



# Norma de Gestão de Backup

## SUMÁRIO

1. OBJETIVO.....	3
2. CAMPO DE APLICAÇÃO.....	3
3. DEFINIÇÕES.....	3
4. PAPÉIS E RESPONSABILIDADES .....	4
4.1. Usuários e Clientes de TI.....	4
4.2. Equipe de Infraestrutura de TI .....	4
4.3. Encarregado de Segurança da Informação (ESI) .....	4
5. DOCUMENTOS DE REFERÊNCIA .....	4
6. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO.....	5
6.1 Regras gerais .....	5
6.2 Procedimentos de Backup .....	5
6.3 Formas e geração dos backups .....	7
6.4 Retenção .....	8
6.5 Restauração .....	8
6.6 Teste de Restauração.....	9
7. EVIDÊNCIAS GERADAS.....	9
8. TABELA ORIENTATIVA PARA GERAÇÃO DOS BACKUPS .....	9
7. DOCUMENTOS DE REFERÊNCIA .....	10
8. REGISTRO DE ALTERAÇÕES .....	10
9. FORMALIZAÇÃO.....	10

## 1. OBJETIVO

Esta Norma define as regras e os procedimentos para gestão de backup atendidos pela Equipe de Infraestrutura de Bennercloud com ênfase especial aos processos de backup

## 2. CAMPO DE APLICAÇÃO

Aplicável a todos os colaboradores, próprios ou terceiros, que utilizam recursos de TI fornecidos pelo **Grupo Benner\*** para o exercício de suas atividades.

\* Denominação utilizada para designar as empresas: Benner Sistemas S.A., Benner Tecnologia e Sistemas em Saúde Ltda., Benner Tecnologia e Serviços em Saúde Ltda., Otto HX Tecnologia e Sistemas Ltda e Itessa Tecnologia e Serviços S.A.

## 3. DEFINIÇÕES

- **Backup** – Cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes. O termo também pode ser associado ao processo de geração da cópia de segurança, acepção que tem no restore seu complemento (vide restore).
- **Backup Full** – Backup de todos os dados contemplados na rotina de backup.
- **Bucket OCI** – Um bucket OCI é um contêiner de armazenamento usado para armazenar dados na OCI (Oracle Cloud Infrastructure).
- **Dado** – Qualquer registro de conteúdo armazenado em meio magnético. Pode compreender software, dados propriamente ditos (arquivos, bancos de dados), conteúdo multimídia ou qualquer outro passível de armazenamento em meio magnético.
- **Janela de Backup** – Período requerido para a geração do backup.
- **Job** – É um arquivo que contém instruções ou comandos para realizar uma determinada tarefa ou trabalho de forma automatizada em um servidor.
- **Log** – Resultado gerado após a realização do backup ou restore.
- **OCI** – A Oracle Cloud Infrastructure (OCI) é uma plataforma de nuvem pública oferecida pela Oracle Corporation.
- **Restore** – Restaurar (Restore) processo de recuperação, a partir de cópias de segurança, de dados ou arquivos gravados em disco. Visa retornar uma situação anterior para teste ou simulação do ambiente.

- **Servidor** – Computador responsável por gerenciar e oferecer serviços para uma rede de computadores clientes.
- **SGBD** – O Sistema de Gerenciamento de Banco de Dados é um software projetado para permitir a criação, o armazenamento, a manipulação e a recuperação de dados de forma eficiente e segura.

## 4. PAPÉIS E RESPONSABILIDADES

### 4.1. Usuários e Clientes de TI

Providenciar a abertura de um chamado no sistema Siscon, caso identifique qualquer anormalidade no uso dos recursos de TI que lhe forem disponibilizados ou que estejam em desacordo com a Política de Segurança da Informação e a Política de Privacidade da Empresa.

### 4.2. Equipe de Infraestrutura de TI

Analisar os chamados abertos pelos Usuários e Clientes; classificar e atender os chamados relacionados à sua área de atuação; manter os usuários informados a respeito do andamento das solicitações; manter os registros e os controles de TI atualizados.

### 4.3. Encarregado de Segurança da Informação (ESI)

Avaliar os incidentes de segurança da informação e nomear um Ponto Focal responsável por sua tratativa; suportar junto ao Ponto Focal as decisões a serem tomadas para resolução do incidente; notificar o DPO nos casos de incidentes de segurança da informação que envolvam dados pessoais; manter o CSI, o DPO e demais partes interessadas cientes a respeito das informações e decisões envolvendo incidentes de segurança da informação; identificar e obter autorizações e aprovações, quando necessárias para tratativa de incidentes de segurança da informação.

## 5. DOCUMENTOS DE REFERÊNCIA

O presente documento será complementado pela Política de Segurança da Informação e demais Normas de Segurança da Informação do GRUPO BENNER e está em consonância com a norma ABNT NBR ISO/IEC 27002:2013 – “Código de prática para controles de

segurança da informação”, a Lei n.º 12.965 de 2014 (Marco Civil da Internet) e com a legislação vigente no Brasil.

