# RESOLUÇÃO N.º 008/2023 - CAD/UENP

Dispõe sobre a criação da Política de Segurança da Informação e Comunicação da Universidade Estadual do Norte do Paraná - UENP.

O Reitor da Universidade Estadual do Norte do Paraná – UENP, Prof. Dr. Fábio Antonio Néia Martini, nomeado pelo decreto nº 11.309, de 06 de junho de 2022, do Governo do Estado do Paraná, no uso de suas atribuições legais e regimentais, considerando o e-Protocolo 20.449.589-0; as recomendações do Tribunal de Contas do Estado do Paraná acerca da necessidade de estabelecer diretrizes para resposta a incidentes de Tecnologia da Informação, conforme Acórdão 963/2022; o Memorando n.º 22/2022 do Controle Interno que indica a adoção de medidas recomendadas pelo Acórdão 963/2022; o princípio da boa governança que consiste no gerenciamento de incidentes e na definição de mecanismos de controle interno necessários à prevenção de incidentes, assegurando a eficácia e contribuindo para a melhoria da segurança dos sistemas ligados a tecnologia da informação; a implantação e designação do Comitê de Segurança da Informação e Privacidade de Dados regulado pela Portaria n.º 241/2022; a implantação e designação do Comitê de Tecnologia da Informação regulado pela Portaria nº 224/2022; a necessidade de atualização da regulamentação e normatização da criação, exclusão, desativação e utilização do e-mail institucional no âmbito da Universidade Estadual do Norte do Paraná; que contas eletrônicas de e-mail são recursos intangíveis de trabalho institucional; o disposto na Lei Geral de Proteção de Dados Pessoais; e aprovação do Conselho de Administração - CAD, em reunião realizada no dia 04 de dezembro de 2023,

**RESOLVE**

**Art. 1.º** Instituir a Política de Segurança da Informação e Comunicação da Universidade Estadual do Norte do Paraná (UENP), na forma do Anexo I desta Resolução, que contém as Normas de Gestão de Incidentes, na forma do Anexo II, e a Normativa de e-mails, na forma do Anexo III.

Gabinete da Reitoria da UENP em
Jacarezinho, 06 de dezembro de 2023

FABIO ANTONIO NEIA MARTINI:70460841904

Assinado de forma digital por FABIO ANTONIO NEIA MARTINI:70460841904
Dados: 2023.12.07 10:37:32 -03'00'

**Prof. Dr. Fábio Antonio Néia Martini**
Reitor

# ANEXO I

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

## CAPÍTULO I

## DA FINALIDADE

**Art. 1°.** A Política de Segurança da Informação e Comunicação (POSIC) da Universidade Estadual do Norte do Paraná tem como objetivo a proteção das informações de sua propriedade e/ou sob sua guarda e é regida pelas Diretrizes apresentadas a seguir.

Parágrafo único. A Política de Segurança da Informação e Comunicação (POSIC) da Universidade Estadual do Norte do Paraná deve orientar a elaboração de Normas e Procedimentos específicos relacionados à segurança da informação e comunicação.

## CAPÍTULO II

## DOS TERMOS E DEFINIÇÕES

**Art. 2°.** Para os efeitos desta Política, são adotadas as seguintes definições:

I - **ativo de informação:** qualquer informação que tenha valor para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;

II - **recursos de processamento da informação:** qualquer sistema, serviço ou infraestrutura de processamento da informação, ou as instalações físicas que os abriguem;

III - **segurança da informação:** preservação da confidencialidade, da integridade, da disponibilidade, da autenticidade, da responsabilidade, do não repúdio e da confiabilidade da informação;

IV - **controle:** forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também é usado como sinônimo para proteção ou contra-medida;

V - **evento de segurança da informação:** todo fato que envolva um sistema, serviço ou rede e que exponha a risco, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação, nos termos da Norma ISO/IEC TR nº 18044:2004;

VI- **incidente de segurança da informação:** ocorrência indicada por um único evento ou por uma série de eventos indesejados ou inesperados que apresentem grande probabilidade de comprometer as operações e ameaçar a segurança da informação, nos termos da Norma ISO/IEC TR nº 18044:2004;

VII - **risco:** combinação da probabilidade de ocorrência de um evento e de suas possíveis consequências danosas;

VIII - **ameaça:** potencial causa de um incidente de segurança da informação que possa resultar em dano para um sistema ou para a Instituição, nos termos da Norma ISO/IEC nº 13335-1:2004;

IX - **vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

X - **contingência:** indisponibilidade ou perda de integridade da informação que os controles de segurança não tenham conseguido evitar;

XI - **plano de continuidade de operações:** conjunto de medidas, regras e procedimentos, pertinente à gestão das informações, a ser adotado quando a Instituição se deparar com problemas que comprometam o andamento normal dos processos, das funções ou das atividades críticas da Instituição, ISO/IEC nº 13335-1:2004;

XII - **princípios da Segurança da Informação e Comunicações**: princípios que regem a Segurança da Informação e Comunicações, ou seja, a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não-repúdio;

