**UNIVERSIDADE NOVE DE JULHO**

**UNINOVE**

**CURSO DE**

**CIÊNCIAS DA COMPUTAÇÃO**

**E**

**SISTEMAS DE INFORMAÇÃO**

**DISCIPLINA DE SEGURANÇA DA INFORMAÇÃO**

Professor Evandro Carlo Teruel

Integrantes do grupo:

DIEGO FERNANDES ARAUJO - 421100207

São Paulo - 2023

| **Controle de Versões** | | | |
| --- | --- | --- | --- |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
| 1.0 | 17/10 | Diego F. |  |

Sumário

[1. Objetivos 3](#_heading=h.3rdcrjn)

[2. Escopo 3](#_heading=h.26in1rg)

[3. Responsabilidades](#_heading=h.lnxbz9) 4

[4. Frequência de Backup](#_heading=h.35nkun2) 5

[5. Retenção de Dados](#_heading=h.1ksv4uv) 6

[6. Procedimentos de Backup](#_heading=h.44sinio) 7

[7. Testes e Validação](#_heading=h.2jxsxqh) 9

[8. Recuperação de Desastres](#_heading=h.z337ya) 10

[9. Criptografia e Segurança](#_heading=h.3j2qqm3) 11

[10. Monitoramento e Auditoria](#_heading=h.1y810tw) 13

# Objetivos

O objetivo da Política de Backup é garantir a recuperação de dados em caso de perda, minimizar o tempo de inatividade e proteger os ativos de informação da organização.

# Escopo

A Microsoft, como qualquer outra organização, define o escopo de suas políticas de segurança e conformidade com base em suas necessidades e requisitos específicos. Embora eu não tenha informações atualizadas sobre as políticas específicas da Microsoft após setembro de 2021, posso lhe dar uma ideia geral de como as empresas costumam definir o escopo de suas políticas de segurança.

A definição do escopo da política de segurança é um processo que envolve várias etapas, incluindo:

1. **Identificação de Ativos**: A Microsoft, ou qualquer outra organização, começa identificando todos os ativos de TI relevantes. Isso inclui hardware, software, dados e outros recursos.
2. **Classificação de Ativos**: Depois de identificar os ativos, a organização classifica esses ativos com base em seu valor e sensibilidade. Isso ajuda a priorizar a proteção dos ativos mais críticos.
3. **Avaliação de Riscos**: A organização realiza uma avaliação de riscos para entender as ameaças e vulnerabilidades associadas a esses ativos. Isso ajuda a determinar quais ativos são mais suscetíveis a ameaças e onde os controles de segurança são mais necessários.
4. **Definição de Objetivos**: Com base na avaliação de riscos, a organização define objetivos de segurança específicos para proteger os ativos identificados.
5. **Escopo da Política**: A política de segurança é então definida com base nos ativos identificados, nas classificações de sensibilidade e nos objetivos de segurança. Isso envolve a especificação dos sistemas, dados e recursos que estão abrangidos pela política.
6. **Implementação de Controles**: Com o escopo definido, a organização implementa os controles de segurança necessários para proteger os ativos no escopo da política.
7. **Monitoramento e Auditoria**: A organização estabelece processos de monitoramento e auditoria para garantir que os controles de segurança sejam eficazes e estejam sendo seguidos.
8. **Revisão e Atualização**: A política de segurança deve ser revisada periodicamente para garantir que esteja alinhada com as mudanças na organização, nas ameaças cibernéticas e nos requisitos regulatórios.

# Responsabilidades

A Microsoft, como muitas outras organizações, costuma definir claramente as responsabilidades em relação à implementação, gerenciamento e monitoramento do plano de backup, com base em uma estrutura de funções e responsabilidades bem definidas. A alocação de responsabilidades é uma parte fundamental da gestão de backups eficaz. No contexto de suas ofertas de serviços em nuvem, como o Microsoft 365 ou o Azure, as responsabilidades podem variar, dependendo do modelo de serviço em uso (por exemplo, modelo "in cloud" ou "shared responsibility").

No caso do Microsoft 365, por exemplo, a divisão de responsabilidades geralmente é feita entre a Microsoft e os administradores do cliente. A Microsoft é responsável pela infraestrutura subjacente e pela redundância dos dados, enquanto os administradores do cliente são responsáveis por configurar e gerenciar a proteção de dados para suas próprias necessidades específicas.

