PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO
Gabinete da Presidência

ANEXO ÚNICO
(PORTARIA GP nº 061/2019

Norma de cópias de segurança (backup)

1 Objetivo

Estabelecimento de norma para o gerenciamento de cópias de segurança (backup), testes e recuperação de dados, visando preservar a confidencialidade, a integridade e a disponibilidade dos dados, no âmbito do Tribunal Regional do Trabalho da 15ª Região (TRT).

2 Abrangência

Aplica-se aos dados armazenados em meio digital nos arquivos de rede privativos de cada unidade judiciária e administrativa, e nos sistemas e serviços de informação do TRT, quer estejam hospedados no datacenter principal, secundários ou nos servidores de redes das varas de trabalho.

3 Referências legais e normativas

ISO ABNT, 2013, NBR ISO 27001: Sistemas de gestão de segurança da informação, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

ISO ABNT, 2013, NBR ISO 27002: Código de prática para gestão de segurança da informação, que fornece diretrizes para práticas de gestão de segurança da informação.

Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

Resolução Nº 211 de 15/12/2015 do Conselho Nacional de Justiça (CNJ), que Institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

TRT15 - Ato GP Nº 15/2007, de 27 de novembro de 2007. Institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 15ª Região.

4 Diretrizes

4.1 Procedimentos de cópia de segurança

4.1.1 A frequência, tipo, ponto objetivado de recuperação, tempo objetivado de recuperação e período de retenção de cópia de segurança dos sistemas e serviços de informação devem ser definidos pelos Gestores de Serviços de TIC, e dos arquivos de rede privativos pelo Comitê de Governança de TI.

4.1.2 Os procedimentos de cópia de segurança devem considerar os requisitos legais, técnicos e a criticidade dos dados relacionados prioritariamente com a área judicial e área administrativa.

4.1.3 A SETIC é responsável pela definição dos procedimentos de cópia de segurança, podendo a execução ser delegada com anuência do Comitê de Governança de TI.

4.1.4 Os procedimentos de recuperação de cópia de segurança devem ser verificados regularmente, de forma a garantir que estes são efetivos e que podem ser concluídos dentro dos prazos estabelecidos.

4.1.5 Para sistemas críticos, os procedimentos de cópia de segurança devem abranger todas as aplicações, dados, configurações e informações essenciais para a completa recuperação e restauração do sistema, sendo possível igual tratamento para sistemas não críticos, condicionado à viabilidade técnica.

4.1.6 Os procedimentos de cópia de segurança, sempre que possível, devem ser automatizados para facilitar o processo de geração, recuperação das cópias e minimização de erros.

4.1.7 Não é de responsabilidade da SETIC realizar cópia de segurança de dados armazenados em estações de trabalho, notebooks, ultrabooks, tablets e dispositivos de armazenamento portáteis, não sendo garantida sua recuperação em caso de falha nas mídias de gravação desses equipamentos ou de instabilidade no seu sistema operacional.

4.2 Recuperação de dados

4.2.1 As solicitações de recuperação de cópia de segurança de arquivos de rede privativos de cada unidade judiciária e administrativa devem ser encaminhadas formalmente à SETIC, por intermédio da Central de Serviços de TIC.

4.2.2 As solicitações de recuperação de cópia de segurança de sistemas e serviços de informação devem ser encaminhadas, pelo respectivo Gestor de Serviço de TIC à SETIC, por intermédio da Central de Serviços de TIC.

4.2.3 A SETIC deve analisar tecnicamente a solicitação de recuperação de cópia de segurança, justificando em caso da impossibilidade ou inviabilidade de sua realização.

4.2.4 Deve ser formalmente estabelecido e divulgado acordo de nível de serviço para a recuperação de dados pelos Gestores de Serviços de TIC, SETIC e Comitê de Governança de TI.

4.2.5 Nos casos em que a SETIC tiver ciência de eventuais perdas de dados na rede corporativa, deverá agir proativamente buscando a recuperação dos mesmos, notificando os usuários envolvidos.

4.3 Testes de recuperação de dados

4.3.1 A SETIC deve realizar testes periódicos de recuperação de cópia de segurança, visando garantir que as cópias geradas são confiáveis para uso em caso de necessidade.

4.3.2 A periodicidade dos testes de sistemas e serviços de informação deve ser definida conjuntamente pelo Gestor de Serviço de TIC e a SETIC.

4.3.3 A periodicidade dos testes de arquivos de rede privativos de cada unidade judiciária e administrativa deve ser definida conjuntamente pelo Comitê de Governança de TI e a SETIC.

4.3.4 A periodicidade e os testes de recuperação de dados deve considerar os requisitos técnicos e a criticidade dos dados relacionados prioritariamente com a área judicial e área administrativa.

4.3.5 Os resultados dos testes devem ser realizados, de forma documentada, pelas equipes responsáveis, sendo, em caso de sistemas e serviços de informação, validados pelo respectivo Gestor de Serviço de TIC.

4.3.6 Os testes de recuperação devem ser realizados em um local de armazenamento segregado do ambiente original para evitar a sobreposição dos dados.

4.4 Armazenamento e Segurança

As mídias de cópia de segurança devem ser mantidas em uma localidade remota, que possua um nível apropriado de proteção física, lógica e ambiental, além de uma distância suficiente do local principal de armazenamento.