

Política de Salvaguarda de informação (backup)

Gabinete de Tecnologia de Informação (GTI)

Sede, Versão 2

Versão	Data da Emissão	Entrada em Vigor	Aprovado	Entidade Responsável
02	31/03/2021		Comissão Executiva (CE)	GTI

Histórico de revisões

Versão	Revisor	Revisão	Proxima revisão
02	Arson Ribisse	Adição do Wemake (SGSI) no cronograma de Backup Removido: O ERP Primavera, sistema de gestão de recursos humanos;	30/04/2023



INTRODUÇÃO

A presente política estabelece as directrizes para a gestão do processo de armazenamento, recuperação e segurança de dados gerados nos vários sistemas da Indico Seguros.

- a) A Unidade Orgânica responsável por esta política é a Gabinete de Tecnologias de Informação (GTI);
- b) Esta política deverá ser revista anualmente para aferir a sua eficácia e a sua conformidade com as melhores práticas. Quaisquer modificações têm necessariamente que ser aprovadas pela Comissão Executiva CE mediante proposta do GTI;

OBJECTO

Constitui objecto desta política os dados gerados pelos servidores e equipamentos de produção:

- O KIT, a aplicação core para a gestão do *core business* (produção, sinistros, gestão de valores, resseguro, custos de aquisição, comissões e demais aspectos da conta técnica);
- O CHEGUS, o sistema de gestão do seguro de saúde;
- O ERP PHC, CRM de avaliação de desempenho, gestão de fornecedores, pagamentos e qualidade;
- SAGE – Accpack, sistema de contabilidade;
- Servidores (Domínio, de aplicações, de ficheiros, Web);
- WeMake - sistema de Gestão de Segurança da Informação
- • SGCN – Sistema de Gestão de Continuidade de Negócio - permite a gestão, de forma estruturada da Documentação (manuais, planos e políticas operacionais, procedimentos, processos, modelos, relatórios e a declaração de aplicabilidade), Incidentes de Segurança da Informação, Auditorias ISO 27001, Gestão de Planos de Ações (Planos de melhoria, planos de continuidade de negócio), e Avaliação de Riscos

Os procedimentos de backup de dados incluem:

- Cronograma e descrição / retenção / registro / teste da backup.
- Tratamento de erros e backups com falha.
- Acesso ao backup.
- Procedimentos de retenção e destruição de backup.
- Procedimento para restauração e Teste de backup.
- Procedimentos de recuperação para activos de TI críticos.

Cópias de segurança de informações, software e imagens do sistema são realizadas e testadas regularmente de acordo com o tabela 1 de cronograma de backup.

A política de backup define os requisitos de retenção e proteção.

CRONOGRAMA E DESCRIÇÃO DE BACKUP

O plano de backup descrito na tabela, são considerados os seguintes itens:



- a) Registos precisos e completos das cópias de backup e procedimentos de restauração documentados deve ser produzido;
- b) A extensão (por exemplo, backup completo ou diferencial) e a frequência dos backups devem refletir os requisitos do negócio, os requisitos de segurança das informações envolvidas e a criticidade das informações para a operação continuada da organização;
- c) Os backups devem ser armazenados em local remoto (cloud), a uma distância suficiente para escapar de qualquer dano de um desastre no site principal;
- d) As informações de backup devem receber um nível adequado de protecção física e ambiental;
- e) Os suportes de backup devem ser testados regularmente para garantir que seja confiável para uso em emergência quando necessário; isso deve ser combinado com um teste dos procedimentos de restauração e verificado contra o tempo de restauração necessário. Testar a capacidade de restaurar dados de backup deve ser realizado em suporte de teste dedicada, não sobrescrevendo o suporte original no caso de backup ou o processo de restauração falha e causa danos ou perda de dados irreparáveis;
- f) Em situações onde a confidencialidade é importante, os backups devem ser protegidos por meio de criptografia.

É efectuada monitoração da execução de backups de modo a resolver as falhas de backups para garantir a integridade dos backups de acordo com esta política de backup.

O período de retenção de informações comerciais essenciais deve ser determinado, levando em consideração qualquer requisito para que as cópias de arquivo sejam retidas permanentemente.