XIII - **termo de confidencialidade**: acordo de confidencialidade e não divulgação de informações que atribui responsabilidade ao servidor e ao administrador de serviço quanto ao sigilo e à correta utilização dos ativos de propriedade da Instituição ou por ela custodiados;

XIV - **quebra de segurança**: espécie de incidente de segurança da informação, ocasionada por ação ou omissão, intencional ou acidental;

XV - **tratamento da informação**: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive das sigilosas;

XVI - **continuidade de operações**: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de operações, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável e previamente definido;

XVII - **plano de Gerenciamento de Incidentes:** plano para ser utilizado quando ocorrer um incidente e que especifique pessoas, recursos, serviços e outras ações que forem necessárias para implementar o processo de gerenciamento de incidentes;

XVIII - **gestão da continuidade de operações:** processo contínuo de gestão e governança coordenado pelo Núcleo de Tecnologia da Informação, visando: a

continuidade de fornecimento dos serviços; identificação do impacto de perdas em potencial; e a manutenção de estratégias e de planos de recuperação;

XIX - **identificação de riscos:** conjunto de técnicas e procedimentos para identificar, localizar, enumerar e caracterizar os elementos do risco;

XX - **avaliação de riscos:** processo por intermédio do qual se compara o risco para classificar o seu grau de importância;

XXI - **gestão de Riscos de Segurança da Informação e Comunicação**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias, especificamente, para mitigar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXII - **tratamento dos riscos:** processo de implementação de ações de Segurança da Informação e Comunicações como forma de evitar, reduzir, reter ou transferir um risco;

XXIII - **gestor:** agente da Instituição responsável pela definição de critérios de acesso, classificação, tempo de vida e normas específicas de uso da informação;

XXIV - **usuário interno:** qualquer pessoa física ou unidade interna que faça uso de informações e que esteja vinculada administrativamente à Universidade Estadual do Norte do Paraná;

XXV - **usuário externo:** qualquer pessoa física ou jurídica que faça uso de informações e que não esteja vinculada administrativamente à Universidade Estadual do Norte do Paraná;

XXVI - **comunicação oficial:** tráfego de documentos, informações ou formulários emitidos por caixas postais eletrônicas da Universidade Estadual do Norte do Paraná de atividades especiais ou ainda de projetos específicos;

XXVII - **comunicação não oficial:** tráfego de documentos, informações ou formulários que não estejam incluídos no conceito de que trata o inciso anterior;

XXVIII - **comitê de Segurança da Informação e Privacidade de Dados:** Órgão da UENP cujas atribuições são avaliar, supervisionar, prestar orientações, desenvolver, propor e atender demandas relacionadas à Lei Geral de Proteção de Dados (LGPD);

XXIX - **comitê de Tecnologia da Informação:** Órgão da UENP cujas atribuições são promover, orientar, estabelecer, formular e atender demandas relacionadas ao acesso, utilização, manutenção e controle dos recursos computacionais no âmbito da Universidade;

XXX - **Conselho de Administração (CAD)**: Responsável pela definição de políticas administrativas, financeiras e de pessoal.

XXXI - **informação:** Dado ou Conjunto de Dados e conhecimento organizados que possam constituir referência sobre determinado acontecimento.

## CAPÍTULO III

## DOS PRINCÍPIOS

**Art. 3º.** Esta Política trata de aspectos básicos de Segurança da Informação e Comunicações, destacados a seguir:

I - **confidencialidade**: somente pessoas devidamente autorizadas pelo gestor da informação devem ter acesso a informação não pública;

II - **integridade**: somente operações de alteração, supressão e adição autorizadas pela Universidade Estadual do Norte do Paraná devem ser realizadas nas informações;

III - **disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou solicitado;

IV - **autenticidade**: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação;

V - **criticidade**: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

VI - **não-repúdio**: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo sua identificação;

VII - **responsabilidade**: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os servidores da Universidade Estadual do Norte do Paraná são responsáveis pelo tratamento da informação e pelo cumprimento das Normas de Segurança da Informação advindas desta Política;

VIII - **ciência**: todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IX - **ética**: todos os direitos e interesses legítimos de servidores, colaboradores, estagiários, prestadores de serviço e usuários do sistema de Informação da Universidade Estadual do Norte do Paraná devem ser respeitados;

X - **legalidade**: além de observar os interesses da Universidade Estadual do Norte do Paraná, as ações de Segurança da Informação e Comunicações levarão em consideração leis, normas, políticas organizacionais, administrativas, técnicas e operacionais, padrões, procedimentos aplicáveis e contratos com terceiros, dando atenção à propriedade da informação e aos direitos de uso; e

XI - **proporcionalidade:** o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações no âmbito da Universidade Estadual do Norte do Paraná serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

## CAPÍTULO IV

## DO ESCOPO

**Art. 4°.** O escopo do Plano de Segurança da Informação e Comunicação da Universidade Estadual do Norte do Paraná é composto por:

I - aspectos estratégicos, estruturais e organizacionais, que orientam a elaboração dos demais documentos que normatizam o tema;

II - requisitos de segurança humana;

III - requisitos de segurança física;

IV - requisitos de segurança lógica; e

V - sustentação dos procedimentos, dos processos de trabalho e dos ativos que influirão diretamente nos produtos e serviços oriundos da informação e comunicação da Universidade Estadual do Norte do Paraná.

