INSTRUÇÃO NORMATIVA Nº 002/2023-DTI

Regulamenta os Procedimentos Relativos à Gestão, Notificações e Resposta aos Incidentes de Segurança da Informação no Âmbito da Universidade Estadual do Paraná – UNESPAR.

O **NÚCLEO DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE ESTADUAL DO PARANÁ**, no uso de suas atribuições legais e estatutárias, considerando a Lei 13709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

RESOLVE:

Art. 1º Instituir o Plano de Resposta a Incidentes de Segurança da Informação.

I. Todas as notificações de incidentes de segurança da informação deverão ser comunicadas por e-mail institucional no seguinte endereço eletrônico:

seguranca.informacao@unespar.edu.br

Art. 2º Para efeitos desta Instrução Normativa, considera-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 Universidade ou que tenha acesso;

II. **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;

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

IV. **Engenharia social:** é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com *malware* ou abrir *links* para sites infectados;

V. **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;
VI. **Scripts:** conjunto de instruções para que uma função seja executada em determinado aplicativo;
VII. **Malware:** é um termo genérico para qualquer tipo de software malicioso projetado para prejudicar ou explorar qualquer dispositivo, serviço ou rede programável;
VIII. **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;
IX. **Spyware:** programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
X. **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;
XI. **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;
XII. **Worm:** programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;
XIII. **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;
XIV. **Dados pessoais:** qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente;
XV. **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;
XVI. **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;
XVII. **Abuso de sítio eletrônico:** acesso não autorizado à administração ou código-fonte de um sítio, que possa resultar em desfiguração, pichação ou modificação;
XVIII. **Negação de serviço (DoS):** ou DDoS, negação de serviço distribuída, é um tipo de ataque cibernético que tenta indisponibilizar um *website* ou recurso de rede inundando-o com tráfego mal-intencionado e deixando-o incapaz de operar;
XIX. **NTI:** Núcleo de Tecnologia da Informação da UNESPAR;

XX. **DTI:** Diretoria de Tecnologia da Informação;
XXI. **DADS:** Divisão de Análise e Desenvolvimento de Sistemas;
XXII. **DIRSI:** Divisão de Infraestrutura de Redes e Segurança da Informação;
XXIII. **DASU:** Divisão de Apoio e Suporte ao Usuário;
XXIV. **ANPD:** Agência Nacional de Proteção de Dados.

Art. 3º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETRIC) na UNESPAR deve ser composta por representantes técnicos das seguintes unidades:

I. DTI/NTI;
II. DADS/NTI;
III. DIRSI/NTI;
IV. DASU/NTI.

Parágrafo 1º A depender do nível do incidente ocorrido com base na Tabela de Classificação de Incidentes (ANEXO I), os membros da ETRIC poderão contar ainda com a participação do Encarregado de Proteção de Dados Pessoais, de um Especialista em Privacidade, de um Especialista em Comunicação ou quaisquer outros especialistas técnicos que se fizerem necessários.

Parágrafo 2º Quando da necessidade do Encarregado de Proteção de Dados Pessoais, é atribuição do mesmo passar as devidas orientações aos envolvidos, nos termos do inciso III, §2º, art. 41 da LGPD.

Art. 4º As unidades que compõem a ETRIC têm como papel:

I. Receber notificações;
II. Avaliar notificações;
III. Executar medidas de contenção;
IV. Conduzir e documentar as respostas relacionadas a incidentes envolvendo sistemas e recursos computacionais;
V. Manter o registro e a documentação proveniente de processos de incidente;
VI. Encaminhar para ciência do controle interno e do gestor, após conclusão, os processos de incidente finalizados;
VII. Apresentar ao controle interno e ao gestor, anualmente, relatório contendo todos os processos de incidentes abertos na UNESPAR;
VIII. Solicitar à alta gestão autorização para contratação de apoio externo quando não dispuser de recursos suficientes para contenção ou recuperação de incidente.

Art. 5º 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 da 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;
IX. Outros: incidente não categorizado.

Art. 6º Ao receber a comunicação da ocorrência ou suspeita de um incidente cibernético, o NTI acionará a ETRIC, de maneira a efetuar a classificação do incidente, de acordo com a Tabela de Classificação de Incidentes (ANEXO I) e tomar as ações correspondentes.

Parágrafo único. Caso seja identificada a necessidade de contato com os titulares de dados pessoais, este deverá ser feito seguindo o modelo definido no ANEXO II desta Instrução Normativa.

Art. 7º São responsabilidades da ETRIC:
I. Planejar a resposta a incidentes cibernéticos;
II. Avaliar e implementar ações técnicas e administrativas para prevenir a ocorrência de incidentes cibernéticos;
III. Avaliar periodicamente a infraestrutura de TI da Universidade, de maneira a mantê-la sempre atualizada;
IV. Realizar o tratamento e as respostas necessárias quando da ocorrência de incidentes cibernéticos;
V. Prover a divulgação institucional sobre a responsabilidade individual de notificação de incidentes cibernéticos;
VI. Comunicar imediatamente todos os envolvidos, incluindo as autoridades indicadas na Tabela de Classificação de Incidentes (ANEXO I), de acordo com o nível do incidente e quando for necessário.

