Política de Backup e Restauração

Sumário

1. Preâmbulo

1.1. Para garantir a continuidade das operações da ON LINE ENGENHARIA DE SISTEMAS LTDA., é essencial adotar mecanismos eficazes de proteção e recuperação de dados. Esses mecanismos devem assegurar a integridade, disponibilidade e confidencialidade das informações, mesmo diante de incidentes como erros humanos, ataques cibernéticos, desastres naturais ou outras ameaças.
Com esse objetivo, o presente documento estabelece a **Política de Backup e Restauração de Dados**, definindo os procedimentos, a frequência e os meios para a realização de cópias de segurança dos dados armazenados nos sistemas computacionais da empresa, bem como os critérios para sua restauração em caso de necessidade.

2. Objetivos

2.1. Regulamentar a política de backup das informações eletrônicas no âmbito da ON LINE ENGENHARIA DE SISTEMAS LTDA., com o objetivo de estabelecer diretrizes para os processos de cópia e armazenamento de dados, visando assegurar a segurança, integridade e disponibilidade das informações, em conformidade com a Política de Segurança da Informação.

3. Definições

3.1. Para o disposto neste documento considera-se:

> I – Administrador de Backup: colaborador do quadro da ON LINE ENGENHARIA DE SISTEMAS LTDA, responsável pelos procedimentos de configuração, execução, monitoramento e testes relacionados as rotinas de backup e restauração;

II – Administrador de Recurso: colaborador do quadro da ON LINE ENGENHARIA DE SISTEMAS LTDA, responsável pela administração de ativo de TIC(Tecnologia da Informação e Comunicação), físicos ou virtuais, sob responsabilidade da empresa;
III – Backup Completo (Full): modalidade de backup na qual os dados selecionados são copiados integralmente;
IV – Backup Diferencial: modalidade de backup na qual são copiados apenas os arquivos novos ou alterados desde o último backup completo;
V – Backup Incremental: modalidade de backup na qual somente os arquivos novos ou alterados desde a última execução do backup - seja ele completo, diferencial ou incremental.
VI – Clientes de backup: todos os equipamentos servidores nos quais são instalados o agente de backup;
VII – Recuperação de Desastre: conjunto de estratégias e procedimentos para recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
VIII – Mídia: meio físico ou virtual utilizado para armazenar os dados copiados em uma rotina de backup;
IX – Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;
X – Objeto: qualquer dado, arquivo ou conjunto de informações passível de ser incluída em uma rotina de backup e posterior restauração;
XI – Tarefa de Backup: processo automatizado executado sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção.

4. Referências

4.1. A presente política tem como referências:

I – A Política Corporativa de Segurança da Informação, que estabelece diretrizes e controles internos voltados à proteção dos ativos informacionais da organização;
II – A norma **ABNT NBR ISO/IEC 27001:2013**, que define os requisitos para a implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI), com base em uma abordagem de riscos;
III – A norma **ABNT NBR ISO/IEC 27002:2013**, que fornece um conjunto de controles e práticas recomendadas para a gestão da segurança da informação, complementando os requisitos estabelecidos pela ISO/IEC 27001;
IV – A **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)**, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

5. Responsabilidade e Atribuições

5.1. O Departamento de Tecnologia da Informação (TI), atuara como Administrador de Backup, sendo responsável pela definição, implementação e manutenção da política e dos procedimentos relacionados aos serviços de backup e restauração dos dados. Compete ainda ao departamento o gerenciamento seguro das mídias moveis utilizadas, bem como a garantia do cumprimento das normas internas e regulamentações aplicáveis.

