MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ

INSTRUÇÃO NORMATIVA N° 02/2023 - CIGD

Institui o Plano de Resposta a Incidentes da Universidade Federal do Paraná

O **Comitê Institucional de Governança Digital da Universidade Federal do Paraná,** no uso de suas atribuições e, considerando:

1) A Lei 13709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
2) O Decreto 9637/2018, que institui a Política Nacional de Segurança da Informação;
3) A IN 01/2020, do Gabinete de Segurança Institucional, que dispõe sobre a estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
4) O Decreto 10748/2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos; e
5) A Resolução 38/22-COPLAD, que estabelece a Política de Segurança da Informação da UFPR;

RESOLVE:

Art. 1 – Instituir o Plano de Resposta a Incidentes da Universidade Federal do Paraná.

Art. 2 – Para efeitos dessa Instrução Normativa, considera-se:

I. Abuso de sítio eletrônico: acesso não autorizado à administração ou código-fonte de um sítio, que possa resultar em desfiguração, pichação ou modificação da aparência do mesmo.

II. **AGTIC:** Agência de Tecnologia da Informação e Comunicação da UFPR.

III. **ANPD:** Agência Nacional de Proteção de Dados Pessoais.

IV. **CGR:** Coordenadoria de Gestão de Riscos da PROPLAN.

V. **CPTRIC:** Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, órgão do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República, criada no §1º do art 5 do Decreto 10748/2021.

VI. **CSA:** Seção de Central de Serviços e Atendimento da AGTIC.

VII. **CSGD:** Coordenadoria de Software e Gestão de Dados da AGTIC.

VIII. **CSI:** Coordenadoria de Serviços e Infraestrutura da AGTIC.

IX. **CSGD:** Coordenadoria de Sistemas e Gestão de Dados da AGTIC.

X. **Gestor da Segurança da Informação:** pessoa formalmente indicada por ato da Reitoria para atuar como responsável pela gestão da segurança de informação e comunicação na Universidade, nos termos da PNSI.

XI. **Encarregado de Proteção de Dados Pessoais:** pessoa indicada pela reitoria para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos da LGPD. Também chamado de *Data Protection Officer (DPO).*

XII. **Engenharia social:** técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware, abrir links infectados, fornecer senhas ou realizar outras ações que coloquem em risco o usuário ou a instituição.

XIII. **Escaneamento em redes:** varredura minuciosa em uma rede de computadores, com o objetivo de coletar informações sobre os mesmos.

XIV. **Especialista em Privacidade:** gestor de governança em privacidade na Universidade e responsável pelo projeto de adequação da Universidade à LGPD, também chamado de *Data Protection Expert (DPE).* Na UFPR, figura exercida pelo coordenador da CSGD.

XV. **Fraude de sítio eletrônico:** criação de página falsa com o objetivo de capturar dados pessoais ou institucionais.

XVI. ***Malware:*** programas maliciosos, especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

XVII. **Negação de Serviço:** DoS (*Denial of Service)*, técnica pela qual um atacante visa tirar de operação um serviço, um computador ou uma rede conectada à internet.

XVIII. ***Phishing message:*** envio de e-mails falsos, normalmente com alteração de campos do cabeçalho, com o objetivo infectar o computador do usuário com os mais diversos fins, como por exemplo se fazer passar por outra pessoa.

Art. 3 – A Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETRIC) na UFPR será composta por representantes técnicos das seguintes unidades:

I. CSA/AGTIC

II. CSI/AGTIC;

III. CSGD/AGTIC;

IV. CGR/PROPLAN;

§1º A depender do nível do incidente ocorrido, a ETRIC poderá 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.

§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. 4 – São atribuições 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 TIC da Universidade, de maneira a mantê-la atualizada;

IV. Fazer comunicações ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, quando couber;

V. Realizar o tratamento e as respostas necessárias quando da ocorrência de incidentes cibernéticos;

VI. Prover a divulgação institucional sobre a responsabilidade individual de notificação de incidentes cibernéticos.

Art. 5 – Ao receber a comunicação da ocorrência ou suspeita de um incidente cibernético, a AGTIC acionará a ETRIC, de maneira a efetuar a classificação do incidente, de acordo com a tabela constante no Anexo I dessa Instrução Normativa, e tomar as ações correspondentes.

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

Art. 6 – Sempre que houver um incidente cibernético, o mesmo deverá ser documentado pela ETRIC, sendo que o relatório deverá conter, no mínimo:

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.7 – Os comunicados à ANPD, quando ocorrerem, em consonância com as designações definidas no anexo I dessa Instrução Normativa, deverão conter, no mínimo:

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 efeitos do prejuízo.

Art. 8 – Essa Instrução Normativa entra em vigor na data de sua publicação.

ANEXO I
CLASSIFICAÇÃO DE INCIDENTES

Nível	**Descrição**	**Equipe Necessária**	**Ações**
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 (DoS); - 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.

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 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 Centro de Incidentes do Governo; c) Alta: resolver o incidente, comunicar a ANPD, o CPTRIC e os titulares de dados pessoais;
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 CPTRIC e os titulares de dados pessoais;

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 UFPR

Curitiba, 18 de abril de 2023

Documento assinado eletronicamente por **RICARDO MARCELO FONSECA**, **REITOR**, em 18/04/2023, às 16:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida aqui informando o código verificador **5497019** e o código CRC **8D41ADFF**.