Tipo de informação	Suporte de dados	Frequência	Tempo de retenção	Tipo de backup	Tipo de protecção
Servidor de domínio	Discos Internos (storage)	Diario	Semanal	Full	Compactada
KIT e Chegus	Discos Internos (storage)	Diário	Semanal	Full	Cópia
Wemake (SGSI)	Discos Internos (storage)	Diário	Semanal	Full	Cópia
ERP PHC	Discos Internos (storage)	Diário	Semanal	Full	Cópia
Sage Accpack	Discos Internos (storage)	Diário	Semanal	Full	Cópia
BACKOFFICE – aplicação Viva sem Medo	Discos Internos (storage)	Diário, Semanal e Mensal	Semanal	Full	Cópia



Tabela 1: Cronograma de Backup

TRATAMENTO DE ERROS E BACKUPS COM FALHA

Cada manhã, o trabalho de backup da noite anterior deve ser verificado, verificando (extraído) os logs de backup. Quaisquer erros encontrados devem ser investigados, registados e resolvidos antes do próximo backup, sempre que possível.

PROCEDIMENTO PARA REVISÃO DE BACKUP

Deve ser extraído o log de backup diariamente e registar o estado do backup no livro de registo de revisão ou assinar os backups.

PROCEDIMENTO PARA RETENÇÃO E DESTRUIÇÃO DE BACKUP

Os dados devem ser retidos por 5 anos. A mídia que excedeu seu ciclo de vida deve ser destruída.

O processo de destruição deve ser aprova pelo dono do processo e pela comissão executiva.

PROCEDIMENTO PARA RESTAURAÇÃO E TESTE DE BACKUP

O backup deve ser testado regularmente para verificar se os dados que residem nela podem ser recuperados com sucesso.

O procedimento a seguir descreve como os testes aleatórios de rotina de backup deve ser realizada:

- Frequência: testes aleatórios de rotina (restauração parcial) de backup devem ser realizados a cada rês meses. Uma restauração completa deve ser realizada, quando possível, pelo menos uma vez por ano.
- Um meio de backup é escolhido para testes aleatórios de rotina com base nas informações fornecida na lista de informações de backup.
- Uma restauração completa ou parcial é executada usando o backup escolhido para testes de rotina.
- Se a restauração falhar, o GTI deve verificar a causa.
- Se o problema não foi causado por backup corrompido, o problema deve ser corrigido, e o teste deve ser repetido.
- Se o problema foi causado por backup corrompido, ele deve ser destruído, a lista de backup deve ser actualizada e um novo backup realizado.
- Se a restauração for bem-sucedida, a lista de informações de backup deve ser actualizada. Onde a restauração completa do backup não é possível, a restauração parcial é feita nos arquivos seleccionados.

Semestralmente o GTI testa a recuperação dos dados guardados. Backup logs são retidos por um período de um ano.



DIVULGAÇÃO DA POLÍTICA

a) Esta política deve ser divulgada à todos os colaboradores envolvidos no processo de backup, bem como a outros, de outras Unidades Orgânicas que se demonstre apropriado.




RESPONSABILIDADES

Compete ao administrador de sistemas:

- a) Realizar o backup de acordo com as directrizes desta política;
- b) Garantir a disponibilidade, integridade e confidencialidade das informações;
- c) Rever o procedimento e propor actualização das suas directrizes sempre que necessário.

As dúvidas e/ou esclarecimentos que o presente normativo suscitar, deverão ser GTI, através dos meios de comunicação conhecidos. O presente normativo entra em vigor após a sua aprovação pela Comissão Executiva.

HISTÓRICO DO DOCUMENTO

Revisão Nº	Páginas revistas	Alterações efectuadas	Data	Validação		
				Elabobrou	Aprovação(CE)	Assinaturas
2	3	2ª Edição	30 de junho de 2022	GTI	Ruben Chivale Olivio Melembe Nasma Omar	DocuSigned by:  BB56AA22FCF9481... DocuSigned by:  B9A336054376452... DocuSigned by:  7A41BCF05F2F42F...