NORMA COMPLEMENTAR 03, DE 11 DE MAIO DE 2021

Dispõe sobre a Política de Backup e Restauração de dados no Instituto Federal do Sertão Pernambucano.

OBJETIVO

Art.1º A Política de Backup e Restauração de dados estabelece diretrizes, critérios, responsabilidades e requisitos básicos para a segurança, proteção e disponibilidade dos dados custodiados pelos setores de tecnologia da Informação das Unidades Organizacionais do IF SERTÃO-PE, definidos formalmente como de obrigatória salvaguarda.

CONCEITOS

Art.2º Para os fins desta Normativa Complementar específica devem ser adotadas as seguintes definições:

I. Administrador de rede: pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

II. Backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

III. Backup completo: modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup.

IV. Backup incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado;

V. Backup diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

VI. Comitê de Governança Digital (CGD): grupo de pessoas com a responsabilidade de determinar e priorizar as ações de Tecnologia da Informação e Comunicação no IF SERTÃO-PE;

VII. Comitê Gestor de Segurança da Informação (CGSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do IF SERTÃO-PE;

VIII. Criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização;

IX. Diretoria de Gestão Tecnologia da Informação (DGTI): órgão executivo que planeja, dirige, avalia e executa as políticas de tecnologia da informação e comunicação (TIC) em todo o IF SERTÃO-PE.

X. Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XI. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

XII. Janela de backup: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIII. Restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

XIV. Retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XV. Rotina de backup: procedimento utilizado para se realizar um backup;

XVI. Sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens.

XVII. Unidade de armazenamento de backup: dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

XVIII. Unidade organizacional: Repartição refere-se à Reitoria e a cada campus do IF Sertão - PE.

XIX. Usuário: pessoa física seja servidor ou equiparado, empregado ou prestador de serviços, aluno e pessoa da sociedade civil habilitada pela administração para acessar os ativos de informação do IF SERTÃO-PE.

DISPOSIÇÕES GERAIS

Art.3º As diretrizes estabelecidas neste documento serão aplicadas em todas as Unidades Organizacionais do IF SERTÃO-PE que tenham dados sob sua guarda.

Art.4º A salvaguarda e recuperação dos dados do IF SERTÃO-PE abrange exclusivamente os sistemas de informação em ambientes de produção e homologados sob custódia dos setores de TI das Unidades Organizacionais, armazenados nos centros de processamento de dados destas repartições.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente nos microcomputadores dos usuários ou em quaisquer outros sistemas fora dos centros de processamento de dados mantidos pelos setores de TI.

Art.5º A salvaguarda e a recuperação dos dados de sistemas de informação custodiados por outras entidades, públicas ou privadas, utilizados pelo IF SERTÃO-PE deverá ser estabelecido em contrato.

DIRETRIZES OPERACIONAIS

Art.6º As rotinas de backup deverão ser orientadas para a restauração das informações no menor tempo possível, principalmente quando houver indisponibilidade dos sistemas que dependam da operação de recuperação de dados e sejam considerados críticos para o IF SERTÃO-PE.

Art.7º Os sistemas de informação críticos às atividades institucionais deverão ser formalmente especificados pelo Comitê de Governança Digital do IF SERTÃO-PE.

Art.8º As rotinas de backup deverão ter requisitos mínimos diferenciados de acordo com o tipo de sistema ou dado salvaguardado, dando prioridade aos sistemas de informação críticos às atividades do IF SERTÃO-PE.

Art.9º Deverão ser utilizadas soluções de backup e restauração adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

Art.10º As cópias de segurança dos sistemas críticos as atividades do IF SERTÃO-PE deverão observar as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal;

IV – anual.

Art.11º Os sistemas de informação críticos às atividades do IF SERTÃO-PE deverão ser resguardados sob os seguintes padrões mínimos, ao qual deverão ser observadas suas correlações frequência/retenção dos dados:

I – diária: 1 semana;

II – semanal: 1 mês;

III – mensal: 1 ano;

IV – anual: 5 anos.

Art.12º Os sistemas de informação não críticos às atividades do IF SERTÃO-PE deverão ser resguardados sob os seguintes padrões mínimos, ao qual deverão ser observadas suas correlações frequência/retenção dos dados:

I – diária ou semanal: 1 mês;

II – mensal: 1 ano;

III – anual: 5 anos.

Art.13º Poderão ser estabelecidos frequência e tempo de retenção diferenciada para cada sistema de informação de acordo com o nível de criticidade desde que respeitados os padrões mínimos estabelecidos.

Art.14º Os sistemas de informação abarcados por esta política deverão ser resguardados sob um padrão mínimo, estabelecido em Planos de Backup e Restauração específicos.

Art.15º Deverão ser registrados pelos administradores de rede, técnicos de TI ou Analistas de TI planos de Backup e Restauração exclusivos aos sistemas sob sua custódia.

Art.16º O Plano de Backup e Restauração deverá conter, ao menos, os seguintes requisitos (vide anexo):

I – Escopo (dados a serem salvaguardados)

II – Tipo de backup (completo, incremental, diferencial);

III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV – Tempo de retenção;

V – Unidade de armazenamento;

VI – Janela de backup;

VI – Estratégia de backup;

VII – Periodicidade de teste de restauração;

VIII – Procedimento de teste de restauração;

IX – Procedimento de restauração.