Art. 8º Sempre que houver um incidente cibernético, o mesmo deverá ser documentado pela ETRIC, por meio de relatório detalhado contendo no mínimo as seguintes informações:
I. Onde ocorreu o incidente e quem o reportou, caso não tenha sido denúncia anônima;
II. Como o incidente foi descoberto;

III. Qual foi a causa do incidente;
IV. Quais foram as vulnerabilidades exploradas ou que levaram ao incidente;
V. Se houve o uso de credenciais comprometidas e quais são essas credenciais;
VI. Quais sistemas, equipamentos e redes foram comprometidos;
VII. Quais unidades da universidade foram afetadas;
VIII. Se houve exposição, transferência ou sequestro de dados;
IX. Quais dados e quais titulares, exatamente, foram afetados;
X. Quais foram as medidas adotadas para contenção, erradicação e recuperação; e
XI. Quais foram as lições aprendidas;
XII. Encaminhamento para instância competente para que sejam tomadas as providências cabíveis, quando se fizer necessário.

Art. 9º Os comunicados à ANPD, quando ocorrerem, em consonância com as designações definidas na Tabela de Classificação de Incidentes (ANEXO I), deverão conter no mínimo as seguintes informações:

I. A descrição da natureza dos dados pessoais afetados;
II. As informações sobre os titulares envolvidos;
III. A indicação das medidas técnicas e de segurança, utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV. Os riscos relacionados ao incidente;
V. Os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI. As medidas que foram ou que serão adotadas para reverter ou mitigar os impactos do incidente.

Art. 10º Esta Instrução Normativa entrará em vigor na data de sua publicação.

Paranaguá, 12 de dezembro de 2023

Maike dos Santos
Diretoria de Tecnologia da Informação – DTI
Portaria N.º 110/2021 – Reitoria

ANEXO I
CLASSIFICAÇÃO DE INCIDENTES

Nível	Descrição do Incidente	Equipe Responsável	Ações de Resposta
I	- Invasão dos ambientes virtuais da Universidade, sem vazamento de dados; - Falhas ou indisponibilidade em sistemas de informações e/ou perda de serviços; - Código malicioso; - Abuso ou fraude de sítio eletrônico; - Ataque de engenharia social / phishing; - Negação de serviço (DDoS); - Uso impróprio de sistemas de informação; - Escaneamento não permitido da rede interna.	- ETRIC; - Especialista em comunicação, quando se fizer necessário.	- Resolução do incidente, havendo comunicação aos usuários, caso necessário.
II	- Vazamento ou sequestro de dados, não comportando dados pessoais. - Erros resultantes de dados incompletos ou inconsistentes, não comportando dados pessoais.	- ETRIC; - Especialista em comunicação, quando se fizer necessário.	- Resolução do incidente, havendo comunicação aos usuários, caso necessário. - Recuperação de Backup caso necessário.
III	- Vazamento, sequestro ou perda de dados pessoais devido a ataques cibernéticos; - Acesso a dados pessoais por qualquer pessoa não autorizada; - Exposição de dados pessoais, de forma acidental em sites, comunicados ou redes sociais; - Alteração indevida, eliminação indesejada ou inconsistência de dados pessoais; - Violações de confidencialidade e integridade.	- ETRIC; - Especialista em comunicação, quando se fizer necessário; - Encarregado de Proteção de Dados Pessoais; - Especialista em Privacidade.	- A depender da probabilidade de dano ao titular de dados pessoais: a) Baixa: resolver o incidente; b) Média: resolver o incidente e comunicar a ANPD e o Comitê de TI; c) Alta: resolver o incidente, comunicar a ANPD, O Comitê de TI e os titulares de dados pessoais. - Recuperação de Backup caso necessário.
IV	- Perda de dados em decorrência de catástrofes naturais, quedas de energia e outros incidentes adversos.	- ETRIC; - Especialista em comunicação; - Encarregado de Proteção de Dados Pessoais; - Especialista em Privacidade.	- Resolver o incidente, comunicar a ANPD, O Comitê de TI e os titulares de dados pessoais. - Recuperação de Backup caso necessário.

ANEXO II

Texto padrão para comunicação de incidentes aos titulares de dados pessoais

Prezado titular de dados pessoais,

Comunicamos que houve um _____, o que acarretou _____ (vazamento/perda/publicação indevida/etc.) dos seus seguintes dados: _____.

Este incidente ocorreu, apesar de tomarmos todas as medidas técnicas para evitar esse tipo de situação, por conta de _____ (especificar o motivo). Nossa Equipe de Tratamento e Resposta a Incidentes Cibernéticos já está trabalhando para normalizar a situação e evitar que o mesmo volte a ocorrer. No entanto, é recomendável que você adote as seguintes medidas:

1. Xxxxxx
2. Xxxxx
3. X

Lamentamos o ocorrido e agradecemos sua compreensão.

Atenciosamente,

Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UNESPAR