## CAPÍTULO V

## DA ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

**Art. 5°.** A estrutura normativa da Segurança da Informação e Comunicação da Universidade Estadual do Norte do Paraná é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

I - **Política de Segurança da Informação e Comunicação (POSIC)**: constituída por este documento, que define a estrutura, as diretrizes e as obrigações referentes à Segurança da Informação, e que será detalhada em um conjunto de normas específicas.

II - **Normas de Segurança da Informação (Normas)**: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes desta Política, a serem observados em diversas instâncias em que a informação seja tratada. Cada norma será composta por um conjunto de procedimentos destinados a orientar sua implementação e quando definidas será acrescentada como anexo a este documento.

III - **Procedimentos de Segurança da Informação e Comunicações (Procedimentos)**: instrumentalizam o disposto nas Normas, permitindo sua direta aplicação nas atividades da Universidade Estadual do Norte do Paraná, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções serão de uso interno, não sendo obrigatória sua publicação.

## CAPÍTULO VI

## DAS DIRETRIZES GERAIS

**Art. 6°.** São diretrizes desta POSIC.

I – **Acesso à informação**: Todo serviço será regulamentado por normas específicas de tratamento da informação. Toda e qualquer informação acessada, gerada, adquirida, utilizada ou armazenada pela Universidade Estadual do Norte do Paraná é considerada seu patrimônio e deve ser protegida.

II – **Preservação da Finalidade Pública**: na condição de recursos da propriedade da Universidade Estadual do Norte do Paraná, estes serão fornecidos com o propósito único de garantir o desempenho das suas atividades.

III – **Tratamento de informações**: as normas para as operações de armazenamento, divulgação, reprodução, transporte, recuperação e destruição da

informação serão definidas de acordo com a classificação desta política, sem prejuízo de outros cuidados que vierem a ser especificados pelo gestor.

IV – **Gestão de incidentes**: será estabelecido um serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.

V – **Gestão de Riscos**: será estabelecido um processo de Gestão de Riscos, contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicação, de modo a produzir subsídios para a Gestão de Continuidade das Operações. Os riscos são monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco como ameaça, vulnerabilidade, probabilidade e impacto.

VI – **Auditoria e Conformidade**: deverão ser levantados regularmente os aspectos legais de segurança aos quais as atividades da Universidade Estadual do Norte do Paraná estão submetidas, de forma a evitar ações penais decorrentes da não observância de tais aspectos por desconhecimento ou omissão.

VII – **Segurança Física**: controles que monitorem o acesso físico a equipamentos, documentos, suprimentos e locais físicos da Universidade Estadual do Norte do Paraná e que garantam a proteção dos recursos, de forma que apenas as pessoas autorizadas tenham acesso, garantindo maior restrição à entrada e saída de visitantes, pessoal interno, equipamentos e mídias e estabelecer perímetros de segurança.

VIII – **Uso de e-mail**: o serviço de correio eletrônico disponibilizado pela Universidade Estadual do Norte do Paraná constitui recurso disponibilizado na rede de comunicação de dados para aumentar a agilidade, segurança e economia da comunicação oficial e informal.

IX - **Capacitação e Aperfeiçoamento**: os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação.

X - **Acesso à Internet**: todos os servidores têm o direito de acesso à internet, com utilização exclusiva para fins diretos e complementares às atividades do setor, para o enriquecimento intelectual de seus servidores ou como ferramenta para busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos. O acesso à Internet pelo corpo discente da Instituição deverá observar estritamente os objetivos acadêmicos constantes dos programas de cursos.

XI - **Patrimônio Intelectual**: as informações, os sistemas e os métodos criados pelos servidores da Universidade Estadual do Norte do Paraná, no exercício de suas funções, são patrimônios intelectuais da Instituição, não cabendo a seus criadores qualquer forma de direito autoral.

XII - **Termo de Responsabilidade e Sigilo**: é o documento oficial que compromete colaboradores, terceirizados e prestadores de serviço com a POSIC da Universidade Estadual do Norte do Paraná.

**Art. 7°.** Esta POSIC deve ser cumprida por todos que exerçam atividades no âmbito da Universidade Estadual do Norte do Paraná ou quem quer que tenha acesso a dados e informações no ambiente da Universidade.

Parágrafo único. Aquele que violar a presente Política de Segurança da Informação e Comunicação, violará o Programa de Compliance, podendo sofrer as sanções disciplinares previstas no Código de Conduta, sem prejuízo de eventuais sanções nas esferas administrativa, civil e criminal.