Em relação ao administrador de backup que você mencionou, suas responsabilidades podem incluir:

1. **Configuração do Sistema de Backup**: O administrador de backup é responsável por configurar as políticas de backup, definir os horários e frequências dos backups e configurar as fontes de dados que precisam ser protegidas.
2. **Manutenção do Sistema de Backup**: Isso envolve a manutenção regular do software ou hardware de backup, aplicação de atualizações e correções, bem como a otimização do desempenho do sistema de backup.
3. **Agendamento de Backups**: O administrador de backup deve agendar backups de acordo com as necessidades da organização, garantindo que os dados críticos sejam copiados regularmente.
4. **Monitoramento do Status das Operações**: Monitorar constantemente o status das operações de backup é fundamental. Isso inclui verificar se os backups foram concluídos com êxito e agir prontamente em caso de falhas.
5. **Configuração de Políticas de Retenção**: Definir políticas de retenção é importante para determinar por quanto tempo os backups devem ser mantidos. Isso ajuda a cumprir requisitos regulatórios e a gerenciar o armazenamento de dados.
6. **Verificação e Teste de Restauração**: Além de fazer backups, o administrador de backup também deve realizar verificações e testes de restauração regularmente para garantir que os dados possam ser recuperados com sucesso, se necessário.
7. **Resolução de Problemas**: Quando ocorrem problemas com os backups, o administrador de backup é responsável por identificar as causas e tomar medidas para corrigi-los.
8. **Garantia de Conformidade**: Em ambientes regulamentados, o administrador de backup também pode ser responsável por garantir que os procedimentos de backup estejam em conformidade com os requisitos regulatórios aplicáveis

# Frequência de Backup

A frequência com que você deve fazer um backup depende basicamente da quantidade de mudanças nos arquivos no período entre cada procedimento. Se tratando da Microsoft, uma empresa que é ativa 24 horas durante 7 dias, e com ela contendo uma vasta quantia de dados, se é recomendado que diversos backups sejam feitos, diário, semanal, mensal e anual, todos os tipos se conectariam idealmente com os valores que a Microsoft deseja mostrar ao seus clientes e patrocinadores. Por isso aqui estamos apresentando alguns exemplos de como a Microsoft pode lidar com a frequência de backup em diferentes cenários:

**Microsoft 365 (anteriormente Office 365):**

Para o Microsoft 365o que mais se encaixaria seriam backups automáticos de dados do Microsoft 365, incluindo e-mails, documentos, calendários e contatos. Isso permite a recuperação de dados excluídos acidentalmente por usuários. Os backups seriam realizados em um ciclo contínuo e podem ser restaurados a qualquer momento, ou seja diários.

**Azure Backup:**

No Azure, os administradores iriam poder configurar backups de máquinas virtuais e serviços de nuvem com base em um agendamento flexível. Isso pode incluir backups diários, semanais ou personalizados, dependendo das necessidades da organização.

**Windows Server:**

No Windows Server incluiria uma funcionalidade de backup que permite que os administradores programem backups regulares de servidores. Isso pode ser diário, semanal ou conforme definido pela organização.

**SQL Server (no Azure ou no local):**

No SQL Server permitiria o agendamento de backups regulares de bancos de dados. Isso pode ser configurado de acordo com a política de retenção da organização, incluindo backups diários, semanais ou personalizados.

**Outros Serviços do Azure:**

Já a Microsoft Azure oferece uma série de serviços, e a frequência de backup pode variar de acordo com o serviço. Por exemplo, alguns serviços podem suportar backups em tempo real, enquanto outros podem ter uma programação de backup mais flexível com base nas necessidades da organização.

Com a parte de backup contendo diversas opções para o mesmo assim como citamos acima algumas das mais conhecidas para que haja uma base. Dentre essas opções chegamos a conclusão, e seguiremos com backups diários, semanais, mensais e anuais, para melhor desempenho e confiança, tendo em vista que seriam várias opções onde algumas não se encaixam para o modelo em questão.

# Retenção de Dados

A Microsoft oferece recursos para a definição da política de retenção de dados em seus produtos e serviços, como o Microsoft 365, o Azure e o Windows Server. A política de retenção de dados determina por quanto tempo os backups serão mantidos e como os dados antigos serão gerenciados. A empresa oferece flexibilidade para que os administradores possam configurar a retenção de acordo com as necessidades da organização. Aqui estão alguns exemplos de como a Microsoft pode lidar com a retenção de dados em diferentes cenários:

**Microsoft 365 (anteriormente Office 365)**:

* **Políticas de Retenção de Itens**: Os administradores do Microsoft 365 podem configurar políticas de retenção de itens para determinar por quanto tempo os e-mails, documentos, calendários e outros dados serão mantidos. Isso pode incluir retenção de itens excluídos por um determinado período (por exemplo, 30 dias) e retenção de itens de caixa de correio inativas.

