CHECK LIST TECNOLOGIA DA INFORMAÇÃO

Sumário

Introdução

Com o avanço tecnológico e suas consequentes implicações, cada vez mais as rotinas administrativas se veem atreladas aos instrumentos de tecnologia da informação, sejam eles no sentindo físico, naquilo que se refere a equipamentos e maquinários, bem como ao ambiente virtual onde as atividades são desenvolvidas. Portanto, tais fatores assumiram uma importância fulcral no dia-a-dia das atividades funcionais, sendo assim sua preservação, matéria de regulação por parte das instituições. Dessa maneira, o presente manual foi desenvolvido no intuito de estabelecer critérios e procedimentos para a segurança da informação dos registros organizacionais armazenados eletronicamente, emitindo diretrizes gerais para sua confidencialidade, integridade e disponibilidade, de forma a serem efetivamente controlados e executados pelo Setor de Informática do Instituto Municipal de Previdência de Viradouro-SP.

Conceitos

Backup

Cópia de segurança de caráter preventivo, preferencialmente feita por meio de armazenamento interno e externo.

Confidencialidade da Informação

Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Disponibilidade da Informação

Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Active Directory

Ferramenta da Microsoft utilizada para o gerenciamento de usuários de rede, denominada serviço de diretório.

Integridade da Informação

Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Política de Backup

Onde são definidas regras que o software de backup automático utilizará para realizar o backup.

Restore

Restauração do ambiente e/ou dados armazenados por backup.

Responsabilidades Gerais

FUNÇÃO	RESPONSABILIDADE
Setor de Infraestrutura de Ti	• Manter o ambiente computacional em situação satisfatória de desempenho e integridade; • Manter a manutenção e suporte dos sistemas corporativos dos servidores; • Fornecer ao Serviço de Processamento de Dados, infraestrutura para o correto armazenamento dos backups; • Analisar e levantar as características do banco de dados a ser preservado; • Estudar e sugerir a melhor e mais recomendada forma de backup para aquele banco de dados; • Analisar e solucionar a razão para falha de determinada rotina de backup; • Fornecer solução para o erro, durante a execução de determinada rotina de backup;

	• Solicitar suporte de terceiros em caso de tecnologia ou erro não documentado nas rotinas elaboradas pelos sistemas administrativos contratados. • Implementar política de backup automática; • Comunicar prontamente falhas que interrompam a execução das rotinas de backup às empresas contratadas; • Manter os dispositivos de backup corretamente armazenados; • Executar o procedimento manual de destruição dos backups;

Backup – Disposições Gerais

As políticas de Backup podem ser divididas segundo plataformas e sistemas usados e foram definidas de acordo com a seguinte estruturação:

ALVO DO BACKUP	PERIODICIDADE	ARMAZENAMENTO	RETENÇÃO	DESCARTE DO BACKUP
Sistemas Corporativos Administrativos de Gestão	Diário (Segunda a Sexta) as 20:00hrs	Disco Local / Onedrive	Mensal / 3 dias	Manual / Automático

Servidor de Arquivos	Diário (Segunda a Sexta) as 19:00hrs	Disco Local / Onedrive	3 dias	Automático

Os procedimentos de backup são realizados apenas pelo Setor de Infraestrutura de Tecnologia da Informação do IMPREV.

Backup Eletrônico: Os registros das atividades de backup automático contêm informações tais como horário de início e fim dos procedimentos, volume de dados gravados, servidor e tipo de backup, sendo estes registros controlados e armazenados eletronicamente pelo software de backup automático

Backup – Etapas e Procedimentos

1º Procedimento: Elaborar e manter Procedimentos de Backup

- **Procedimentos para elaboração**
  Identificar a plataforma de hardware, o sistema operacional do servidor, o meio de armazenamento externo disponível para aquele servidor e o software instalado.
  Estimar a quantidade de objetos de banco e sua adequação ao limite de espaço do meio de armazenamento.
  Estudar a melhor política ou a mais recomendada pelo fabricante do banco de dados.
  Analisar a sua adequação à situação presente.
  Procurar melhor horário e períodos de execução do procedimento, seja ele manual ou automático.
- **Procedimento para manutenção**

Auxiliar e orientar permanentemente os operadores do IMPREV quando do surgimento de dúvidas ou novos procedimentos de backup, bem como na catalogação dos armazenamentos para facilitar a sua recuperação quando for necessário o *restore*.