## **6. DIRETRIZES DA SEGURANÇA DA INFORMAÇÃO**

### **6.1 Regras gerais**

- 6.1.1 A execução de backups das informações e dos sistemas devem, essencialmente, garantir a proteção do atributo da disponibilidade;
- 6.1.2 Devem ser igualmente preservadas a confidencialidade e a integridade dos backups realizados;
- 6.1.3 Para que seja possível atender às diferentes necessidades de salvaguarda de informações e sistemas, os backups serão executados mediante o emprego de variadas;
- 6.1.4 Ferramentas, tais como, mas não se limitando a, jobs, scripts, robôs, servidores, storage e softwares de gerenciamento de rotinas de backup;
- 6.1.5 A necessidade de execução do backup deve ser definida a partir:
- 6.1.6 Da criticidade da disponibilidade de uma informação ou sistema para a normalidade e continuidade dos processos de negócio e operacionais do BENNERCLOUD, mediante a classificação realizada;
- 6.1.7 Dos requisitos legais, fiscais e de auditoria para a guarda de informações.

### **6.2 Procedimentos de Backup**

- 6.2.1 A Gerência de Tecnologia da Informação é responsável por definir e executar os procedimentos e manuais operacionais específicos, de acordo com as características das informações, dos sistemas e das ferramentas de geração de backup, para:
- 6.2.2 A construção e programação de execução de backups automatizados;
- 6.2.3 O desempenho das atividades manuais relacionadas à execução dos backups;
- 6.2.4 A rotulação, catalogação e o método de rodízio dos diferentes tipos de backups;
- 6.2.5 O registro e auditoria da execução bem-sucedida dos backups;

- 6.2.6 O registro, análise e solução das falhas de execução dos backups;
- 6.2.7 O teste ou a verificação de consistência para a validação dos backups realizados;
- 6.2.8 A recuperação (restore) das informações contidas nos backups realizados;
- 6.2.9 A instalação, configuração e manutenção das ferramentas para geração de backups;
- 6.2.10 O controle da disponibilidade e da vida útil das mídias novas e já utilizadas, incluindo a previsão orçamentária para aquisição esporádica de novas mídias ou formatos de backup;
- 6.2.11 O controle da capacidade da memória e espaço em disco de storages;
- 6.2.12 O armazenamento seguro e ambientalmente adequado em instalações locais e remotas das mídias, incluindo a eventual geração de backups redundantes como suporte às estratégias de contingência operacional e de continuidade de negócios;
- 6.2.13 Utilização de criptografia e restrição de acesso ao material salvaguardado, de acordo com as Normas para Classificação e Tratamento da Informação, de modo a evitar incidentes de segurança através do conjunto de dados reunido por este processo;
- 6.2.14 O descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciados e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.
- 6.2.15 Todo procedimento de geração de backups deve especificar e definir previamente:
  - 6.2.16 Quais as informações e sistemas que devem ser salvaguardados;
  - 6.2.17 O local onde as informações e os sistemas se encontram armazenados ou instalados;
  - 6.2.18 O nível de acesso necessário para que os backups automatizados sejam capazes de acessar e reproduzir as informações ou os sistemas;
  - 6.2.19 A frequência da geração dos backups;
  - 6.2.20 As ferramentas de backup disponíveis, além dos tipos de mídias que serão empregadas;
  - 6.2.21 O mapeamento da estimativa de duração média das execuções completa (Total) e parcial (Incremental ou Diferencial) do backup, considerando o tamanho do conteúdo (incluindo, eventualmente, a taxa de crescimento esperada) frente à capacidade de

processamento e velocidade de comunicação dos Recursos Computacionais e das ferramentas específicas envolvidas;

6.2.22 Os períodos ideais para execução do backup, considerando o período de menor carga de utilização e impacto aos processos operacionais (Janela de Execução);

6.2.23 As medidas alternativas ou de contorno para os casos em que a execução do backup ultrapasse a previsão da Janela de Execução ou naqueles em que ela falhe parcial ou completamente.

6.2.24 O backup de arquivos ou conteúdo de estações de trabalho individuais é responsabilidade da Gerência de Tecnologia da Informação, que deve definir os procedimentos e as documentações operacionais para:

6.2.25 O encaminhamento, registro e arquivamento das solicitações de backups específicos por colaboradores ou gestores;

6.2.26 A análise da pertinência da solicitação e os requisitos de aprovação aplicáveis; e

6.2.27 O desempenho das atividades operacionais relativas à reprodução do conteúdo e, quando necessário, de transposição em mídia e entrega ao solicitante.