**Azure Backup**:

* **Política de Retenção Personalizável**: No Azure, os administradores podem criar políticas de retenção personalizadas para backups de máquinas virtuais e serviços de nuvem. Isso permite definir a retenção de acordo com as necessidades da organização, como retenção de backups diários por 30 dias, semanais por 3 meses e assim por diante.

**Windows Server**:

* **Configuração de Políticas de Backup**: Os administradores podem configurar políticas de backup no Windows Server para definir por quanto tempo os backups serão mantidos. Isso pode incluir a retenção de backups diários por um número específico de semanas ou meses.

**SQL Server (no Azure ou no local)**:

* **Configuração de Políticas de Retenção**: No SQL Server, as políticas de retenção podem ser configuradas para bancos de dados. Isso permite especificar por quanto tempo os backups de banco de dados serão mantidos.

**Outros Serviços do Azure**:

* **Flexibilidade na Retenção**: A Microsoft Azure oferece flexibilidade para configurar políticas de retenção de acordo com os requisitos específicos de cada serviço. A duração da retenção pode variar com base nas necessidades da organização.

# Procedimentos de Backup

A Microsoft fornece orientações abrangentes e ferramentas em seus produtos e serviços para a configuração de procedimentos de backup. A seguir, estão alguns dos procedimentos técnicos comuns relacionados à realização de backups que são aplicáveis em ambientes onde a Microsoft desempenha um papel significativo:

**Seleção de Dados para Backup**:

* Administradores podem selecionar quais dados e recursos são críticos e precisam ser incluídos nos backups. Isso pode incluir bancos de dados, servidores de arquivos, contas de e-mail, documentos, configurações de servidores e muito mais.

**Programação de Backup**:

* Os administradores configuram quando os backups devem ser realizados, com base em políticas definidas. Isso pode incluir backups diários, semanais, mensais ou de acordo com um cronograma personalizado.

**Métodos de Backu**p:

* A Microsoft oferece suporte a vários métodos de backup, incluindo:
* **Backup Completo**: Cria cópias completas dos dados selecionados em cada execução.
* **Backup Incremental**: Apenas os dados que foram modificados desde o último backup são copiados.
* **Backup Diferencia**l: Copia todos os dados modificados desde o último backup completo.
* **Backup em Tempo Real**: Alguns serviços, como o Microsoft 365, oferecem proteção de dados contínua e em tempo real.

**Armazenamento de Backup**:

* Os backups podem ser armazenados em várias localizações, incluindo:
* **Dispositivos Locais**: Em servidores locais, dispositivos de armazenamento em rede (NAS), ou dispositivos de armazenamento externo.
* **Nuvem**: A Microsoft oferece armazenamento em nuvem seguro para backups em serviços como Azure e Microsoft 365.
* **Locais Geograficamente Separados**: Para redundância e recuperação de desastres, os backups podem ser armazenados em locais geograficamente separados da empresa.

**Criptografia de Dados de Backup**:

* Os dados de backup podem ser criptografados para garantir que permaneçam seguros durante a transferência e armazenamento. A Microsoft oferece opções de criptografia para proteger os dados de backup.

**Teste e Validação de Backup**:

* Testes regulares de restauração são importantes para garantir que os backups sejam bem-sucedidos e os dados possam ser recuperados quando necessário.

**Tratamento de Falhas**:

* Procedimentos de contingência e planos de recuperação de desastres são necessários para lidar com falhas nos procedimentos de backup e para garantir a recuperação eficaz em caso de problemas.

# Testes e Validação

A Microsoft, assim como muitas outras organizações e fornecedores de serviços de backup, reconhece a importância de testar e validar regularmente os backups para garantir que os dados possam ser restaurados com sucesso em caso de necessidade. A seguir, estão alguns dos procedimentos comuns relacionados aos testes e validação de backups:

**Programação de Testes**:

* A programação de testes regulares é fundamental. Os administradores devem definir uma frequência para a realização dos testes, como mensal, trimestral ou de acordo com a política da empresa.

**Seleção de Dados para Testes**:

* Selecionar conjuntos de dados representativos para os testes. Isso pode incluir dados críticos e variados que abrangem diferentes tipos de arquivos e informações.

