MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA
CAMPUS MINISTRO REIS VELLOSO

RESOLUÇÃO CONSUNI N° 171 DE 16 DE JULHO DE 2025

Aprova a Política de Tratamento de Incidentes de Segurança da Informação no âmbito da Universidade Federal do Delta do Parnaíba (UFDPar).

O REITOR DA UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA e PRESIDENTE DO CONSELHO UNIVERSITÁRIO (CONSUNI), no uso de suas atribuições legais, tendo em vista decisão do mesmo Conselho em reunião realizada no dia 11/06/2025, e considerando:

- a Lei Geral de Proteção de Dados (LGPD) - Lei n° 13.709, de 14 de agosto de 2018;

- a Resolução CONSUNI n° 63, de 1° de março de 2024, referente à Política de Segurança da Informação e Comunicação no âmbito da UFDPar;

- a Resolução CONSUNI n° 100, de 14 de outubro de 2024, referente à Política de Proteção de Dados Pessoais e cria o Comitê Gestor de Proteção de Dados Pessoais, no âmbito da UFDPar;

- a Associação Brasileira de Normas Técnicas: ABNT NBR ISO/IEC 27701:2019: técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes. Rio de Janeiro, 2019;

- a Associação Brasileira de Normas Técnicas: ABNT NBR ISO/IEC 27001:2022: segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2022;

- a Associação Brasileira de Normas Técnicas: ABNT NBR ISO/IEC 27002:2022: segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação - Requisitos. Rio de Janeiro, 2023. BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei n° 13.709, de 14 de agosto de 2018;

- o Decreto n° 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI);

- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria n° 93, de 26 de setembro de 2019. Glossário de Segurança da Informação;

- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. Instrução Normativa n° 01, de 27 de maio de 2020. Brasília - DF, GSI/PR, 2020;

- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. Instrução Normativa n° 03, de 28 de maio de 2021;

- Modelo de Política de Segurança da Informação. Programa de Privacidade e Segurança da Informação (PPSI). Brasília, DF, MGI, agosto de 2024;

- Guia do Framework de Privacidade e Segurança da Informação da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital (DPSI/SGD), de março 2024;

- Autoridade Nacional de Proteção de Dados (ANPD). Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023;

- Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR n° 93, de 18 de outubro de 2021;

- o Processo n° 23855.010686/2024-55;

RESOLVE:

Art. 1° Aprovar, no âmbito da Universidade Federal do Delta do Parnaíba (UFDPar), a Política de Tratamento de Incidentes de Segurança da Informação.

Art. 2° Esta Resolução entra em vigor na data de sua publicação.

ICP Brasil
Documento assinado digitalmente
JOAO PAULO SALES MACEDO
Data: 16/07/2025 17:34:34-0300
Verifique em https://validar.iti.gov.br

João Paulo Sales Macedo

Reitor

ANEXO I DA RESOLUÇÃO CONSUNI N° 171 DE 16 DE JULHO DE 2025

POLÍTICA DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA (UFDPar)

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1° A Política de Tratamento de Incidentes de Segurança da Informação, aplica-se a todas as unidades organizacionais da UFDPar, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração.

Parágrafo único. Os incidentes de segurança da informação devem ser tratados de forma adequada, eficaz e de uma maneira que minimize o impacto adverso à UFDPar.

Art. 2° O Tratamento de Incidentes de Segurança da Informação abrange os recursos de sistema da informação, pertencentes, operados, mantidos e controlados pela UFDPar.

Art. 3° No caso de um incidente ou violação de segurança da informação real (ou suspeita), a UFDPar tomará medidas imediatas para mitigar os riscos de danos potenciais a indivíduos, aos negócios operacionais e custos financeiros, legais e de reputação.

Parágrafo único. Quando os incidentes de segurança da informação não são relatados, ou quando os relatórios são atrasados, as consequências podem ser graves e incluem:

I - danos ou interrupções em sistemas corporativos;

II - danos e sofrimento a pessoas;

III - penalidades monetárias de reguladores (incluindo multas significativas por violações de proteção de dados);

IV - danos à reputação da UFDPar;

V - perda de ativos;

VI - aumento do risco de fraude ou roubo de identidade.

Art. 4° Esta Política será revisada periodicamente visando adequá-la às inovações tecnológicas, mudanças legislativas e evolução das ameaças à segurança da informação, incluindo, mas não se limitando, a riscos relacionados à inteligência artificial, computação quântica, segurança em *internet* das coisas e cadeia de suprimentos de *software*.