5.2. São atribuições do Administrador de Backup:

I – Propor melhorias continuas na política de backup, com base em requisitos técnicos, legais e operacionais;

II – Planejar, configurar e manter as rotinas de backup conforme os níveis de criticidade dos ativos de informação;
III – Configurar e manter operacional a solução de backup, incluindo agentes/clientes nos dispositivos-alvos;
IV – Gerenciar a criação, rotatividade e manutenção das mídias, quando aplicável;
V – Realizar testes periódicos de backup e restauração para validar a integridade e a eficácia dos dados;
VI – Implementar mecanismos de notificação e geração de relatórios de execução de falhas;
VII – Monitorar regularmente os relatórios de backup avaliando falhas e inconformidades;
VIII – Executar processos de restauração de dados sempre que houver demanda autorizada;
IX – Analisar e tratar mensagens e logs gerados pelas rotinas de backup, garantindo a continuidade dos processos e a mitigação de erros;
X – Realizar manutenções preventivas e corretivas nos dispositivos de backup, quando aplicável;
XI – Realizar o carregamento e gerenciamento das mídias necessárias para a execução dos backups agendados;
XII – Comunicar ao Administrador do Recurso quaisquer falhas, inconsistências ou ocorrências críticas identificadas durante as rotinas de backups;
XIII – Assegurar o armazenamento seguro das mídias de backup em local apropriado, com controle de acesso e proteção contra ameaças físicas e logicas.

6. Escopo do backup e sua formalização

6.1. Todo ativo de Tecnologia da Informação e Comunicação (TIC), que armazene dados deverá ser avaliado quanto a sua inclusão nas rotinas de backup, considerando seu nível de criticidade e impacto em caso de perda de informação.
6.1.1. O Administrador de Recursos será responsável por definir os diretórios e arquivos a serem incluídos de backup, observando como prioridade:

a) Arquivos de configuração de sistemas operacionais e aplicativos instaladas em servidores;
b) Arquivos de log gerados por aplicações, incluindo registros da ferramenta de backup e restauração;
c) Informações e parâmetros de configuração de banco de dados;
d) Conteúdo armazenados em repositórios de dados vinculados a sistemas;
e) Arquivos institucionais de usuários, como planilhas, documentos e e-mails;
e) Arquivos de sistemas e aplicações desenvolvidas pela ON LINE ENGENHARIA DE SISTEMAS LTDA, ou quaisquer outros cuja perda possa acarretar prejuízos operacionais, legais ou financeiros a organização.

6.2. O Administrador de Backup ou o Administrador de Recurso que solicita a inclusão de um cliente no processo de backup, deverá identificar e excluir da rotina, tendo como referência:

a) Arquivos pertencentes ao sistema operacional ou de aplicações que possam ser reinstalados a partir de fontes oficiais;
b) Arquivos temporários, caches ou arquivos que não exigem retenção.

6.3. Para o backup de aplicações e/ou bancos de dados, deverão ser observadas rigorosamente as recomendações técnicas do desenvolvedor ou fabricante da solução, a fim de garantir a consistência dos dados e a eficácia do processo de restauração.

6.4. Os procedimentos de backup deverão ser revisados e atualizados sempre que ocorrerem as seguintes situações:

I – Desenvolvimento ou implantação de novas aplicações;
II – Alteração nos novos locais de armazenamento de arquivos e dados;
III – Instalação de novos bancos de dados;
IV – Adição de novos aplicativos instalados;
V – Inclusão de novas informações consideras críticas para continuidade dos negócios.

6.5. Para solicitar a inclusão de um recurso no processo de backup, o Administrador de Recursos deverá formalizar a demanda por meio da ferramenta oficial de controle de chamados técnicos. A solicitação deve conter, obrigatoriamente, as seguintes informações:

a) Identificação do servidor ou equipamento;
b) Diretórios e arquivos a serem incluídos na rotina de backup;
c) Outras observações relevantes;

6.5.1. A configuração das rotinas de backup deverá ser realizada pelo Administrador de Backup na ferramenta apropriada, com base nas especificações detalhadas no chamado técnico, respeitando as diretrizes e os padrões definidos nesta política.