**Simulação de Restauração**:

* Simular o processo de restauração é uma parte fundamental dos testes. Isso envolve a tentativa de restaurar os dados de backup para um ambiente de teste ou para um local alternativo. Os procedimentos de restauração devem ser documentados e seguidos.

**Verificação de Integridade**:

* Durante o processo de restauração, é importante verificar a integridade dos dados restaurados. Certifique-se de que os dados não foram corrompidos durante o processo de backup e restauração.

**Correção de Problemas**:

* Se durante o teste for identificado algum problema na restauração, é fundamental documentar e investigar a causa raiz do problema. Qualquer problema encontrado deve ser corrigido para garantir que os backups sejam confiáveis.

**Documentação de Testes**:

* Documentar os resultados dos testes é importante para acompanhar o desempenho do sistema de backup ao longo do tempo. Isso também ajuda na resolução de problemas e na melhoria contínua.

**Envolvimento de Stakeholders**:

* Stakeholders, como membros da equipe de TI e partes interessadas no negócio, devem estar cientes dos testes e dos resultados. Isso ajuda a garantir que todos estejam alinhados quanto à confiabilidade do sistema de backup.

**Automatização de Testes**:

* Em alguns casos, é possível automatizar partes dos testes, o que pode economizar tempo e garantir que os testes sejam realizados consistentemente.

**Testes de Recuperação de Desastres**:

* Além dos testes regulares de restauração, também é importante realizar testes de recuperação de desastres, onde todo o ambiente de produção é simulado em um ambiente de recuperação de desastres. Isso verifica a capacidade de recuperar todo o ambiente em caso de desastre.

# Recuperação de Desastres

A Microsoft oferece orientações e soluções para ajudar as organizações a lidar com situações de desastre, incluindo planos de recuperação de desastres (DR) e estratégias de continuidade de negócios (BC). Essas estratégias são projetadas para garantir que a organização possa manter suas operações críticas em funcionamento, mesmo após eventos disruptivos, como desastres naturais, falhas de hardware, ataques cibernéticos, entre outros. A seguir, são abordados aspectos-chave relacionados à recuperação de desastres com a Microsoft:

**Avaliação de Riscos e Impacto**:

* O primeiro passo é realizar uma avaliação de riscos para identificar as ameaças que podem afetar a organização e o impacto que essas ameaças teriam nos negócios. Isso ajuda a priorizar os esforços de recuperação.

**Elaboração de Planos de Recuperação de Desastres**:

* Com base na avaliação de riscos, a organização desenvolve planos de recuperação de desastres que especificam como lidar com diferentes cenários de desastres. Isso pode incluir a definição de procedimentos, responsabilidades e recursos necessários para a recuperação.

**Soluções de Continuidade de Negócios**:

* A Microsoft oferece soluções e serviços que suportam a continuidade de negócios, incluindo a replicação de dados, a recuperação de desastres em nuvem e a virtualização de servidores. O Azure Site Recovery, por exemplo, permite replicar máquinas virtuais e serviços em nuvem para um local de recuperação.

**Armazenamento Redundante e Recuperação na Nuvem**:

* O uso de armazenamento em nuvem e a redundância geográfica dos dados são estratégias comuns para garantir que os dados estejam disponíveis em caso de desastre. A Microsoft oferece opções de armazenamento redundante em seus serviços em nuvem, como o Azure.

**Testes Regulares**:

* Os planos de recuperação de desastres devem ser testados regularmente para garantir que funcionem conforme o esperado. Isso inclui testes de recuperação de dados, testes de failover e simulações de desastres.

**Treinamento e Conscientização**:

* Os funcionários devem ser treinados para saber como agir em caso de desastre. Isso inclui a familiarização com os planos de recuperação e a capacidade de tomar ações rápidas e apropriadas.

**Comunicação de Crise**:

* Estabelecer um plano de comunicação de crise é crucial para manter todas as partes interessadas informadas durante uma situação de desastre. Isso inclui clientes, parceiros, funcionários e reguladores.

**Monitoramento e Atualização Contínuos**:

* As estratégias de recuperação de desastres e continuidade de negócios não são estáticas. Elas devem ser revisadas e atualizadas regularmente para garantir que estejam alinhadas com as mudanças na organização e nas ameaças.