Periodicamente acompanhar as execuções, medindo tempos de execução e quantidade de dados que está sendo copiada.

No caso de ocorrer falha na execução do procedimento, averiguar a origem de falhas nas execuções de backup e procurar a solução para ocorrência do erro na execução do backup.

Acompanhar o surgimento de novas tecnologias que forneçam velocidades de gravação superior ou novas formas de realização de backup.

2º Procedimento: Executar Backup

- **Backup Automático:**

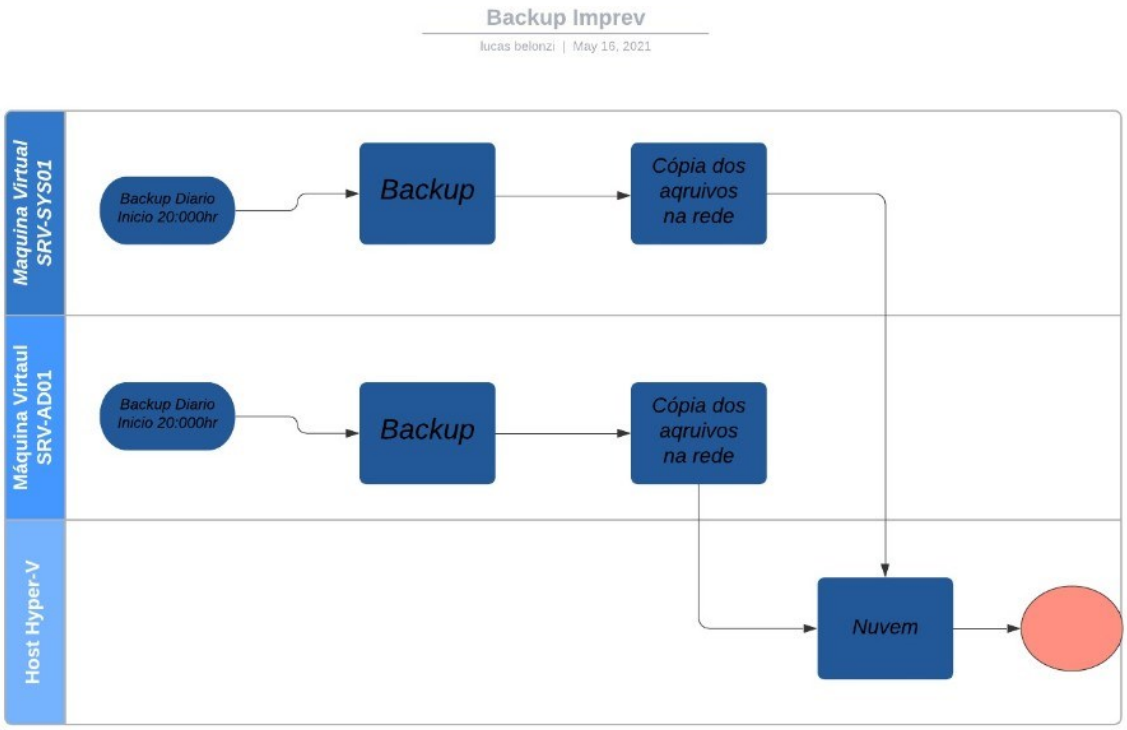
Executar os programas necessários para o backup.

Criar o catálogo para todos os tipos de armazenamentos, definindo o tempo de retenção e expiração.

