepção de mecanismos de controle através de Plano de Controle de Acesso (PCA), e Planos de Segurança Física e do Ambiente, com objetivo de proteger os ativos contra danos, perda, modificação ou divulgação não autorizada.

Art. 29 O Processo de Backup é o conjunto de procedimentos periódicos estabelecidos a fim de evitar que dados e arquivos institucionais sejam permanentemente perdidos ou danificados em caso de algum incidente, seja ele físico, lógico, ambiental ou falha humana, através da criação periódica de cópias dos dados e informação em local seguro, devendo ser normatizado por Plano ou Política de Backup.

Art. 30 A Gestão de Riscos de Segurança da Informação em nível institucional constitui o desenvolvimento de Plano de Gestão de Riscos de Segurança da Informação para aumentar a capacidade da organização de lidar com incertezas, por meio de um conjunto de atividades e tarefas que permitam identificar e implementar as medidas de proteção necessárias, minimizando ou eliminando os riscos a que estão sujeitos os ativos de informação, equilibrando os custos operacionais e financeiros envolvidos.

Art. 31 A Gestão de Incidentes de Segurança da Informação prevê a concepção de um Plano de Gestão de Incidentes de Segurança da Informação que descreva o processo para responder às situações de emergência, ou evento de risco, que venham ocasionar algum impacto aos ativos da informação mantidos pela FURG, definindo assim, os passos necessários para uma resposta ágil e precisa, atendendo as exigências legais de comunicação e transparência para segurança da informação e privacidade.

Art. 32 A Gestão de Continuidade de Negócios em segurança da informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da FURG, além de recuperar perdas de ativos de informação em nível aceitável, e prevê a concepção de Planos de Continuidade Operacional (PCO) e Planos de Recuperação de Desastres (PRD).

Art. 33 A Gestão de Mudanças visa a implementação de processos apresentados em Planos de Mudanças, que preparem e adaptem as unidades para as mudanças decorrentes da evolução da tecnologia da informação e do ambiente, e deve ser respaldado pelas informações no Relatório de Identificação, Análise, Avaliação e Tratamento de Riscos de Segurança.

Art. 34 As atividades, documentos e competências relacionadas a cada processo devem ser regulamentadas em normativas específicas.

## CAPÍTULO VIII
## DAS VEDAÇÕES

Art. 35 É vedado ao usuário dos recursos de TI:
I – acessar ou tentar acessar os recursos de TI sem autorização;
II – passar-se por outra pessoa ou omitir sua identidade na utilização dos recursos de TI da FURG, salvo nos casos em que o acesso anônimo é explicitamente permitido;
III – violar as autorizações da FURG ou de terceiros, como também os contratos de licenças de uso e outros relativos ao uso de recursos de TI;
IV – interferir no uso correto e na integridade dos recursos da FURG ou externos, se acessados por meio da rede FURG;
V – violar a propriedade intelectual, inclusive direitos autorais ou patentes;
VI – obter benefícios financeiros ou de outra espécie, para si ou para terceiros, por meio da utilização dos recursos de TI da FURG, salvo quando autorizado explicitamente pelo representante legal da Universidade.

Art. 36 Qualquer suspeita ou constatação de infração ao disposto desta política devera ser comunicada ao CGSI.

Art. 37 As condutas que importem em infração ao disposto nesta política serão apuradas por meio de instauração de procedimentos administrativos em que se assegure a ampla defesa e o contraditório.

Art. 38 Na inobservância desta Política o usuário pode ter seu acesso ao serviço restringido e serão apuradas as responsabilidades, na forma da legislação em vigor, podendo haver responsabilização penal, civil e/ou administrativa.

## CAPÍTULO IX
## DAS DISPOSIÇÕES FINAIS

Art. 39 Ficam instituídos os seguintes canais oficiais de comunicações sobre o tema de segurança da informação na FURG:

I - O site: https://*segurancadainformacao.furg.br*;

II - O e-mail: *gestorsegurancadainformacao@furg.br*.

Art. 40 Os instrumentos normativos gerados a partir da PSI, incluindo a própria PSI, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 04 (quatro) anos.