CAPÍTULO II

DO OBJETIVO

Art. 5° A Política de Tratamento de Incidentes de Segurança da Informação tem o objetivo de garantir uma abordagem consistente e eficaz para o gerenciamento, incluindo a identificação e comunicação de Eventos de Incidentes de Segurança, conforme listado a seguir:

I - estabelecer diretrizes para o gerenciamento de resposta a incidentes de segurança da informação;

II - determinar como e por que o incidente ocorreu, identificando vulnerabilidades para evitar futuras ocorrências semelhantes;

III - documentar e formalizar os procedimentos de tratamento de incidentes da informação na UFDPar;

IV - garantir a segurança dos recursos do sistema de informação da UFDPar, em caso de incidentes;

V - garantir que as partes interessadas internas e externas sejam informadas apropriadamente, e que as informações sobre o incidente sejam compartilhadas de forma clara e oportuna para evitar alarmes desnecessários ou mal-entendidos;

VI - minimizar o possível impacto do incidente de segurança da informação em termos de vazamento de informações, corrupção e interrupção de serviços;

VII - permitir que a equipe de segurança reaja rapidamente a incidentes, a fim de controlar os possíveis danos e reduzir o tempo de resposta;

VIII - preservar informações para investigação;

IX - prevenir ataques e danos futuros;

X - promover a gestão efetiva e eficaz da segurança da informação na UFDPar;

XI - prover respostas estruturadas e eficazes de modo que os serviços comprometidos sejam restaurados no menor tempo possível;

XII - registrar todas as particularidades do incidente para análise e usar essas informações para que o time de tratamento e prevenção de acidentes realize os tratamentos para testes e prevenção em outros sistemas da UFDPar, aprimorando a estratégia de segurança e consolidar os procedimentos de resposta a incidentes;

XIII - disponibilizar os recursos necessários para lidar com os incidentes, incluindo pessoas, tecnologia, entre outros.

CAPÍTULO III

DO ESCOPO

Art. 6° Esta Política de Tratamento de Incidentes de Segurança da Informação se aplica a:

I - todas as informações criadas ou recebidas pela UFDPar em qualquer formato, sejam mantidas no *campus* ou remotamente, armazenadas em dispositivos de mesa ou estáticos, ou dispositivos e mídia portáteis, sejam transportadas do local de trabalho física e eletronicamente, ou acessadas remotamente;

II - qualquer incidente que possa ter um efeito prejudicial em quaisquer ativos ou sistemas de informações da UFDPar;

III - todos os usuários de informações e sistemas da UFDPar, incluindo servidores, discentes, funcionários terceirizados e visitantes que trabalham em nome da UFDPar;

IV - todos os sistemas de Tecnologia da Informação (TI) de propriedade e gerenciados pela UFDPar;

V - quaisquer sistemas de TI, em que as informações da UFDPar são mantidas ou processadas, incluindo dispositivos de propriedade pessoal.

CAPÍTULO IV

DAS DEFINIÇÕES

Art. 7° Para os fins dispostos nesta Política, consideram-se as seguintes definições:

I - ameaça: conjunto de fatores com o potencial de causarem dano para um sistema ou organização;

II - análise de incidentes: traduz-se em averiguar os elementos disponíveis sobre o incidente, que inclui artefatos e outros indícios associados ao incidente, ou seja, identificar o escopo, sua dimensão, sua natureza e os prejuízos provocados;

III - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que ele tem acesso e conhecimento ou dado que tem valor para o usuário ou à UFDPar;

IV - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa, sistema, órgão ou entidade;

V - classificação da informação: processo que compreende a identificação e definição de níveis e critérios de proteção para as informações, para garantir sua confidencialidade, integridade e disponibilidade;

VI - confidencialidade: propriedade que garante que a informação não seja acessada, divulgada ou disponibilizada a pessoas, sistemas ou entidades não autorizados. Assegura que a informação sensível não esteja disponível ou revelada às pessoas, sistema, órgão ou entidade não autorizados;

VII - contenção: ações para evitar que mais danos ocorram;

VIII - contenção de curto prazo: ações para cortar o ataque ou dano;

IX - contenção de longo prazo: ações adotadas para mitigar temporariamente um problema de segurança da informação, garantindo a continuidade das operações enquanto se desenvolve e implementa uma solução definitiva;

X - dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável;

XI - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XII - encarregado pelo tratamento de dados pessoais (ETDP): pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XIII - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;

XIV - incidente de segurança da informação: qualquer evento que represente uma ameaça potencial, suspeita ou real à segurança, confidencialidade, integridade ou disponibilidade das informações;

XV - incidente de baixo impacto: incidentes isolados por natureza e podem não ter o potencial de afetar um número significativo de usuários. Por exemplo, infecção por vírus em um dispositivo de usuário final, suspeita ou entrada não autorizada ocorrida nas instalações etc.;

XVI - incidente de impacto médio: incidentes que têm um impacto significativo ou têm o potencial de escalar para um incidente monumental/catastrófico. Por exemplo, uma tentativa de *hacking* em andamento, infecção por vírus detectada em alguns sistemas em rede, dentre outros;

XVII - incidente de alto impacto: incidentes que têm um impacto monumental/catastrófico nos negócios ou serviços. Por exemplo, ataque de *ransomware*, ataque DDoS, comprometimento de privilégios administrativos de aplicativos de negócios principais, dentre outros;

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

XIX - integridade: propriedade pela qual se garante que a informação não foi alterada ou destruída de forma não autorizada, ou acidental;

XX - medida técnica: controle relacionado à segurança cibernética, obtido por técnica que possibilite confidencialidade, disponibilidade e integridade dos dados e conformidade legal e normativa;