Verificar através do programa o armazenamento cujo espaço encontra-se insuficiente, liberando para reutilização ou substituição do dispositivo para um maior.

Os procedimentos de backup iniciam automaticamente, conforme políticas previamente estabelecidas.

Abaixo fluxograma da execução dos backups, de acordo com a tabela do item “Backup – disposições gerais”.



3º Procedimento: Monitorar Backup

Acompanhar a execução de todos os procedimentos de backup executados automaticamente.

Comunicar prontamente falhas que interrompam a execução das rotinas de backup aos administradores responsáveis.

Em caso de falha na execução do backup fazer a correção de suas diretrizes.

Login e Controle de acesso

O nome de usuário é a resposta à pergunta: "quem é você?" Como tal, o nome de usuário tem um requisito principal — deve ser único. Em outras palavras, cada usuário deve ter um nome de usuário diferente de todos os outros nomes de usuários no sistema.

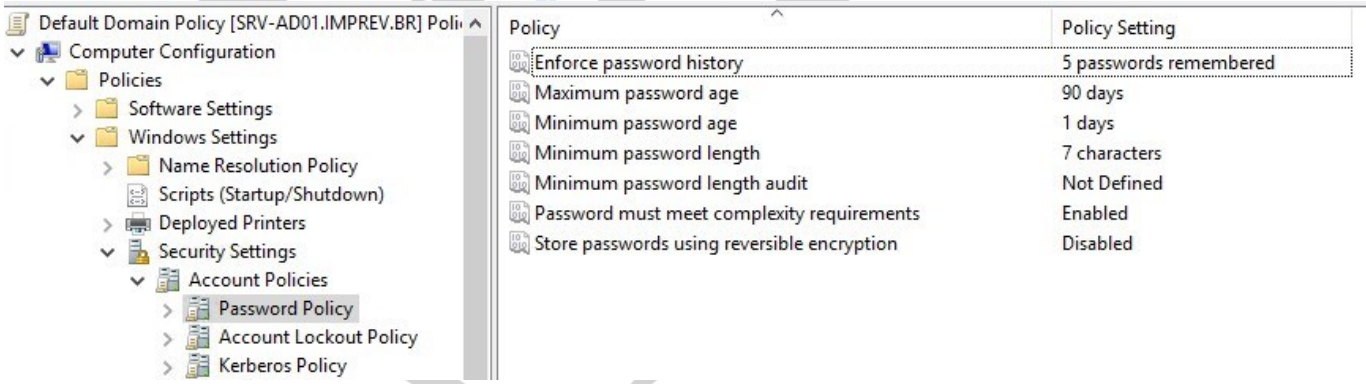
Criação de Usuários no Active Directory

Atualmente os computadores presentes no IMPREV estão conectar ao servidor através de um serviço de diretório conhecido como Active Directory.

Esse serviço de diretório permite a gestão centralizada de e padronização de usuários e computadores.

A imprev segue por convenção a criação de usuário utilizando a primeira letra do nome seguido do sobrenome.

A senhas seguem o padrão de complexidade exigido pelo fabricante, vide imagem abaixo:



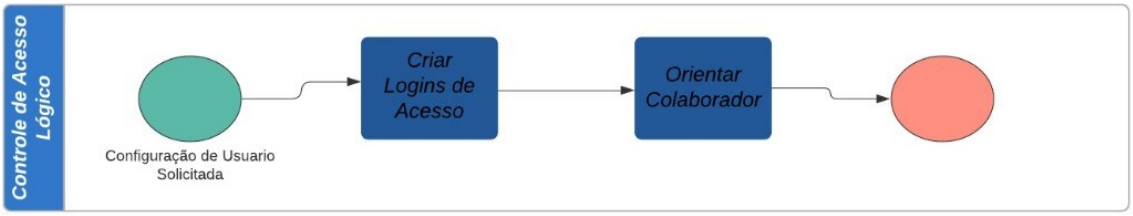
Controle de Acesso

Registro de usuário

Uma solicitação de acesso à rede e aos sistemas de computadores da organização deve primeiro ser enviada à Equipe de TI para aprovação.