### 6.3 Formas e geração dos backups

Os backups podem ter as seguintes formas de execução:

6.3.1 **Total (Full):** salvaguarda completa de todo o conteúdo;

6.3.2 **Diferencial:** salvaguarda apenas das informações modificadas ou geradas após a última salvaguarda Total realizada; ou

6.3.3 **Incremental:** salvaguarda apenas das informações modificadas ou geradas após a última salvaguarda Incremental ou Total realizada

A inexistência de critérios específicos para a criação de backups implica na adoção dos seguintes critérios de recorrência e retenção:

6.3.4 **Diária:** executada na modalidade "Total Full";

6.3.5 **Semanal:** executada na modalidade "Total Full", aos sábados, exceto no último sábado do mês, quando é processado o backup mensal;

6.3.6 **Mensal:** executada na modalidade "total", no último domingo do mês

## 6.4 Retenção

6.4.1 As mídias físicas ou digitais e/ou demais recursos utilizados para armazenamentos dos dados salvaguardados devem ser acondicionados em ambiente separado do de produção, devidamente protegidos contra riscos físicos, como incêndios, intempéries, líquidos, radiação e outras ameaças que possam comprometer a integridade das mídias ou das informações lá contidas;

6.4.2 O meio de armazenamento deve manter condições ideais para as mídias lá mantidas, dentro das recomendações técnicas específicas e melhores práticas de mercado;

## 6.5 Restauração

As atividades de restauração é responsabilidade da Gerência de Tecnologia da Informação, que deve definir os procedimentos e os manuais operacionais para:

6.5.1 Mapeamento da estimativa de duração média para a recuperação completa dos backups ou de determinados conteúdos solicitados, considerando o seu tamanho, frente à capacidade de processamento e velocidade de comunicação dos Recursos Computacionais e das ferramentas específicas de backup envolvidas;

6.5.2 Encaminhamento, registro e arquivamento das solicitações de restauração por colaboradores ou gestores;

6.5.3 Análise da pertinência da solicitação e os requisitos de aprovação aplicáveis;

6.5.4 Desempenho das atividades operacionais relativas à recuperação do conteúdo solicitado e de encaminhamento ao solicitante inclusive, quando necessário, mediante transposição em mídia; e

6.5.5 Garantir que todas as atividades realizadas no processo de restauração disponham de controles de segurança compatíveis, especialmente no que tange ao trânsito e



manuseio de mídias, além da eliminação segura de qualquer conteúdo temporário ou transitório eventualmente gerado.

## 6.6 Teste de Restauração

- 6.6.1 Semanalmente serão realizados testes de restauração de dados, que devem ser baseados em dados pré-selecionados dos backups gerados, visando garantir a efetividade, eficiência e confiabilidade do procedimento;
- 6.6.2 Os resultados dos testes devem ser validados, de forma documentada;
- 6.6.3 O responsável por segurança da informação pode solicitar a realização de testes específicos aleatoriamente, a seu critério.

## 7. EVIDÊNCIAS GERADAS

- **Sistema Siscon:** registro dos chamados abertos pelos Usuários e Clientes, posteriormente classificados como Incidentes.
- **NGI RISI – Relatório** de Incidente de Segurança da Informação preenchido e anexado no sistema Siscon para todo chamado classificado como incidente de segurança da informação.
- **Indicador:** Incidentes de SI e de violação de privacidade no período.

## 8. TABELA ORIENTATIVA PARA GERAÇÃO DOS BACKUPS

TABELA					
ITENS	ORIGENS	TIPO DE BACKUP	PERIODICIDADE	RETENÇÃO	JANELA DE BACKUP
Databases	Base de dados dos clientes	Backup FULL	Diária	7 dias	20:00hrs ≅ 06:00hrs
Repositório de arquivos sistemas Benner (BDOC)	Arquivos de anexo aos sistemas Benner com a função de Benner documentos (BDOC)	Backup FULL	Diária	7 dias	20:00hrs ≅ 06:00hrs
Instalação do Sistema	Discos de Instalação do sistema Benner	Backup FULL	Diária	7 dias	20:00hrs ≅ 06:00hrs
Servidores Virtuais (VMI)	Backup dos servidores virtuais (Windows, Linux) dos clientes	Backup FULL	Semanal (Domingo)	4x ao mês	20:00hrs ≅ 06:00hrs

## 7. DOCUMENTOS DE REFERÊNCIA

PSI - Política de Segurança da Informação

MSI - Manual de Segurança da Informação

NGA - Norma de Gestão de Ativos de TI

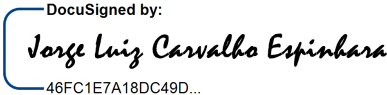

Plano de Resposta a Incidentes Envolvendo Dados Pessoais

Plano de Resposta a Incidentes Envolvendo Ransomware

## 8. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapa	Responsável
01	11/01/2024	Emissão do documento	Jorge Espinhara

## 9. FORMALIZAÇÃO

Elaboração	Aprovação
<b>Jorge Espinhara – Governança de TI</b>   46FC1E7A18DC49D...	<b>Severino Benner - Presidente</b>   B5112A47CD594F7...