XXI - plano de continuidade do negócio: fornece meios para asseverar que os serviços indispensáveis sejam identificados, para garantir a manutenção após a ocorrência de um desastre e até o retorno da situação normal de funcionamento;

XXII - recuperação e restauração: assegurar que todos os sistemas e dados afetados sejam restaurados ao estado operacional, minimizando a perda de dados e garantindo a continuidade das operações;

XXIII - remediação: conjunto de ações tomadas pela equipe de tratamento de incidentes para mitigar os impactos e restaurar a normalidade após a ocorrência de um incidente de segurança da informação;

XXIV - resposta a incidentes: processo estruturado para detectar, analisar, conter, erradicar, recuperar e aprender com incidentes de segurança da informação, minimizando impactos e protegendo ativos críticos da organização;

XXV - risco: possibilidade de ocorrência de um evento que pode comprometer a confidencialidade, integridade e disponibilidade da informação, causando impactos negativos para a organização;

XXVI - riscos cibernéticos: riscos de ataques cibernéticos, internos ou externos, com origem de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDos e *Botnets*), sabotagem, bem como violação de acessos e privacidade, que podem desproteger dados, redes e sistemas;

XXVII - segurança da informação: conjunto de práticas, políticas e controles destinados a proteger a confidencialidade, integridade e disponibilidade das informações, prevenindo acessos não autorizados, modificações indevidas, destruição ou interrupção dos serviços, sejam esses dados armazenados, em trânsito ou em processamento. Ela também abrange aspectos físicos, organizacionais e tecnológicos, incluindo a proteção de pessoas, infraestrutura e sistemas computacionais;

XXVIII - titular do dado: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

XXIX - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): conforme Resolução CONSUNI n° 63, de 1° de março de 2024, que aprovou a Política de Segurança da Informação e Comunicação no âmbito da Universidade Federal do Delta do Parnaíba;

XXX - Time de Resposta a Incidentes de Segurança da UFDPar (TRISE): conforme Resolução CONSUNI n° 100, de 14 de outubro de 2024, referente à Política de

Proteção de Dados Pessoais e cria o Comitê Gestor de Proteção de Dados Pessoais da Universidade Federal do Delta do Parnaíba;

XXXI - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov): corresponde ao *Computer Security Incident Response Team* (CSIRT) nacional;

XXXII - Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP);

XXXIII - Divisão de *Datacenter* e Segurança da Informação (DDSI);

XXXIV - Diretoria de Sistemas e Infraestrutura de TIC (DSTIC); e

XXXV - violação de segurança: qualquer incidente que resulta em acesso não autorizado a dados, aplicativos, serviços, redes e/ou dispositivos ao ignorar seus mecanismos de segurança subjacentes.

CAPÍTULO V

DOS PRINCÍPIOS E DIRETRIZES

Art. 8° As ações de segurança da informação da UFDPar têm como base os princípios constitucionais e administrativos que regem a Administração Pública Federal, além de seguirem os princípios:

I - adequação: o tratamento de dados deve ser compatível com os objetivos e finalidades para os quais foram coletados, considerando o contexto em que são utilizados;

II - alinhamento estratégico: alinhar a Política de Segurança da Informação com o planejamento estratégico da UFDPar, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

III - aprendizado contínuo e melhoria: aprender com o incidente, aprimorando processos e controles para evitar incidentes futuros, e promover uma cultura de segurança e proteção de dados dentro da organização;

IV - confidencialidade: garantir que o acesso a informações sensíveis seja restrito apenas a pessoas autorizadas, protegendo os dados contra acessos não autorizados ou vazamentos;

V - conformidade com a legislação e normas: todas as operações de classificação e compartilhamento de dados devem estar conforme a legislação aplicável, incluindo as leis de proteção de dados, e aderir a padrões reconhecidos, como as normas da Organização Internacional de Normalização (ISO), para garantir a segurança e a privacidade dos dados;

VI - economicidade da proteção dos ativos de informação;

VII - finalidade: realização do tratamento para propósitos legítimos, específicos e explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

VIII - integridade: manter a precisão e a consistência das informações ao longo de todo o processo de resposta a incidentes, assegurando que os dados não sejam adulterados ou comprometidos;

IX - minimização de dados: coletar, processar e compartilhar apenas os dados estritamente necessários para tratar o incidente, para limitar o risco de exposição desnecessária de informações pessoais e empresariais;

X - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos;

XI - necessidade: limitação das ações do tratamento de incidentes ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades e objetivos do tratamento de dados;

XII - proporcionalidade: as medidas adotadas devem ser proporcionais à gravidade e ao impacto do incidente, evitando reações excessivas que possam comprometer a continuidade dos serviços ou gerar alarmes desnecessários;

XIII - responsabilidade e prestação de contas: assegurar que todos os envolvidos na resposta ao incidente cumpram suas obrigações, documentando todas as ações e decisões para posterior auditoria e análise de conformidade;

XIV - resposta ágil e eficaz: a resposta deve ser rápida e eficiente, mas sempre respeitando os limites legais e os direitos das pessoas afetadas pelo incidente;

XV - segurança: utilização de medidas técnicas e administrativas aptas a proteger os ativos de informação de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação ou difusão não autorizada por legislação, ou por ordem judicial, durante o processo de tratamento de incidentes;

XVI - segurança no compartilhamento de informações: garantir que, ao compartilhar informações sobre o incidente com terceiros, sejam usados meios seguros e que haja cláusulas de confidencialidade e segurança nos contratos com esses parceiros;

XVII - transparência: informar, de forma clara e objetiva, às partes interessadas (como usuários afetados e autoridades competentes) sobre a natureza do incidente, o impacto potencial e as medidas adotadas para mitigar danos e prevenir ocorrências futuras.