## CAPÍTULO IX

## DAS ATRIBUIÇÕES

**Art. 8º.** A implementação, o controle e a gestão da POSIC observará a seguinte estrutura de gerenciamento:

I - O Comitê de Segurança da Informação e Privacidade dos Dados tem como atribuições:

a) Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos.

b) Propor alterações nas versões da POSIC, assim como a inclusão, a eliminação ou a mudança de normas complementares.

c) Propor ações corretivas nos casos de incidentes de segurança.

d) Definir as medidas cabíveis nos casos de descumprimento da POSIC e/ou das Normas de Segurança da Informação complementares.

II – São atribuições do Comitê de Tecnologia da Informação:

a) Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

b) Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Universidade Estadual do Norte do Paraná.

c) Publicar e promover as versões da POSIC e suas normas aprovadas pelo Conselho de Administração.

d) Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Universidade Estadual do Norte do Paraná, mediante campanhas, palestras, treinamentos e outros meios de publicidade.

e) Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

f) Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação e Privacidade dos Dados.

g) Manter comunicação efetiva com o Comitê de Segurança da Informação e Privacidade dos Dados sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Universidade Estadual do Norte do Paraná.

h) Buscar alinhamento com as diretrizes corporativas da instituição.

i) Propor Normas adicionais e procedimentos relativos à Segurança da Informação no âmbito da Universidade Estadual do Norte do Paraná.

## CAPÍTULO X

## DA DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

**Art. 9°.** A Política e as Normas de Segurança da Informação e Comunicação devem ser divulgadas a todos os servidores da Universidade Estadual do Norte do Paraná e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

**Art. 10**. Os órgãos diretamente envolvidos na execução da POSIC são imediatamente responsáveis pela elaboração e proposição de normas, procedimentos e atividades necessárias ao seu cumprimento.

**Art. 11**. As áreas deverão submeter suas propostas de normas ao Comitê de Segurança da Informação e Privacidade dos Dados para análise, discussão, aprovação e posterior encaminhamento ao Conselho de Administração (CAD).

## CAPÍTULO XI

## DAS DISPOSIÇÕES FINAIS

**Art. 12**. Esta POSIC será revista e alterada sempre que as atribuições e as normas da Universidade Estadual do Norte do Paraná justificarem tais alterações.

**Art.13** Os casos omissos e as excepcionalidades deverão ser resolvidos pelo Conselho de Administração (CAD).

**Art. 14**. A presente política entra em vigor a partir da data de sua publicação.

# ANEXO II

# NORMA DE GESTÃO DE INCIDENTES (NGI-TI)
# DA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

## CAPÍTULO I

## SEÇÃO I

## DA FINALIDADE

**Art. 1.º** Esta norma tem por finalidade a definição de procedimentos de gestão de incidentes de TI na UENP.

## SEÇÃO II

## DAS DEFINIÇÕES

**Art. 2.º** Para os efeitos desta norma, consideram-se:

I - **Incidente**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, ou ainda, qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da UENP ou que tenha acesso;

II - **Processo**: é o conjunto de procedimentos, estruturados em um processo bem definido, à disposição da Equipe responsável pela Gestão, Tratamento e Resposta aos Incidentes;

III - **Tratamento de incidentes**: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

IV - **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados;

V - **Anonimização**: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

VI - **Ataque**: evento de exploração de vulnerabilidades. Ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

VII - **Dados pessoais sensíveis**: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;

VIII - **Dados pessoais**: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;

IX - **Expurgo de dados**: significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo controlador de qualquer forma;

X - **IP**: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede de dados;

XI - **Log**: processo de registro de eventos relevantes num sistema computacional;

XII - **Porta**: uma porta de conexão está sempre associada a um endereço IP de um *host* e ao tipo de protocolo de transporte utilizado para a comunicação.

Exemplo: o servidor de e-mail que executa um serviço de SMTP ele usa a porta 25 do protocolo TCP;

XIII - **Scripts**: conjunto de instruções para que uma função seja executada em determinado aplicativo;

XIV - **Sistemas**: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela UENP para dar suporte na execução de suas atividades;

XV - **Spam**: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas, e podem ser carregados de itens maliciosos;

XVI - **Spyware**: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

XVII - **Tratamento**: qualquer operação ou conjunto de operações efetuado sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

XVIII - **Trojan**: programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário, utilizado principalmente de forma maliciosa para apropriação de dados;

XIX - **Vazamento de dados**: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

XX - **Violação de privacidade**: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

XXI - **Vírus**: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

XXII - **Worm**: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

XXIII - **Autoridade Nacional de Proteção de Dados (ANPD)**: é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados (LGPD) em todo o território brasileiro;

XXIV - **Encarregado pelo tratamento de dados pessoais e privacidade dos dados**: responsável por assegurar o cumprimento da legislação local aplicável, além de atuar como contato para os titulares dos dados e para a ANPD;

XXV - **Notificador**: pessoa ou sistema de monitoração que notifica o incidente;

XXVI - **Acionadores**: servidores lotados nas Unidades de TI, responsáveis pela gestão das Ordens de Serviço;

XXVII - **Comitê de Tecnologia da Informação (CTI)**: Órgão da UENP cujas atribuições são promover, orientar, estabelecer, formular e atender demandas relacionadas ao acesso, utilização, manutenção e controle dos recursos computacionais no âmbito da Universidade;

XXVIII - **Responsável por sistema**: é um servidor especialmente designado para propor soluções de resposta a um determinado incidente em um sistema;

XXIX - **Assessor(a) Especial de TI do Gabinete**: responsável por avaliar se há dano ou risco relevante ao titular de dados pessoais;

XXX - **Assessoria de Comunicação**: responsável por encaminhar comunicações formais de incidentes envolvendo dados pessoais;

XXXI - **Aviso de Incidente**: formulário de Identificação do Incidente, anexado a esta Norma, a ter início com o notificador;

XXXXII - **Unidade de TI**: Setor de TI da Reitoria ou dos *Campi*;

XXXIII - **Gestor de unidade de TI**: dirigente de unidade de tecnologia da informação.

