MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DA INTEGRAÇÃO LATINO-AMERICANA

COMITÊ DE GOVERNANÇA DIGITAL

RESOLUÇÃO Nº 1, DE 15 DE OUTUBRO DE 2021

Estabelece as diretrizes para os procedimentos de backup, guarda e recuperação de dados digitais da UNILA.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL - CGD, designado pela Portaria nº 260/2021/GR/UNILA, no exercício de suas atribuições e, CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais); CONSIDERANDO a IN Nº 1, de 27 de Maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal; CONSIDERANDO a ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação; CONSIDERANDO a iniciativa 3.2 de aperfeiçoar a governança de TIC, identificada no PETIC 2019-2021; e CONSIDERANDO a iniciativa 5.2 de aperfeiçoar a gestão de segurança da informação da instituição, identificada no PETIC 2019-2021, resolve:

Art. 1º Estabelecer as diretrizes e normas para os procedimentos de backup e guarda de dados digitais na UNILA.

DAS DISPOSIÇÕES GERAIS

Art. 2º Para efeitos desta normativa, considera-se:
I - Backup: conjunto de procedimentos que permitem preservar os dados de um sistema computacional, garantindo a guarda e a recuperação;
II - Mídia: meio físico ou virtual no qual efetivamente são armazenados os dados de um backup;
III - Objeto: qualquer dado passível de backup e restauração;
IV - Ativos de Informação - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;
V - Administrador do serviço de backup: Divisão de Serviços Corporativos e Segurança - DISEG, subordinada à Coordenadoria de Tecnologia da Informação - CTIC;
VI - Administrador de recurso: agente responsável pela administração de um ativo de informação ou pelos dados por este produzidos;
VII - Plano de backup: documento onde estão descritos os procedimentos, objetos, prazos de retenção, modalidades, frequência e descarte dos dados e das tarefas de backup.

Art. 3º Esta normativa passa a compor a Política de Segurança da Informação (POSIN) e alcança toda a UNILA.

Art. 4º A preservação e a recuperação de dados abrange exclusivamente repositórios de dados institucionais, armazenados nos centros de dados custodiados pela CTIC.

Art. 5º Não são objetos desta normativa:
I - dados armazenados nas estações de trabalho de usuários; e
II - imagens de câmeras de segurança.

DAS DIRETRIZES

Art. 6º O serviço de backup deve:
I - garantir a segurança, a privacidade e a confidencialidade dos dados;
II - utilizar criptografia nos dados armazenados e em trânsito pela rede;
III - garantir a redução dos riscos associados à perda de dados.
Parágrafo único. A critério dos administradores do plano de backup, levando em consideração a criticidade dos dados, o tempo de transferência e de restauração da cópia de segurança, a criptografia poderá ser dispensada.

Art. 7º Os backups deverão ser testados periodicamente, com o objetivo de garantir a integridade e disponibilidade dos dados.

Art. 8º Deverão ser consideradas as seguintes características na seleção dos meios de armazenamento utilizados:
I - a criticidade dos dados;
II - o tempo de retenção dos dados;
III - o tempo para restauração.

Art. 9º Nos locais onde são armazenados os backups, deverão ser implementadas medidas de controle de acesso físico e o registro dos acessos realizados.

Art. 10. Antes do envio para descarte ou garantia, deverão ser aplicados procedimentos físicos ou lógicos nos equipamentos e mídias defeituosas ou inservíveis, que impossibilitem a recuperação dos dados por terceiros.

DO PLANO DE BACKUP

Art. 11. O plano de backup deve:
I - considerar a criticidade dos objetos, os requisitos legais e os riscos associados à continuidade do negócio ao estabelecer os ciclos de execução, retenção e testes de restauração;
II - estabelecer medidas, dentro dos limites operacionais, para que a restauração dos objetos seja realizada no menor tempo, com o menor volume de informações perdidas;
III - estabelecer as responsabilidades pela execução dos testes de restauração e pelo atesto de integridade;
IV - considerar o armazenamento dos backups em local geográfico distinto da origem dos dados;
V - considerar o armazenamento dos backups em destino offline;
VI - ter seu acesso restrito aos administradores do serviço e de recursos, por conter informações sensíveis como dados de equipamentos, locais de armazenamento, nomes de pastas e de arquivos.

Art 12. Objetos de backup referentes a projetos de ensino, pesquisa ou extensão, serão mantidos por até 90 dias após o encerramento do projeto.
Parágrafo único. O administrador do recurso deverá fornecer os equipamentos ou mídias necessárias para a cópia final dos dados.

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 13. Compete ao Comitê de Governança Digital - CGD, estabelecer e revisar regularmente a relação de ativos de informação críticos para a instituição e que devem ser considerados nas tarefas de backup, conforme ANEXO I.

Art. 14. Compete ao administrador do serviço de backup:
I - elaborar o plano de backup em conjunto com o administrador de recurso;
II - configurar as ferramentas, softwares e os clientes de backup;
III - criar e manter as tarefas de backup;
IV - restaurar backups;
V - emitir notificações e relatórios;
VI - fazer manutenções periódicas nos equipamentos de backup;
VII - definir padrões de equipamentos, conforme a infraestrutura utilizada em cada centro de dados.

Art. 15. Compete ao administrador de recurso, solicitar ao administrador do serviço, a inclusão ou atualização do plano de backup, referente aos ativos de informação sob sua responsabilidade.

DAS DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 16. A CTIC, como responsável pela curadoria de dados técnicos e operacionais, deve projetar, com o auxílio das demais unidades envolvidas, os mecanismos e ferramentas para aplicação desta norma.

Art. 17. Os planos de backup, referentes a cada um dos ativos de informação, serão elaborados a partir da publicação desta normativa.
§1. No prazo de 60 dias, o administrador do serviço providenciará, em conjunto com os administradores de recurso, a elaboração dos planos de backup dos ativos de informação críticos, definidos no ANEXO I;
§2. O administrador do serviço notificará os administradores de recursos, para que no prazo de 90 dias, procedam com a adequação ao plano de backup ou realizem a cópia final dos dados, conforme estabelecido nos arts. 12 e 15;
§3. Serão removidos das tarefas de backup e terão os dados excluídos os ativos de informação que não estiverem com os planos elaborados no prazo estabelecido.

Art. 18. Casos omissos serão resolvidos pela CTIC.

Art. 19. Esta normativa entra em vigor na data de sua publicação.

ANEXO I

Ficam previamente estabelecidos como ativos de informação críticos para a UNILA:
I - o Sistema Integrado de Gestão (SIG) e seus sistemas orbitais;
II - o correio eletrônico;
III - a plataforma de Educação à Distância (Moodle);
IV - sistema inscreva;
V - o portal institucional;
VI - portal de atos oficiais;
VII - a base de usuários;
VIII - o serviço interno de armazenamento e compartilhamento de arquivos;
IX - o repositório interno de códigos fontes e arquivos de configuração de ativos de rede, servidores e estações de trabalho.

GLEISSON ALISSON PEREIRA DE BRITO

Observações:

Publicada no Boletim de Serviço nº 117, de 21 de outubro de 2021.