Art. 9° O tratamento de incidentes de segurança da informação abrange todos os incidentes, confirmados ou sob suspeita, que envolvam o nome ou propriedade da

UFDPar, bem como qualquer membro da comunidade acadêmica no exercício da sua relação com a UFDPar.

Parágrafo único. Entre outros, são incidentes de segurança da informação, contemplados por este processo:

I - dispositivo de tecnologia conectado à rede da UFDPar que esteja contaminado com vírus de computador;

II - vulnerabilidade de segurança incomunicada, conhecida em um sistema ou processo de TI, bem como a tentativa, bem ou malsucedida, de explorá-la para obtenção de acesso indevido, interrupção de serviço ou outros impactos à segurança da informação;

III - fluxo de comunicação de rede caracterizado como atividade maliciosa, ou envolvendo dispositivos identificados por grupos de segurança como fonte de atividades maliciosas;

IV - quaisquer outros eventos que constituam violação de requisito de segurança estabelecido por gestor de informação da UFDPar, tenham eles origem na própria Universidade ou em grupos externos;

V - violação de norma de utilização ou configuração de sistema, ou dispositivo de tecnologia, conectado ou não à rede da UFDPar;

VI - violações da Política de Segurança da Informação da UFDPar e demais normas associadas;

VII - tentativa de fraude, bem ou malsucedida, independentemente do dano causado; e

VIII - utilização de credenciais de autenticação por pessoa não autorizada.

Art. 10. As ações de Segurança da Informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da UFDPar;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da UFDPar;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV - visar à prevenção da ocorrência de incidentes.

Art. 11. Os incidentes devem ser detectados por:

I - monitoração automatizada: monitorar todo o ambiente de infraestrutura tecnológica e respectivos *logs* por intermédio de *softwares* específicos;

II - monitoração manual: relato de usuários por *e-mail*, Central de Serviços (CS) e de forma presencial.

CAPÍTULO VI

RESPONSABILIDADES

Art. 12. Os usuários internos, externos, colaboradores e discentes da UFDPar são responsáveis por garantir a segurança da informação e reportar ao TRISE qualquer incidente de segurança da informação, confirmado ou não, de que tenham conhecimento, utilizando um dos mecanismos nesta Política. Dentre as responsabilidades específicas, compete:

I - ao TRISE, executar os procedimentos de tratamento de incidentes de segurança da informação definidos nesta Política, no surgimento de qualquer denúncia ou detecção, devendo os incidentes tratados serem adequadamente registrados;

II - aos envolvidos, direta ou indiretamente em um incidente de segurança da informação sendo investigado, fornecer ao TRISE toda a informação necessária e auxílio para o adequado tratamento e resposta ao incidente;

III – à DDSI e ao Comitê de Segurança da Informação da UFDPar, definir, divulgar e promover medidas, controles e sugestões de modificações em processos de trabalho que diminuam a probabilidade da ocorrência de incidentes de segurança da informação envolvendo a UFDPar. As unidades da UFDPar ficam responsáveis pela implantação das indicações da DDSI e do Comitê de Segurança da Informação;

IV - à DDSI, a avaliação periódica e análise crítica dos registros de incidentes que resultam do processo de tratamento de incidentes de segurança e a promoção de ações que evitem a reincidência de incidentes já ocorridos;

V - as unidades da UFDPar, no desenvolvimento e operação de processos e serviços de TI, deverão manter, por um período de 3 (três) anos, os registros de suas atividades, de forma a permitir auditorias que facilitem a detecção, o tratamento e a resposta a incidentes de segurança;

VI - ao TRISE, publicar anualmente relatório com o número de incidentes, para propiciar o acompanhamento pela comunidade; e

VII - à comunidade interna e externa, devem notificar qualquer incidente de segurança da informação relativo aos ativos de informação da UFDPar ao TRISE, conforme descrito no Anexo II desta Resolução.

CAPÍTULO VII

PROCEDIMENTOS

Art. 13. O procedimento padronizado para o tratamento de incidentes de segurança é definido pelas seguintes etapas:

I - recepção da denúncia ou detecção de evento suspeito;

II - classificação e priorização;

III - contenção e mitigação;

IV - tratamento do incidente;

V - erradicação e recuperação;

VI - coleta e análise de evidências e registro;

VII - encaminhamentos e notificação dos envolvidos;

VIII - revisão pós-incidente e lições aprendidas.