Art.17º Deverá ser considerado para a execução das rotinas de Backup o seu impacto sobre o desempenho da rede computacional, garantindo que o tráfego necessário para tal evite a indisponibilidade dos demais sistemas da Instituição em horário de expediente.

Art.18º A execução do backup deverá ocorrer, preferencialmente, no período de janela de backup.

Art.19º Deverão ser determinados pelos responsáveis técnicos em conjunto com a Diretoria de Gestão de Tecnologia da Informação (DGTI) os períodos de janela de backup exclusivos aos sistemas sob sua custódia.

Art.20º A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá atender as seguintes características dos dados resguardados:

I – a criticidade;

II – o tempo de retenção;

III – a probabilidade de necessidade de restauração;

IV – o tempo esperado para restauração;

V – o custo de aquisição da unidade de armazenamento de backup;

VI – a vida útil da unidade de armazenamento de backup.

Art.21º Deverá ser identificada a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada cenário.

Art.22º Poderão ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados não seja expressivo.

Art.23º As unidades de armazenamento das cópias de segurança deverão ser acondicionadas em locais apropriados, seguros e com acesso restrito a pessoas autorizadas.

Art.24º As cópias de segurança deverão ser submetidas a testes de recuperação inicialmente ao serem programadas em soluções de backups e posteriormente realizar outros testes não excedendo 01 (um) ano para sistemas críticos.

Art.25º Os testes de restauração das cópias de segurança deverão ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis em cada repartição do IF SERTÃO-PE.

Art.26º As unidades de armazenamento consideradas inservíveis ou defeituosas deverão passar por procedimentos que impossibilitem a recuperação de dados por terceiros, devendo o descarte ser registrado.

RESPONSABILIDADES

Art.27º São atribuições dos responsáveis pela execução e gestão das rotinas de *backup* e restauração:

I. Planejar os recursos necessários para implantar a política e os planos de *backup* e restauração;

II. Propor soluções de cópia de segurança das informações produzidas ou custodiadas pelas Unidades Organizacionais do IF SERTÃO-PE;

III. Providenciar a criação e manutenção das cópias de segurança;

IV. Configurar as soluções de *backup*;

V. Manter as unidades de armazenamento de *backups* funcionais, preservadas e seguras;

VI. Solicitar suporte de terceiros em caso de falha nas unidades de armazenamento;

VII. Elaborar o Plano de *backup* e restauração específico;

VIII. Verificar periodicamente os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;

IX. Tomar medidas preventivas para evitar falhas;

X. Reportar imediatamente os incidentes ou erros que causem indisponibilidade ou que impossibilitem a restauração das cópias de segurança;

XI. Gerenciar mensagens e registros de auditoria (LOGs) dos *backups*;

XII. Providenciar a execução dos testes de restauração;

XIII. Restaurar ou recuperar as cópias de segurança em caso de necessidade.

DISPOSIÇÕES FINAIS

Art.28º A Política de *backup* e restauração dos dados deverá ser divulgada.

Art.29º Esta norma poderá ser revisada a qualquer tempo, quando identificada a necessidade de alteração, não excedendo o período máximo de 04 (quatro) anos.

Art.30º A ETIR tomará as providências necessárias para a adequação das rotinas e dos procedimentos de *backups* definidos nesta norma complementar junto aos respectivos responsáveis técnicos dos sistemas.

Art.31º Caberá ao Comitê Gestor de Segurança da Informação esclarecer os casos omissos a esta Norma.

Art.32º Esta normativa entra em vigor a partir da data de sua publicação

Anexo

PLANO DE *BACKUP* E RESTAURAÇÃO

1. ESCOPO/ABRANGÊNCIA
<quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders>

2. FREQUÊNCIA DE REALIZAÇÃO
<diário, semanal, mensal, anual>

3. TIPO DE CÓPIA A SER REALIZADA
<completa/full, incremental ou diferencial>

4. TEMPO DE RETENÇÃO
<Observar a correlação frequência/retenção de dados declarados na Política>

5. UNIDADE DE ARMAZENAMENTO
<Informar mídia de armazenamento em local seguro diferente do local original>

6. JANELA DE *BACKUP*
<Informar período no qual a execução das cópias de segurança deverá ocorrer preferencialmente>

7. ESTRATÉGIA DE *BACKUP*
<Detalhar o esquema de realização das cópias de segurança; Informar quais tecnologias e equipamentos será utilizado neste esquema; Informar a capacidade necessária para os dados a serem copiados/armazenados; Informar quando deve ser agendada a geração de *backups*; Informar os responsáveis pela execução e acompanhamento>

8. PERIODICIDADE DE TESTE DE RESTAURAÇÃO
<Informar período regular de teste de restauração/recuperação (*restore*) das cópias de segurança>

9. PROCEDIMENTO DE TESTE DE RESTAURAÇÃO
<Detalhar quais os procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento)>

10. PROCEDIMENTO DE RESTAURAÇÃO
<Detalhar quais os procedimentos para realizar a recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o "como" recuperar os *backups*)>

11. ASSINATURAS

<Assinatura dos responsáveis pela execução e gestão das rotinas de *backup*>

_____

Nome:
Cargo/Função:
Data: <dd/mm/aaaa>

Assinado digitalmente por:
Andson da Silva Rodrigues
andson_rodrigues@ifsertao-pe.edu.br
SIAPE 2009529
2021.05.11 17:01:02 BRT

_____

APROVAÇÃO
Presidente do Comitê Gestor de Segurança da Informação