## SEÇÃO III

## AUTORIDADES, PAPÉIS E RESPONSABILIDADES

**Art. 3.º** A gestão de incidentes de TI será realizada pelos seguintes órgãos:

I - Unidades de TI;

II - Comitê de Tecnologia da Informação (CTI);

III - Assessoria Especial do Gabinete.

**Art. 4.º** As Unidades de TI têm como papel:

a) Receber notificações;

b) Avaliar notificações;

c) Executar medidas de contenção;

d) Conduzir e documentar as respostas relacionadas a incidentes envolvendo sistemas e recursos computacionais;

e) Manter o registro e a documentação proveniente de processos de incidente;

f) Encaminhar para ciência do controle interno e do gestor, após conclusão, os processos de incidente finalizados;

g) Apresentar ao controle interno e ao gestor, anualmente, relatório contendo todos os processos de incidentes abertos na UENP;

h) Solicitar à alta gestão autorização para contratação de apoio externo quando não dispuser de recursos suficientes para contenção ou recuperação de incidente.

**Art. 5.º** O Comitê de Tecnologia da Informação (CTI) tem como papel:

a) Propor soluções de resposta quando incidentes necessitarem de melhor avaliação;

b) Propor normas para aperfeiçoar a gestão de incidentes.

**Art. 6.º** A Assessoria Especial do Gabinete tem como papel:

a) Auxiliar a alta gestão quando houver solicitação de autorização para contratação de apoio externo quando as Assessorias de TI não dispuserem de recursos suficientes para contenção ou recuperação de incidente;

b) Dar parecer, mediante solicitação do gestor da UENP ou de gestor de unidade de TI, em processos de incidentes;

c) Acompanhar, supervisionando o NTI e demais unidades de TI, os processos de incidentes.

## SEÇÃO IV

## DA AVALIAÇÃO, MEDIDAS DE CONTENÇÃO E RECUPERAÇÃO DE INCIDENTES

**Art. 7.º** Quando um ou mais incidentes forem notificados por qualquer fonte devem ser cadastrados, pelo Acionador, no sistema da Unidade de TI para avaliação preliminar.

**Art. 8.º** Após o cadastramento, o Acionador deve fazer a avaliação preliminar ou contatar imediatamente a equipe de TI em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

**Art. 9.º** Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar com indicação de qual é a resposta imediata ideal.

**Art. 10.** Conforme a avaliação preliminar, incidentes que não envolvam sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata devem ser encaminhados para trâmites regulares do Comitê de Segurança da Informação e Privacidade de Dados.

Parágrafo único. Caso o incidente envolva dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais e Privacidade dos Dados deverá ser acionado.

**Art. 11.** Se a avaliação preliminar indicar que o incidente exige melhor avaliação, o responsável pelo sistema acionará o Comitê de Tecnologia da Informação (CTI) e proporá soluções.

Parágrafo único. O Comitê deverá fazer a avaliação e deliberar acerca do incidente e das proposições do responsável pelo sistema no prazo de 30 dias.

**Art. 12.** Após avaliação preliminar, o responsável pelo sistema e os acionadores passarão a realizar os seguintes processos:

I - Avaliação mais detalhada do incidente;

II - Classificação conforme grau de criticidade.

**Art. 13.** Os incidentes serão categorizados da seguinte forma:

I - Conteúdo abusivo: *spam*, assédio, etc;

II - Código malicioso: *worm*, vírus, *trojan, spyware, scripts*;

III - Prospecção por informações: varredura, *sniffing*, engenharia social;

IV - Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;

V - Intrusão: acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação;

VI - Indisponibilidade de serviço ou informação: negação de serviço, sabotagem;

VII - Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;

VIII - Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;

XIX - Outros: incidente não categorizado.

**Art. 14.** Em caso de ocorrência simultânea ou concomitante, o gestor de unidade de TI definirá a ordem de atendimento de acordo com a urgência de tratamento e o impacto nas áreas de negócio da UENP.

Parágrafo único. O grau de criticidade do incidente deve ser definido de acordo com a sistemática definida no art. 15.

**Art. 15.** Os graus de criticidade de tratamento de incidentes são os seguintes:

I - Alto (Impacto Grave): Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;

II - Médio (Impacto Significativo): Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;

III - Baixo (Impacto Mínimo): Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

**Art. 16.** A unidade de TI responsável deverá praticar todos os atos necessários para identificar a causa do incidente, os endereços IP e credenciais envolvidas, as transações e transferências de dados irregulares, os métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases.