CAPÍTULO VIII

RECEPÇÃO DA DENÚNCIA OU DETECÇÃO DE EVENTO SUSPEITO

Art. 14. A DDSI receberá notificações internas, provenientes da comunidade acadêmica, de órgãos/grupos de segurança da informação parceiros (Rede Nacional de Ensino e Pesquisa - RNP), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) e outras equipes de tratamento de incidentes de segurança (ETIR's), assim como de reclamantes externos. As notificações devem conter evidências do incidente de segurança da informação que está sendo reportado, bem como, informações de contato do reclamante e dados adicionais que possibilitem melhor classificação e priorização do incidente. Para notificar um incidente, o relator deve utilizar um dos meios de comunicação abaixo relacionados:

I - Central de Serviços: disponível em cs.ufdpar.edu.br;

II - *e-mail*: protic.ddsi@ufdpar.edu.br;

III - atendimento presencial: *Campus* Ministro Reis Velloso, Setor Norte, Bloco C, Piso 2, Leste, Pró-Reitoria de Tecnologia da Informação e Comunicação (PROTIC), setor de infraestrutura;

IV - via Ouvidoria da UFDPar, por meio do Fala.BR: https://falabr.cgu.gov.br/web/.

Art. 15. As seguintes informações devem ser fornecidas para facilitar a análise e resposta adequadas:

I - informações de contato do reclamante;

II - data e hora da primeira identificação do evento/fraqueza;

III - informações da origem do incidente;

IV - informações do alvo do incidente;

V - impactos (se conhecidos);

VI - descrição do incidente;

VII - se o evento/fraqueza for relatado por *e-mail*, telefone ou pessoalmente, a ETIR deverá relatar o evento na Central de Serviços.

CAPÍTULO IX

CLASSIFICAÇÃO E PRIORIZAÇÃO

Art. 16. A ETIR determinará se um evento suspeito em análise constitui ou não um incidente de segurança. Caso o evento não seja classificado como incidente de segurança, o TRISE poderá repassar o evento para outra área, para análise, e o atendimento será encerrado, sem perda do registro da denúncia ou detecção.

§ 1° A ETIR poderá solicitar informações adicionais aos envolvidos em um incidente antes de emitir um parecer.

§ 2° O incidente de segurança deverá ser analisado para determinar se é de responsabilidade da UFDPar. Caso não seja, deverá ser encaminhada uma notificação para uma equipe de segurança externa responsável, para o tratamento do incidente.

Art. 17. O incidente de segurança deverá ser classificado conforme o processo de classificação do tipo de incidentes adotado pelo TRISE.

Parágrafo único. O incidente de segurança deverá ser reclassificado sempre que novas informações obtidas invalidem a classificação inicial.

Art. 18. A Equipe de Tratamento de Incidentes deverá classificar e priorizar a resposta aos incidentes com base no impacto analisado, conforme os seguintes níveis de prioridade:

I - prioridade 1 (crítica): incidentes de maior gravidade, exigindo contenção imediata e resposta inicial em até 10 (dez) minutos, com resolução em até 4 (quatro) horas;

II - prioridade 2 (alta): incidentes de alta gravidade, exigindo contenção imediata e resposta inicial em até 30 (trinta) minutos, com resolução em até 8 (oito) horas;

III - prioridade 3 (média): incidentes de gravidade média, exigindo contenção imediata e resposta inicial em até 1 (uma) hora, com resolução em até 2 (dois) dias úteis;

IV - prioridade 4 (baixa): incidentes de baixa gravidade, exigindo contenção imediata e resposta inicial em até 4 (quatro) horas, com resolução em até 5 (cinco) dias úteis.

Parágrafo único. A contenção de incidentes, independentemente do nível de prioridade, deve ser realizada imediatamente após a identificação. Os prazos de resposta inicial e resolução referem-se às ações de remediação e conclusão do tratamento do incidente.

CAPÍTULO X

CONTENÇÃO E MITIGAÇÃO

Art. 19. A ETIR deverá adotar medidas imediatas para impedir a propagação do incidente e minimizar seus impactos.

Art. 20. A contenção será realizada de acordo com o tipo e gravidade do incidente, podendo envolver isolamento de sistemas, bloqueio de acessos e comunicação com partes envolvidas.

CAPÍTULO XI

TRATAMENTO DO INCIDENTE

Art. 21. A escolha do incidente para atendimento deve levar em consideração a sua criticidade e a priorização, estabelecidos durante a etapa de classificação.

Art. 22. Os procedimentos de gerenciamento de Incidentes de Segurança da Informação devem ser indicados formalmente pelo TRISE que define as etapas necessárias a serem tomadas em resposta a qualquer incidente relacionado à segurança da informação.

§ 1° O conjunto de procedimentos deve ser executado com os seguintes parâmetros e igual peso:

I - o dano potencial total causado pela inação; e

II - o dano potencial causado pelas medidas de contenção em si.

§ 2° A avaliação dos danos deverá considerar:

I - indivíduos, membros ou não da UFDPar;

II - terceiros, envolvidos ou não no incidente; e

III - o dano à UFDPar, à sua propriedade e à sua imagem.

§ 3° Cabe ao TRISE determinar os responsáveis pela execução das ações referidas no *caput* deste artigo. A não execução das ações pelos responsáveis configura vulnerabilidade de segurança, que implica em novo incidente de segurança da informação. A notificação destes responsáveis será feita de forma imediata, ou logo que possível.