Art. 41

Os casos omissos neste documento serão analisados pelo Comitê Gestor de Segurança da Informação (CGSI).

## ANEXO I – DOS CONCEITOS

(RESOLUÇÃO CONSUN/FURG Nº 5, DE 20 DE MAIO DE 2022)

Atividades críticas: Conjunto de processos vinculados às atividades precípuas da FURG, cuja interrupção poderá ocasionar severos transtornos.

Atividades precípuas: Conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade fim da FURG, contemplando todos os ambientes existentes.

Ativos: Todo elemento que agregue valor ao serviço, podendo ser uma informação digital ou física, *hardware* conectado fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (*cloud computing*), *software*, pessoa ou ambiente físico, cuja a quebra da confidencialidade, integridade ou disponibilidade trará prejuízo.

Ativos de informação: Os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

Ativos de rede: Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

Ativos de *hardware*: Equipamentos que compõem os recursos de tecnologia e de informática, como computadores, mídias removíveis, equipamentos de comunicação e conectividade, entre outros, e suas respectivas instalações.

Classificação arquivística: refere-se à organização dos documentos de um arquivo de acordo com um plano/código de classificação ou quadro de arranjo, previamente definido e parte da análise e identificação do conteúdo dos documentos para categorizá-los de modo que possam ser recuperados.

Classificação de sigilo: Atribuição a documentos ou às informações neles contidas, de graus de sigilo, conforme a legislação específica.

Continuidade de negócios: Capacidade de um órgão ou entidade de, quando ocorrer algum incidente de interrupção, manter suas operações em um nível aceitável, previamente definido, minimizando os impactos e recuperando perdas de ativos da informação das atividades críticas.

Custodiante: entidade detentora da posse, mesmo que transitória, de informação produzida ou recebida pela Universidade.

Engenharia social no contexto de SI: refere-se à manipulação psicológica de indivíduos para que executem ações que não deveriam ou, então, que divulguem informações confidenciais, sigilosas ou sensíveis

Incidente em segurança da informação: evento que tenha probabilidade de comprometer

as operações do negócio ou ameaçar a segurança da informação. Exemplos:

[1] *Phishing*: técnica usada para obter informações confidenciais, geralmente utilizando uma mensagem aparentemente real para enganar a vítima a digitar seus dados (*e.g.* nome de usuário, senha, detalhes do cartão de crédito) numa página falsa que imita a aparência, por exemplo, da página do banco ou da tela de acesso a algum sistema que o usuário costuma usar. Essa mensagem, alegando alguma justificativa enganosa, solicita que a vítima realize o "recadastramento" dos seus dados bancários, a alteração da sua senha eletrônica ou mesmo o cadastro para participar de um sorteio ou promoção (falsos).

[2] Pretexto (*pre-texting*): envolver a possível vítima a partir da criação de um cenário inventado (o pretexto) na tentativa de enganá-la a fornecer informações ou a realizar ações que, em circunstâncias normais, ela não forneceria/realizaria. Via de regra, o atacante fez pesquisas ou configurações prévias e, portanto, detém de antemão informações (*e.g.* data de nascimento, número do Seguro Social, valor da última conta) que lhe permitem, perante a vítima, conferir maior legitimidade ao cenário alegado. Assim, o atacante se passa por um colega de trabalho, um policial, um funcionário de banco/empresa/órgão do governo, ou seja, alguém que, pela vítima, seja percebido como uma autoridade e que, portanto, tenha direito legítimo a demandar a informação/ação em questão. Em alguns casos, o atacante só precisa de uma voz autoritária, de um tom sério e da habilidade de pensar rápido para dar respostas convincentes a eventuais perguntas da vítima.

[3] "Isca": o atacante infecta uma mídia física (*pendrive*, CD, DVD etc.) com um malware e a deixa em um local estratégico (*e.g.* estacionamento, banheiro, calçada, elevador) para ser encontrada pela vítima. Essa "isca", em geral, possui uma etiqueta atraente, com vistas a despertar a curiosidade ou a ganância da vítima (*e.g.* "Confidencial", "Salários dos Executivos Q2 2021"). Uma vez que a vítima conecte essa mídia a um computador, este *host* e as redes às quais ele estiver conectado são infectados com o malware, dando ao atacante acesso ao computador da vítima e, possivelmente, à rede interna da organização- alvo.