§ 1º. Em caso de incidentes envolvendo sistemas de terceiros, especialistas do referido sistema poderão ser acionados pelo gestor de unidade de TI da Reitoria (NTI), com ciência do Assessor de TI do Gabinete.

§ 2º. Em caso de incidentes envolvendo sistemas próprios, os especialistas do referido sistema serão acionados pelo gestor de unidade de TI.

§ 3º. Caso as soluções impactadas tenham responsáveis identificados no inventário de soluções, estes devem ser acionados pelo gestor de unidade de TI, para que se manifestem sobre os procedimentos de contenção e erradicação, colaborando nas estratégias de atuação.

§ 4º. No caso da necessidade de implementação de medidas de contenção e erradicação para evitar mais danos, o gestor da unidade de TI deve realizar o desligamento dos sistemas inteiros ou de funcionalidades específicas, além de promover exposição de indisponibilidade para manutenção sempre que possível, tomando cuidados para não impactar evidências que poderiam ser usadas para identificar a autoria, a origem e método usado para quebrar a segurança.

§ 5º. Em caso de incidente envolvendo máquinas virtuais, deve ser feito o registro do estado (*snapshot*) em que se encontram os sistemas, aplicações ou arquivos afetados para posterior análise.

§ 6º. A unidade de TI responsável deverá proceder com a recuperação e tomar as medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais e instalação de sistemas.

§ 7º. O processo de incidente deverá conter: linha do tempo, atores, evidências, conclusões, decisões, autorizações, tomadas de ação e demais procedimentos, bem como a natureza dos dados afetados, se for o caso.

§ 8º. A unidade de TI deverá documentar o incidente em base de conhecimentos apropriada para futuras consultas.

**Art. 17.** Os responsáveis pela unidade de TI nos *campi* deverão encaminhar aos respectivos Diretores, via sistema e-protocolo, seus processos de incidentes, para ciência.

Parágrafo único. O prazo para o encaminhamento será de 10 dias úteis.

**Art. 18.** O responsável pela unidade de TI da Reitoria deverá encaminhar para ciência do controle interno e do gestor, após conclusão, os processos de incidente finalizados.

Parágrafo único. O prazo para o encaminhamento será de 10 dias úteis.

**Art. 19.** Os responsáveis pela unidade de TI nos *campi* deverão encaminhar, ao Núcleo de Tecnologia da Informação, relatório anual de todos os incidentes ocorridos no período.

Parágrafo único. Os relatórios anuais deverão ser encaminhados até o último dia útil do mês de janeiro subsequente.

**Art. 20.** O responsável pelo Núcleo de Tecnologia da Informação deverá encaminhar relatório anual de todos os incidentes ocorridos no período, ao departamento de Controle Interno e ao Reitor.

Parágrafo único. Os relatórios anuais deverão ser encaminhados até o último dia útil do mês de fevereiro subsequente.

## SEÇÃO V

## NATUREZA DOS DADOS PESSOAIS AFETADOS E INFORMAÇÕES SOBRE OS TITULARES DE DADOS PESSOAIS ENVOLVIDOS

**Art. 21.** No caso de incidente envolvendo dados pessoais, a situação deverá ser encaminhada para análise do Encarregado pelo Tratamento de Dados Pessoais e Privacidade dos Dados e da Assessoria Especial de TI do Gabinete da UENP para avaliação de relevância de risco e dano.

**Art. 22.** Caso o Encarregado pelo Tratamento de Dados Pessoais e Privacidade dos Dados e a Assessoria Especial do TI do Gabinete da UENP concluam que o incidente acarretou risco ou dano relevante aos titulares de dados, deverá o Encarregado pelo Tratamento de Dados Pessoais e Privacidade dos Dados e a Assessoria de Comunicação Social fazer as comunicações obrigatórias por Lei.

## SEÇÃO VI

## DISPOSIÇÕES FINAIS

**Art. 23.** O Comitê de Tecnologia da Informação, além de propor melhorias para os sistemas e processos, deve avaliar a eficácia dos procedimentos realizados sobre os incidentes de segurança de informação.

**Art. 24.** Esta normativa entra em vigor na data de sua publicação.

**Art. 25.** Os casos omissos e as excepcionalidades deverão ser resolvidos pelo Conselho de Administração (CAD).

**FORMULÁRIO DE IDENTIFICAÇÃO DE INCIDENTE**

UNIDADE (REITORIA, CCP, CJ OU CLM): _____

DATA DA NOTIFICAÇÃO: _____

NOTIFICADOR: _____

DESCRIÇÃO DO INCIDENTE:

| |
|---|
| |

A ser preenchido pela Unidade de TI

---

ACIONADOR: _____

RESPONSÁVEL PELO SISTEMA: _____

GESTOR DA UNIDADE DE TI: _____

CATEGORIA DO INCIDENTE (ART 13º): _____

GRAU DE CRITICIDADE DO INCIDENTE: (ART 15º):

**(  ) ALTO  (  ) MÉDIO  (  ) BAIXO**

DATA DA CONCLUSÃO: _____

# ANEXO I

# NORMATIZAÇÃO DO USO DO CORREIO ELETRÔNICO

## CAPÍTULO I

## SEÇÃO I

## DOS OBJETIVOS

**Art. 1.º** A presente normatização tem por objetivo definir política de criação, exclusão, desativação e utilização do correio eletrônico institucional na Universidade Estadual do Norte do Paraná, estabelecendo as diretrizes básicas a serem seguidas pelos usuários e administradores dessa ferramenta, com o intuito de garantir sua utilização exclusivamente para fins institucionais.