Art. 23. A resposta a um incidente será registrada conforme os níveis de prioridade abaixo, com os respectivos tempos de resposta inicial e resolução:

I - prioridade 1 (crítica):

a) definição: incidente de maior gravidade, com impacto crítico nos sistemas ou operações;

b) tempo de resposta inicial: até 10 (dez) minutos;

c) tempo de resolução: até 4 (quatro) horas;

II - prioridade 2 (alta):

a) definição: incidente de alta gravidade, com impacto significativo, mas não crítico;

b) tempo de resposta inicial: até 30 (trinta) minutos;

c) tempo de resolução: até 8 (oito) horas;

III - prioridade 3 (média):

a) definição: incidente de gravidade média, com impacto moderado;

b) tempo de resposta inicial: até 1 (uma) hora;

c) tempo de resolução: até 2 (dois) dias úteis;

IV - prioridade 4 (baixa):

a) definição: incidente de baixa gravidade, com impacto mínimo;

b) tempo de resposta inicial: até 4 (quatro) horas;

c) tempo de resolução: até 5 (cinco) dias úteis;

Parágrafo único. Os tempos de resposta inicial referem-se ao início das ações de remediação após a contenção imediata, que deve ser realizada independentemente do nível de prioridade.

Art. 24. Cabe ao TRISE monitorar as medidas de segurança efetuadas para determinar se as ações e medidas tomadas atingiram os seus objetivos.

Art. 25. Os incidentes de segurança da informação devem ser registrados e receber um número de incidente para rastreamento e referência futura. O registro pode incluir, mas não se limitar a:

I - causas: diretas e indiretas, isso levou ao incidente;

II - impacto: quais sistemas sofreram durante o incidente;

III - ações tomadas: pelo usuário e servidores da Diretoria de Sistemas e Infraestrutura de TIC da PROTIC, para relatar e gerenciar o incidente;

IV - nível de dano: quais foram as perdas causadas;

V - data e hora da ocorrência.

Parágrafo único. O procedimento de resposta a incidentes deve dar continuidade ao relato de eventos, incluindo planos de contingência que garantam a manutenção ou rápida retomada dos sistemas afetados.

Art. 26. Após findar o incidente a ETIR deve fazer uma revisão para validar se o incidente foi efetivamente respondido ou não. Se for determinado que o incidente não foi abordado adequadamente, a ETIR deve reiniciar o estágio de 'remediação'.

Art. 27. Após o encerramento do incidente a ETIR deve realizar um *backup* de todas as evidências relacionadas ao relato e resposta ao incidente em um local seguro para que, em caso de novas escalações (por exemplo, para o cliente, autoridades policiais ou órgãos reguladores etc.), as evidências possam ser reproduzidas. Todo o cuidado deve ser tomado pela ETIR para não adulterar as evidências durante o *backup*.

Art. 28. Se o incidente envolver uma violação de dados do cliente ou dados pessoais de qualquer indivíduo, ou grupo de indivíduos, a ETIR deverá preencher o Formulário de Notificação de Violação de Dados (Anexo III desta Resolução) e enviar via processo administrativo ao encarregado de dados da UFDPar, para este notificar a Autoridade Nacional de Proteção de Dados (ANPD) e as pessoas ou entidades afetadas.

Art. 29. Quaisquer alterações no processo feitas como resultado da revisão pós-incidente devem ser formalmente registradas.

Art. 30. Após o encerramento do incidente, deve ser realizada uma análise crítica das ações efetuadas e dos resultados alcançados, para identificar possíveis melhorias no processo de tratamento e resposta a incidentes.

Art. 31. Após cada incidente, um exercício de lições aprendidas deve ser conduzido pela ETIR que deve manter e conduzir uma sessão retrospectiva (reunião) com todo o pessoal envolvido na resposta ao incidente e capturar as lições aprendidas durante tal resposta. Essas devem ser usadas pela ETIR para iniciar mais mudanças nos ativos de informação ou instalações de processo de informação para garantir que tais incidentes ou similares não ocorram no futuro.

CAPÍTULO XII

ERRADICAÇÃO E RECUPERAÇÃO

Art. 32. Após a contenção, a ETIR deverá atuar na erradicação da vulnerabilidade ou ameaça que originou o incidente.

Art. 33. O processo de recuperação incluirá a restauração segura dos sistemas e a verificação da estabilidade operacional antes da retomada dos serviços.

CAPÍTULO XIII

COLETA E ANÁLISE DE EVIDÊNCIAS E REGISTRO

Art. 34. A ETIR coletará ou solicitará as evidências necessárias ao tratamento e resposta ao incidente aos devidos responsáveis.

Art. 35. Cabe a ETIR determinar e registrar, quando aplicável, no mínimo, as seguintes informações:

I - identificação das pessoas e organizações envolvidas e sua relação com a Universidade;

II - descrição do incidente e motivo (causa raiz);

III - medidas de contenção efetuadas ou recomendadas e seus resultados;

IV - avaliação do dano efetivamente causado e do dano potencial do incidente;

V - grupos e pessoas que devem ser notificados e respectiva informação a ser fornecida, considerando sempre aspectos de confidencialidade pertinentes;

VI - medidas preventivas a serem tomadas a médio e longo prazo, para evitar a reincidência do incidente, e seus respectivos responsáveis; e

VII - todas as evidências coletadas durante o processo.