[4] Quiproquó (*quid pro quo*): significa, literalmente, "uma coisa por outra". Nesse tipo de ataque, o atacante promete à vítima um benefício em troca de informações ou ações. Enquanto na "isca" a vantagem vem na forma de um bem físico, no quiproquó o benefício assume a forma de um serviço. Por exemplo, um atacante ligando aleatoriamente para funcionários de uma empresa e dizendo que se trata de um retorno do setor de suporte técnico, eventualmente encontrará alguém com um problema legítimo. Assim, ao longo desse processo de "atendimento" para resolução do problema, o atacante instrui a vítima a realizar certas ações e/ou a digitar determinados comandos que instalarão um malware ou lhe darão acesso àquele computador.

[5] "Carona" (*tailgating*): uma das técnicas mais antigas de engenharia social, consiste na obtenção, por uma pessoa não autorizada, de acesso indevido a um ambiente restrito, simplesmente entrando atrás de uma pessoa que possui acesso legítimo. Por exemplo, um atacante mostrando as mãos ocupadas pode cumprimentar o funcionário legítimo e pedir-lhe que, por favor, segure a porta para ele. Se eventualmente questionado, o atacante pode mostrar bem rapidamente um cartão de acesso falso ou mesmo alegar que esqueceu ou que perdeu o próprio cartão.

Informação: Dados, processados ou não, que podem ser utilizados para produção e para

transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação arquivística: Toda e qualquer informação, independente do suporte, que é produzida, recebida e/ou acumulada no decorrer das atividades da FURG.

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.

Proprietário da informação: Unidade da FURG, ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação;

Termo de responsabilidade: Termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso e uso.

Usuários: Todas as pessoas naturais, a quem é destinada serviços e sistemas, incluindo estudantes, participantes de processo seletivo, egressos e visitantes que navegam na rede e utilizam os serviços da FURG.

## ANEXO II - DAS REFERÊNCIAS LEGAIS E NORMATIVAS
(RESOLUÇÃO CONSUN/FURG Nº 5, DE 20 DE MAIO DE 2022)

I. Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

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

III. Decreto nº 10.148, de 2 de dezembro de 2019, que Institui a Comissão de Coordenação do Sistema de Gestão de Documentos e Arquivos da administração pública federal, dispõe sobre a Comissão Permanente de Avaliação de Documentos e dá outras providências;

IV. Lei nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;

V. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

VI. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

VII. Decreto nº 8.539, de 8 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

VIII. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

IX. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

X. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal e dá outras providências;

XI. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

XII. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

XIII. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico

dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

XIV. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988.

XV. NBR ISO/IEC27001 de 11/2013, especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização

XVI. NBR ISO/IEC27002 de 11/2013, fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

XVII. NBR ISO/IEC27005 de 10/2019, fornece diretrizes para o processo de gestão de riscos de segurança da informação.

**ANEXO III – MODELO DE TERMO DE RESPONSABILIDADE E SIGILO**
(RESOLUÇÃO CONSUN/FURG Nº 5, DE 20 DE MAIO DE 2022)

Eu,_____, usuário (a) dos ativos de informação da Universidade Federal do Rio Grande, SIAPE/MATRICULA/CPF_____, declaro estar ciente do disposto na Política de Segurança da Informação da FURG – PSI, publicada eletronicamente em https://conselhos.furg.br, bem como nas normas e procedimentos complementares ali presentes, e comprometo-me a cumprir as suas determinações, bem como a manter-me periodicamente atualizado(a) a respeito de eventuais modificações que estes documentos possam sofrer.

Estou ciente que o descumprimento deste termo poderá acarretar medidas administrativas, bem como em responsabilização administrativa, civil e criminal, quando aplicável.

Declaro também ciência de que os meus dados pessoais serão registrados e operados com a finalidade de identificação do usuário no caso de violação de qualquer dos termos da PSI e/ou de suas normas complementares e legislações ou da ocorrência de incidente de segurança que esteja relacionado ao meu usuário e/ou ativos de informação da FURG sob os meus cuidados.