IT-ONE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PC08 - Política de Backup Corporativo

1. HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
02/06/21	1.0	Criação do documento	Peterson Pires

INTRODUÇÃO

A disponibilidade é considerada um dos pilares da segurança da informação. Sendo assim, visando assegurá-la e, por conseguinte, garantir a continuidade das atividades da organização, a IT-One tem buscado cercar-se de recursos tecnológicos capazes de suportar as atividades administrativas e pedagógicas aos seus colaboradores, alunos e interessados, bem como prover a recuperação das informações geradas (dados e informações), em caso de incidentes.

Observando essa necessidade de assegurar a disponibilidade da informação, tem-se a presente Política Complementar de Backup Corporativo, com as diretrizes acerca do tema.

As cópias de segurança na IT-One contemplam arquivos (dados e informações), sistemas digitais, de máquinas virtuais e bancos de dados, armazenados e/ou hospedados nos data centers da IT-One e IHC, não sendo contemplados dispositivos móveis (tablets e smartphones) ou equipamentos de mesa (PCs).

OBJETIVO

Definir diretrizes de segurança, visando assegurar a disponibilidade da informação, através de cópias de segurança, nomeadas por backup corporativo, para que nos casos de perda de dados, desastre, erro de arquivos, falhas de mídias, entre outros incidentes, estes arquivos e/ou sistemas possam ser recuperados e disponibilizados ao usuário.

ABRANGÊNCIA

Esta política se aplica a todos os colaboradores da IT-One, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da IT-One. Todos esses colaboradores serão tratados nesta política como usuários

DIRETRIZES DE BACKUP CORPORATIVO

1. Diretrizes

1.1. Infraestrutura

a) Para a realização de backup corporativo de arquivos e sistemas digitais armazenados e/ou hospedados em locais diferentes dos data centers da IT-ONE e IHC, deve ser realizada uma solicitação por meio do “Service Desk” e autorizada pelo gestor da informação através de formulário específico;

b) Decorrentes da presente Política Complementar, devem ser estabelecidos procedimentos que considerem:

   I. Cópia de segurança – Escopo, periodicidade, tempo de permanência e descarte;
   II. Recuperação – Disponibilidade da informação, capacidade de armazenamento de destino, tempo de restauração e tempo de permanência preestabelecido.

c) O planejamento das cópias de segurança deve levar em consideração a importância do dado e relacionar o tipo de backup (ex: full ou incremental), a frequência (ex: diária, semanal, mensal, semestral, anual), o período de retenção, local de armazenamento, substituição de mídias, transporte de mídias de dados e requisitos de segurança em relação à criticidade dos dados da IT-One;

d) As solicitações de cópias de segurança (se houver) devem ser realizadas através do “Service Desk”, contendo as informações necessárias para operacionalização e devem ser autorizadas pelo gestor da área ou superior, levando em consideração os níveis de sensibilidade da informação em conformidade com a Política de Classificação da Informação e os procedimentos estabelecidos;

e) O procedimento deve considerar que as cópias sejam efetuadas e testadas regularmente, de maneira que os dados copiados estejam em condições de uso, quando houver necessidade de recuperá-los;

f) O procedimento deve definir e disponibilizar requisitos técnicos e operacionais adequados na geração e restauração de cópias de segurança, assim como, para testes de análise e validação;

g) As solicitações de recuperação das informações devem ser realizadas através do “Service Desk” e autorizadas pelo gestor da área ou superior;

h) A ferramenta de cópia de segurança deve ser mantida atualizada, de acordo com a disponibilização e recomendação do fornecedor e com as licenças ativas consoantes com o contrato estabelecido;

i) As documentações, relativas às configurações da ferramenta de cópia de segurança, inventários e procedimentos, devem ser mantidas atualizadas e disponíveis pela equipe técnica da IT-One.

1.2. Armazenamento e transporte

a) As cópias de segurança devem ser armazenadas em localidade remota, distante do local principal o suficiente para em caso de desastre ou impedimento, não comprometer o acesso para a recuperação quando for necessário. Hoje é realizado uma cópia dos backups da IT-One na cloud da Oracle (OCI);

b) As mídias de cópia de segurança devem ser armazenadas em local com proteção física e ambiental, controle de acesso, e que possua equipamentos de monitoramento e combate a incêndio e ações da natureza;

c) O transporte das cópias de segurança deve ser adequado ao nível de criticidade das informações constante nas mídias trafegadas.

1.3. Recuperação de desastre

a) As cópias de segurança específicas para uma recuperação de desastre devem levar em consideração os sistemas operacionais, aplicações e dados que possibilitem uma completa recuperação;

b) Em caso de desastre, faz-se necessário que a infraestrutura disponibilizada em local de contingência tenha as mesmas características e configurações que o local original.

1.4. Teste e descarte

a) Regularmente as mídias devem ser testadas(quando se aplicar) e analisadas, para garantir a confiabilidade, integridade e disponibilidade nos casos de uso emergencial e aderente aos requisitos necessários à recuperação;

b) As mídias devem ser substituídas no período indicado pelo fabricante ou em casos de erro das mesmas, resguardando os princípios de segurança em relação ao sigilo das informações e descarte de mídias.

1.5. Monitoramento e Auditoria

a) Ferramentas de monitoramento devem ser disponibilizadas no intuito de garantir, entre outras ações, que:

I. As cópias de segurança sejam realizadas em conformidade com o planejado;
II. Seja possível avaliar o crescimento da base de dados para planejar alterações de infraestrutura e compra de mídias;
III. Seja possível identificar erros, analisá-los e tratá-los;

b) Para fins de auditoria interna, toda a atividade relacionada à cópia de segurança deve ser registrada e armazenada por, no mínimo, 2 (dois) anos.