§ 1° Conforme a natureza do incidente, serão registradas informações adicionais, para conformidade com a legislação ou com norma específica.

§ 2° Todas as informações e evidências coletadas deverão ser adequadamente registradas e protegidas de modo a garantir a confidencialidade e integridade.

Art. 36. Cabe ao TRISE receber toda a informação e providência de processos rigorosos para a coleta de evidências forenses, como evidências digitais, evidências físicas, evidências originais e cópias de evidências.

CAPÍTULO XIV

ENCAMINHAMENTOS E NOTIFICAÇÃO DOS ENVOLVIDOS

Art. 37. Ao fim da análise, a ETIR comunicará aos envolvidos, informando:

I - aos responsáveis pela execução das ações de médio e longo prazo;

II - ao denunciante, a respeito dos encaminhamentos feitos e os resultados obtidos;

III - às autoridades, quando o incidente se caracterizar como um crime, quando a legislação ou norma assim o exigir, ou quando houver possíveis consequências jurídicas para a UFDPar;

IV - ao CTIR Gov e ao CAIS, quando os incidentes tiverem associados a agentes externos à Universidade, ou que tenham impacto nos serviços e processos institucionais;

V - a outros grupos de segurança ou interessados que possam fazer uso útil da informação em favor da segurança da informação da Universidade ou de outras instituições;

VI - aos órgãos de controle interno, quando o incidente se caracterizar como infração administrativa e disciplinar provocada por servidor público no exercício das suas funções, bem como atos lesivos praticados por entes privados contra a UFDPar.

CAPÍTULO XV

REVISÃO PÓS-INCIDENTE E LIÇÕES APRENDIDAS

Art. 38. Após o encerramento do incidente, a ETIR realizará uma revisão pós-incidente para avaliar a eficácia das medidas adotadas.

Art. 39. As lições aprendidas serão documentadas e servirão como base para aprimorar os procedimentos futuros e reduzir riscos.

CAPÍTULO XVI

ENCAMINHAMENTOS PARA ANÁLISE FORENSE

Art. 40. O TRISE poderá decidir realizar a análise forense sob demanda em algum caso, desde que julgue necessário e que seja previamente encaminhado pelo diretor das unidades envolvidas, mediante abertura de processo administrativo.

CAPÍTULO XVII

DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

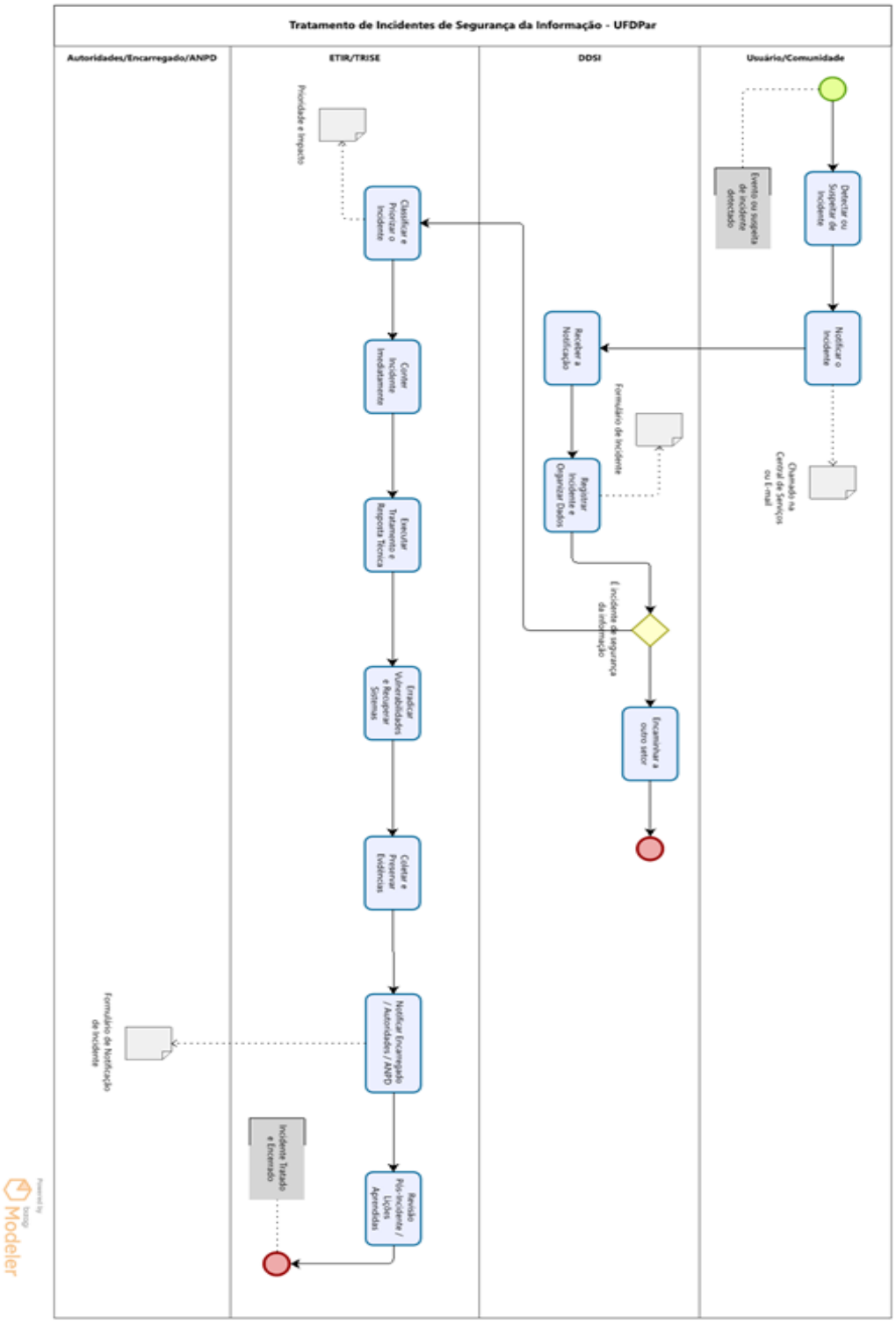
Art. 41. A DDSI deve promover ações de treinamento e conscientização para que a comunidade acadêmica entenda suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 42. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