## SEÇÃO II

## DAS DEFINIÇÕES

**Art. 2.º** Para os fins desta Normativa, aplicam-se os seguintes conceitos:

I - **administrador**: responsável junto ao Núcleo de Tecnologia e Processamento da Informação (NTI) pela gestão do serviço de e-mail institucional nos *campi* e na Reitoria;

II - **e-mail institucional**: serviço de correio eletrônico de domínio da Universidade;

III - **conta de e-mail institucional**: é composta por uma caixa de e-mail, com seu respectivo usuário e senha para acesso ao e-mail institucional;

IV - **usuário individual**: toda pessoa que possui um e-mail institucional e o utiliza no desenvolvimento de suas atividades de trabalho ou estudo;

V - **usuário setorial**: caixa postal vinculada a setores como seções, divisões, direções, órgãos de apoio e assessoramento, Pró-Reitorias, coordenações dos *campi* e Reitoria ou, ainda, algum projeto ou ação institucional;

VI - ***login***: processo de identificação e autenticação de usuários em programas computacionais e serviços de e-mail;

VII - **grupo de e-mail institucional**: associação de diversas contas de e-mail a um determinado endereço;

VIII - ***spam***: Termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

IX - **Unidade de Tecnologia da Informação**: Núcleo de Tecnologia da Informação ou setores de TI dos *campi,* responsáveis pelo gerenciamento de serviços, como: gestão dos recursos, configurações de itens para entrega dos serviços e garantia de acesso aos recursos pelos usuários etc.

## SEÇÃO III

## DO FORNECIMENTO E MANUTENÇÃO DAS CONTAS DE E-MAIL

**Art. 3.º** A criação de contas de e-mail institucional e de grupos de e-mail institucional deverão seguir as regras estabelecidas neste artigo:

§1º. Será fornecida uma única conta de e-mail institucional para usuário individual, destinadas a:

I - servidores públicos com vínculo ativo com a UENP;

II - estudantes matriculados.

§2º. Serão fornecidas contas de e-mail institucional para usuário setorial, destinadas a:

I - setores, coordenações de setor, coordenações de curso, núcleos, direções e presidências (ou equivalente) de comissões, estagiários, bolsistas, residentes técnicos com a aprovação das chefias imediatas;

II - eventos, projetos e programas institucionais durante o período de sua vigência. A conta estará associada à conta do usuário solicitante e sua criação estará sujeita a anuência do responsável pelo evento, projeto ou programa.

§3º. Haverá um grupo de e-mail denominado “TODOS” contendo as contas dos e-mails institucionais mencionados no §1º deste artigo;

§4º Haverá um grupo de e-mail denominado "DOCENTES" contendo as contas dos e-mais institucionais dos docentes efetivos e temporários;

§5º Haverá um grupo de e-mail denominado “AGENTES” contendo as contas dos e-mails institucionais dos agentes universitários efetivos e temporários;

§6º Outros grupos de e-mails institucionais poderão ser criados, desde que para atender finalidade institucional;

§7º Na criação de contas de e-mail institucional para estudantes, deverá ser utilizado o subdomínio @discente.uenp.edu.br.

**Art. 4.º** O nome utilizado para a conta do e-mail institucional deverá atender aos seguintes critérios:

I - o endereço de e-mail do usuário individual será criado na forma "prenome.sobrenome" ou “sobrenome.prenome”. Em casos de repetição, será acrescida numeração sequencial;

II - quando o usuário utilizar nome social, este será considerado para a criação do endereço de e-mail, na forma estabelecida no item I;

III - contas de usuário setorial serão formadas pelo nome do setor.

a) Para Reitoria: sigla ou nome do setor.

b) Para *Campus*: sigla ou nome do setor acompanhado de pontuação e sigla do *campus*.

c) Para Centros de Estudos: sigla ou nome do setor acompanhado de pontuação, mais sigla do centro acompanhado de pontuação, mais a sigla do campus.

§1º. O nome de usuário setorial das contas de e-mail criadas para comissões ou outros grupos de trabalho deverão ter como nome de usuário o nome da comissão ou do grupo de trabalho.

§2º. Havendo coincidência de nome de comissões ou grupos de trabalho, a unidade de TI definirá numeração sequencial para complemento e diferenciação;

§3º. Não serão criadas contas de e-mail cujo nome de usuário esteja fora do padrão proposto neste artigo.