# Criptografia e Segurança

A Microsoft prioriza a segurança e a criptografia em seus produtos e serviços, incluindo soluções relacionadas a backups e recuperação de dados. Abaixo estão algumas das práticas comuns relacionadas à criptografia e segurança de dados de backup:

**Criptografia de Dados de Backup**:

* A criptografia é usada para proteger os dados de backup durante a transmissão e o armazenamento. Isso garante que os dados sejam inelegíveis para qualquer pessoa não autorizada. A criptografia pode ser usada tanto em repouso (armazenamento) quanto em trânsito (durante a transferência).

**Definição de Criptografia Utilizada**:

* As empresas devem definir as políticas de criptografia, incluindo os algoritmos e chaves utilizados. A Microsoft oferece opções de criptografia para se adequar às necessidades de segurança da organização.

**Gerenciamento de Chaves**:

* O gerenciamento de chaves é fundamental para a criptografia de dados de backup. As empresas devem estabelecer procedimentos de gerenciamento de chaves, como rotação de chaves e proteção de chaves mestras.

**Controle de Acesso**:

* É importante definir quem tem acesso aos dados de backup e implementar controles de acesso rigorosos. Isso inclui a autenticação de dois fatores e políticas de controle de acesso baseadas em função.

**Auditoria e Monitoramento**:

* A detecção de atividades suspeitas é fundamental. As empresas devem implementar sistemas de auditoria e monitoramento para rastrear o acesso aos dados de backup e detectar qualquer atividade não autorizada.

**Alertas e Notificações**:

* Configurar alertas e notificações para informar os administradores sobre atividades incomuns ou suspeitas em relação aos dados de backup.

**Políticas de Retenção de Chaves**:

* Algumas empresas adotam políticas de retenção de chaves que garantem que as chaves de criptografia de backup sejam mantidas sob controle da organização, mesmo em caso de terceirização de serviços de backup.

**Teste de Recuperação Segura**:

* Certificar-se de que os procedimentos de recuperação segura sejam estabelecidos, onde a restauração dos dados só ocorre após a validação da identidade e das permissões.

**Conformidade com Regulamentações**:

* Empresas devem considerar regulamentações específicas da indústria ou do país ao definir políticas de criptografia e segurança de dados de backup para garantir a conformidade.

# Monitoramento e Auditoria

A Microsoft, como parte de suas ofertas de produtos e serviços, fornece ferramentas e orientações para o monitoramento e a auditoria de políticas de backup. A seguir estão algumas práticas comuns relacionadas ao monitoramento e à auditoria de políticas de backup em empresas:

**Ferramentas de Monitoramento de Backup**:

* Implementar ferramentas de monitoramento de backup que rastreiam a execução de backups é uma prática comum. Essas ferramentas podem fornecer informações sobre o status dos backups, o tempo de execução e outras métricas relevantes.

**Agendamento de Auditorias Regulares**:

* Programar auditorias regulares da política de backup é uma abordagem importante para garantir a conformidade e a eficácia dos procedimentos de backup. As auditorias podem ser conduzidas internamente ou por terceiros especializados.

**Revisão de Logs de Backup**:

* Revisar regularmente os logs de backup é fundamental para identificar problemas, anomalias ou atividades suspeitas. Isso ajuda a garantir que os backups estejam ocorrendo conforme o planejado.

**Detecção de Atividades Suspeitas**:

* Além de revisar logs, as empresas podem implementar soluções de detecção de atividades suspeitas para identificar potenciais ameaças ou violações de segurança relacionadas ao backup.

**Relatórios de Auditoria:**

* A geração de relatórios de auditoria é uma prática comum para documentar os resultados das auditorias e quaisquer ações corretivas que precisam ser tomadas.

**Política de Conformidade**:

* Desenvolver uma política de conformidade que detalhe os padrões que a política de backup deve cumprir. Isso ajuda a orientar as auditorias e garantir que as políticas estejam em conformidade com as regulamentações e as melhores práticas.

**Avaliação da Política de Backup**:

* Periodicamente, a política de backup deve ser avaliada para garantir que ela esteja alinhada com as necessidades da organização, as mudanças na infraestrutura de TI e as ameaças emergentes.

**Treinamento e Conscientização**:

* Treinar e conscientizar os funcionários sobre a importância do monitoramento e da auditoria das políticas de backup ajuda a garantir que todos na organização compreendam suas responsabilidades.

| **Aprovações** | | |
| --- | --- | --- |
| **Participante** | **Assinatura** | **Data** |
| Chief Executive Officer (CEO) | Erick Alves Santana | 17/10/2023 |
| Chief Security Officer (CSO) | Paulo Vinício Carreiro | 17/10/2023 |