7. Retenção e Manutenção das Mídias de Backup

7.1. Os backups deverão ser mantidos conforme os seguintes prazos de retenção, de acordo com sua periodicidade:

I – Backup diário: conservar as copias dos últimos 10 dias;
II – Backup semanal: conservar as copias das últimas 06 semanas;
III – Backup mensal: conservar as copias dos últimos 60 últimos meses;
IV – Backup semestral: retenção permanente;

7.1.1. Após o termino do prazo de retenção estabelecido, as mídias utilizadas poderão ser:

a. Reutilizadas, desde que estejam em condições adequadas de funcionamento e dentro do ciclo seguro de leitura/gravação;
b. Destruídas, caso apresentem desgaste físico, obsolescência tecnológica ou risco à integridade dos dados.

7.2. Nenhuma mídia física deverá ultrapassar 30 anos de armazenamento. Atingindo esse limite, os dados deverão ser copiados para nova mídia compatível, e a mídia original deverá ser destruída de forma segura e descartada em local apropriado, em conformidade com as legislações ambientais vigentes e políticas internas de descarte de ativos.

7.2.1 A atualização tecnológica das mídias de backup deverá ser realizada sempre que necessário, com o objetivo de preservar a acessibilidade, integridade e legibilidade dos dados, mitigando riscos de obsolescência de hardware ou software.

8. Execução, Monitoramento e Frequência dos Backups

8.1. Os processos de backup deverão ser observar os seguintes critérios operacionais, conforme sua periodicidade e etapa de execução:

I – Criação de backups:

a) As rotinas de backup deverão ser programadas para execução automática, preferencialmente em horários de menor uso dos sistemas, a fim de minimizar o impacto na performance operacional e no trafego da rede.

II – Operação e Monitoramento:

a) A execução das rotinas de backup deverá ser monitorada continuamente pelo Operador NOC (Network Operations Center);
b) A ferramenta de backup deverá gerar extratos automatizados de cada operação realizada. Esses relatórios deverão ser encaminhados por e-mail ao Administrador de Backup;
c) Em caso de falhas na execução, o Operador NOC deverá criar a ocorrência em relatório especifico, contendo a identificação dos clientes de backup afetados e eventuais ações corretivas adotadas. Falhas não resolvida deverão ser encaminhadas ao Administrador de backup para tratativas imediatas.

8.2. As rotinas de backups deverão seguir, preferencialmente, a seguinte frequência e modo de execução:

I – Os backups diários:

- Executados de segunda à sexta-feira, entre 18h e 6h do dia seguinte;
- Devem ser realizados em modo incremental;

II – Em caso de falha na execução de qualquer rotina de backup ou impossibilidade técnica momentânea, serão adotadas pelo Administrador de Backup medidas corretivas visando a proteção da integridade das informações, tais como:

- Re-execução do processo em horário comercial;
- Copia manual dos dados para repositório seguro.
- Adoção de procedimentos compatíveis com ambiente tecnológico.

9. Recuperação de Backups

9.1. A recuperação de dados a partir de backups deverá seguir as diretrizes abaixo, assegurando rastreabilidade, controle e integridade do processo.

9.1.1 A solicitação de restauração de arquivos ou dados deverá ser formalizada exclusivamente, pelo Administrador de Recursos responsável, por meio de chamado técnico aberto na central de chamados da organização.

9.2. O chamado técnico deverá conter, obrigatoriamente, as seguintes informações:

- Nome completo e setor do usuário semelhante;
- Identificação precisa do (s) objeto (s) a ser (em) recuperado (s) (ex.: nome de arquivos, pastas, banco de dados);
- Localização original dos dados (ex.: caminho do diretório, servidor, unidade de armazenamento);
- Data ou período a ser recuperado;

9.3. O chamado será encaminhado ao Administrador do Backup, que realizara a restauração conforme os critérios técnicos estabelecidos. Após a conclusão do procedimento deverá:

- Registrar no chamado os detalhes da ação executada;
- Informar o sucesso ou falha da operação;

Encerrar o chamado com a devida documentação da restauração realizada;

9.4. A restauração de objetos estará limitada aos dados efetivamente contemplados pela estratégia vigente de backup, conforme periodicidade, escopo e tipo de cópia definida. Dados fora desse processo não poderão ser recuperados.