ANEXO II DA RESOLUÇÃO CONSUNI N° 171 DE 16 DE JULHO DE 2025

FLUXO DO TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO DELTA DO PARNAÍBA
CAMPUS MINISTRO REIS VELLOSO

ANEXO III DA RESOLUÇÃO CONSUNI N° 171 DE 16 DE JULHO DE 2025

FORMULÁRIO DE NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS

Informações Gerais			
Nome da instituição:	Universidade Federal do Delta do Parnaíba (UFDPar)		
Unidade responsável pelo relato:			
Nome do responsável pelo relato:			
Telefone:		*E-mail*:	
Detalhes do Incidente			
Data da identificação do incidente:		Hora:	
Data estimada da ocorrência:		Hora:	
Local da ocorrência:			
Quantidade de titulares afetados:			

Quais os tipos de dados envolvidos? (admite mais de uma marcação)

☐ Dados pessoais. ☐ Dados sensíveis. ☐ Dados de clientes. ☐ Outros. (especifique abaixo)

Informe os tipos de dados envolvidos, se cabível:

Quais as categorias de titulares afetados pelo incidente? (admite mais de uma marcação)

☐ Servidores. ☐ Alunos. ☐ Serviços Terceirizados. ☐ Outros. (especifique abaixo)

Informe o quantitativo de titulares afetados, por categoria:

Descrição do Incidente
Qual o tipo de incidente? (informe o tipo mais específico)

☐ Sequestro de Dados (*ransomware*) sem transferência de informações.

☐ Exploração de vulnerabilidade em sistemas de informação.

☐ Roubo de credenciais / Engenharia Social.

☐ Publicação não intencional de dados pessoais.

☐ Envio de dados a destinatário incorreto.

☐ Negação de Serviço (DoS).

☐ Perda/roubo de documentos ou dispositivos eletrônicos.

☐ Falha em equipamento (*hardware*).

☐ Outro tipo de incidente cibernético.

(especifique abaixo)

☐ Sequestro de Dados (r*ansomware*) com transferência e/ou publicação de informações.

☐ Vírus de computador / *Malware*.

☐ Violação de credencial por força bruta.

☐ Divulgação indevida de dados pessoais.

☐ Acesso não autorizado a sistemas de informação.

☐ Alteração / exclusão não autorizada de dados.

☐ Descarte incorreto de documentos ou dispositivos eletrônicos.

☐ Falha em sistema de informação (*software*).

☐ Outro tipo de incidente não cibernético.

(especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Quais medidas foram tomadas para contenção das causas do incidente?

Avaliação dos riscos aos titulares

Possibilidade de uso indevido dos dados:		
☐ Baixa.	☐ Média.	☐ Alta.

Existe evidência de acesso ou uso indevido dos dados?		
☐ Sim.	☐ Não.	☐ Não se aplica.

De que forma o incidente afetou os dados pessoais? (admite mais de uma marcação)	
☐ Confidencialidade.	Houve acesso não autorizado aos dados, violando seu sigilo.
☐ Integridade.	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
☐ Disponibilidade.	Houve perda ou dificuldade de acesso aos dados por período significativo.

Impacto potencial:	
Notificação e Comunicação	
Data de envio ao encarregado de dados:	
Data de notificação à ANPD (se aplicável):	
Data de notificação aos titulares (se aplicável):	

Quais os meios utilizados para notificação?			
☐ *E-mail*.	☐ CS.	☐ Telefone.	☐ Outros.

Qual a forma de mitigação do impacto aos titulares?			
Responsável pela apuração do incidente			
Nome:			
Cargo / Função:			
Telefone:		*E-mail*:	
Assinatura do responsável pelo relato			
Nome:			
Cargo / Função:			
Assinatura:		Data:	