Todas as solicitações serão tratadas de acordo com um procedimento formal que garanta que as verificações de segurança sejam realizadas e que a autorização seja obtida antes da criação da conta de usuário.

Abaixo fluxograma do controle de acesso.



Política de Controle de Acesso

Cada conta de usuário terá um nome de usuário exclusivo que não será compartilhado e será associado a um indivíduo específico, ou seja, não um cargo. Contas de usuário genéricas, ou seja, contas individuais a serem usadas por um grupo de pessoas não devem ser criadas, pois não fornecem garantias suficiente de responsabilidade.

Uma senha inicial forte deve ser criada na configuração da conta e comunicada ao usuário por meios seguros. O usuário deve ser obrigado a alterar a senha no primeiro uso da conta.

Quando o funcionário se retira da organização, em circunstâncias comuns, seu acesso aos sistemas e dados deve ser suspenso no último dia de trabalho. É responsabilidade do supervisor solicitar a suspensão dos direitos de acesso por meio da Equipe de TI. Em circunstâncias excepcionais, em que haja um risco de o funcionário tomar providências que possam prejudicar a organização antes ou após a rescisão, uma solicitação para remover o acesso pode ser aprovada e acionada antes da notificação da rescisão. Esta precaução será aplicável nos casos em que o funcionário tem acessos privilegiados, por ex. administrador de domínio.

As contas de usuário devem ser inicialmente suspensas ou desativadas apenas, e não excluídas. Os nomes das contas de usuários não devem ser reutilizados, pois isso pode causar confusão no caso de uma investigação posterior.

Cada usuário deve ter direito de acesso e permissões a sistemas de computador e dados que sejam compatíveis com as tarefas que deve executar. Em geral, isso será baseado na função, ou seja, uma conta de usuário será adicionada a um grupo com as permissões de acesso exigidas para essa função.

Revisão dos direitos de acesso ao usuário

Anualmente, os responsáveis de ativos e sistemas serão obrigados a analisar quem tem acesso às suas áreas de responsabilidade e o nível de acesso. Isto para identificar:

• Pessoas que não devem ter acesso (por exemplo, saiu da empresa);

• Contas de usuário com mais acesso do que o exigido pela função;

• Contas de usuário com alocações de função incorretas;

•Contas de usuário que não fornecem identificação adequada, por exemplo contas genéricas ou compartilhadas;

• Quaisquer outros problemas que não estejam em conformidade com esta política;

Esta revisão será realizada por um procedimento formal e quaisquer ações corretivas identificadas e realizadas.

Uma revisão das contas de usuários com acesso privilegiado será realizada trimestralmente pelo Gerente de Segurança da Informação para assegurar que esta política esteja sendo cumprida.

Controle de acesso de sistemas e aplicativos

No processo de avaliação de sistemas novos ou significativamente modificados, os requisitos para o controle de acesso devem ser abordados e as medidas adequadas implementadas.

Eles devem consistir em um modelo de segurança abrangente que inclua suporte para o seguinte:

- Criação de contas de usuários individuais;
- Definição de funções ou grupos aos quais as contas de usuário podem ser atribuídas;

- Atribuição de permissões a objetos (por exemplo, arquivos, programas, menus) de tipos diferentes (por exemplo, ler, gravar, excluir, executar) de assuntos (contas e grupos de usuários);
- Fornecimento de visualizações variadas de opções de menu e dados de acordo com a conta do usuário e seus níveis de permissão;
- Administração de conta de usuário, incluindo capacidade de desativar e excluir contas;
- Tempo limite de inatividade do usuário;
- Gerenciamento de senhas, incluindo capacidade de usuário alterar senha;
- Recursos de auditoria de segurança, incluindo login/logoffs, tentativas de login malsucedidas, acesso a objetos e atividades de administração de contas;