10. Teste de confiança

10.1. Os backups mensais e semestrais deverão ser testados quanto à integridade e recuperabilidade dos dados, com base em amostragem representativa, no prazo máximo de 7(sete) dias, após a sua execução.
10.1.1 Caso seja identificada qualquer falha na integridade, inconsistência ou incompletude nos dados testados, um novo backup deverá ser imediatamente executado, garantindo a substituição da cópia anterior por uma versão valida e integra.
10.1.2. Para cada teste de confiança realizado, deverá ser elaborado um relatório técnico contendo:

- Identificação da mídia/teste;
- Objeto (s) recuperados(s);
- Resultado do teste(sucesso, falha parcial, falha critica);
- Ações corretivas, aplicáveis;
- Responsável pela execução;

11.Recuperação de desastre

11.1 As cópias de segurança destinadas ao processo de Recuperação de Desastres (Disaster Recovery – DR), serão geradas com base na replicação das mídias dos backups semestrais. Essa copias deverão ser armazenadas no Centro de Processamento de Dados (CPD) ou, preferencialmente, em lugar remoto, com controle de acesso restrito, proteção ambiental e conformidade com requisitos de segurança física e logica.

11.1.1. A criação das mídias de Recuperação de Desastres será realizada somente após a conclusão e validação bem-sucedida dos testes de integridade do backup (conforme item 10), e terá um prazo de retenção de 06 (seis) meses.

11.2. Toda e qualquer intervenção programada em servidores ou dispositivos de armazenamento que represente risco potencial a integridade, disponibilidade ou funcionamento dos ativos de TCI deverá ser precedida da execução de backup completo e atualizado dos dados armazenados nos referido equipamentos.

12. Descarte das mídias

12.1. O descarte de mídias de backup consideradas inservíveis, danificadas ou fora do ciclo de uso seguro será de responsabilidade do Departamento de TI, e deverá ser realizado mediante solicitação formal do Administrador de Backup.

12.1.1. Todas as mídias de backup destinadas ao descarte deverão ser submetidas a processo de destruição física ou lógica definida, de forma a garantir:

- A irreversibilidade da leitura dos dados previamente armazenados;
- A inviabilidade de reutilização da mídia;
- A conformidade com a Política de Segurança da Informação da organização;
- A observância dos princípios da Lei Geral de Proteção de Dados (LGPD) quanto a eliminação segura de dados pessoais.

12.1.2. O processo de descarte deverá ser documentado por meio de termo de descarte de mídia, contendo:

- Identificação da mídia (número de série, tipo, capacidade);
- Data do descarte;
- Responsáveis pela autorização e execução;

- Método de destruição utilizado (ex.: trituração, desmagnetização, destruição térmica);
- Assinatura dos envolvidos.

13. Disposições finais

13.1 Esta política deverá ser revisada periodicamente, com intervalo máximo de 02 (dois) anos ou sempre que houver alterações significativas nos requisitos legais, normativos, tecnológicos ou organizacionais que impactem direta ou indiretamente os processos de backup, restauração ou segurança da informação decorrentes de atualizações:

- Da legislação vigente (LGPD, Marco Civil da Internet);
- De normas técnicas (ABNT NBR ISSO/IEC 27001/27002);
- De infraestrutura de TI (adoção de novas tecnologias, ferramentas ou ambientes computacionais);

13.2. Esta política poderá ser complementada por normas, instruções normativas, manuais operacionais ou procedimentos técnicos específicos, conforme necessidade identificada pela equipe técnica ou por deliberação da Direção do CPD.

13.3. Situações excepcionais ou não previstas neste documento serão analisadas e deliberadas pela Direção do Centro de Processamento de Dados (CPD), em conjunto com os responsáveis técnicos e jurídicos competentes, quando aplicável.