## SEÇÃO V

## DA CRIAÇÃO, DESATIVAÇÃO E EXCLUSÃO DAS CONTAS DO CORREIO ELETRÔNICO

**Art. 5.º** Para a criação de contas de usuário individual, os interessados deverão estar devidamente cadastrados no sistema institucional.

§1º. A solicitação para criação do e-mail institucional deverá ser feita pelo próprio interessado via formulário eletrônico disponível no sítio do NTI.

§2º. O usuário deverá ler e aceitar, de forma eletrônica, as normas disponíveis nesta Normativa.

§3º. Encerrado o vínculo com o sistema institucional, o e-mail é desativado e, após um ano, será excluído definitivamente.

**Art. 6.º** O Setor de Tecnologia da Informação dos *Campi* ou da Reitoria é o responsável pela manutenção das contas de e-mail institucional e executará ato de criação, desativação ou exclusão de contas de e-mail institucional mediante solicitação de setores competentes.

**Art. 7.º** O Núcleo de Tecnologia da Informação é o órgão competente para criar, desativar ou excluir contas de e-mail institucional.

**Art. 8.º** No caso dos usuários indicados nos incisos I a IV, do artigo 3º, quando houver interrupção do vínculo institucional, o órgão competente deverá comunicar ao usuário o encerramento do e-mail institucional bem como os prazos dispostos na presente Resolução.

Parágrafo único. As contas de e-mail dos servidores aposentados serão excluídas no prazo de um ano. Contudo, havendo interesse na manutenção por questões de histórico acadêmico, deverá encaminhar solicitação à Pró-Reitoria de Recursos Humanos para manutenção ou redirecionamento dos dados para um e-mail particular de sua escolha.

**Art. 9.º** O prazo para exclusão das contas, a partir da perda do vínculo institucional, será de 90 dias.

**Art. 10.** Serão criados grupos de e-mail somente pelos administradores de contas do *campus* ou reitoria mediante solicitação oficial via e-protocolo.

Parágrafo único. Na criação do grupo de e-mail institucional será definido um administrador do grupo, que será responsável pelo gerenciamento, adição ou exclusão de participantes.

## SEÇÃO VI

## DAS CONDIÇÕES GERAIS DE UTILIZAÇÃO

**Art. 11.** São condições gerais de utilização do e-mail institucional:

I - veiculação de mensagens de conteúdo exclusivamente acadêmico ou administrativo, não sendo permitido o uso para fins comerciais, político-partidários, religiosos ou que não sejam consonantes com o uso institucional;

II - adoção de assinatura padrão que identifique o usuário, sua função e seu local de trabalho. As imagens utilizadas na personalização devem restringir-se às logomarcas institucionais;

III - é vedada a cessão, a qualquer título, da lista de endereços dos usuários do e-mail institucional a pessoas não pertencentes ao quadro de servidores da Universidade;

IV- os usuários individuais devem manter como imagem de perfil atrelada à sua conta de e-mail foto que permita sua identificação funcional ou utilizar a opção pré-configurada do e-mail.

**Art. 12.** Toda e qualquer utilização estranha às funções institucionais e funcionais será considerada uso indevido do e-mail institucional.

**Art. 13.** Constatado o uso indevido do e-mail institucional, serão adotados os procedimentos legais previstos na legislação e normativas vigentes.

## SEÇÃO VII

## DOS DEVERES E RESPONSABILIDADES

**Art. 14.** São deveres do usuário individual ou setorial:

I - manter em sigilo sua senha de acesso;

II - realizar a substituição de sua senha em caso de suspeita de violação;

III - fechar a página de acesso utilizando o botão “SAIR” do e-mail institucional sempre que se ausentar;

IV - comunicar imediatamente ao administrador de contas de e-mail o recebimento de mensagens com vírus, spam ou qualquer outro tipo de conteúdo inadequado;

V - efetuar a manutenção de sua Caixa Postal, evitando ultrapassar o limite de armazenamento;

VI - notificar o administrador de contas de e-mail quando ocorrerem alterações que venham a afetar o cadastro do usuário de e-mail.

**Art. 15.** São deveres do administrador das contas de e-mail:

I - disponibilizar a utilização do e-mail institucional conforme disposto nesta Normativa;

II - informar previamente aos servidores sobre interrupções dos serviços;

III - viabilizar a recuperação do acesso ao e-mail institucional;

IV - gerar e manter grupos de e-mail mediante solicitação formal;

V - administrar, propor e executar políticas, procedimentos e melhores práticas relativas aos serviços de e-mail institucional, zelando pelo cumprimento de leis e normas aplicáveis;

VI - verificar periodicamente o desempenho, a disponibilidade e a integridade do sistema de e-mail institucional;

VII – observar o disposto na Lei Geral de Proteção de Dados Pessoais (nº 13.709/2018).

## SEÇÃO VIII

## DISPOSIÇÕES FINAIS

**Art. 16.** Esta Resolução entra em vigor na data de sua publicação.

**Art. 17.** Os casos omissos e as excepcionalidades deverão ser resolvidos pelo Conselho de Administração (CAD).