ÂNCORA
DESPACHANTE

Política de Backup e Recuperação de Dados

1. Objetivo:

1.1 Esta política tem por objetivo estabelecer as práticas e responsabilidades relacionadas à realização de backups regulares e à recuperação de dados na organização.

2. Responsabilidades:

2.1 A equipe de Tecnologia da Informação (TI) é responsável pela implementação, monitoramento e manutenção dos procedimentos de backup e recuperação de dados.

2.2 Todos os colaboradores devem cooperar com a equipe de TI e seguir as diretrizes estabelecidas nesta política.

3. Backups Regulares:

3.1 Deverão ser realizados backups regulares de todos os dados considerados críticos para as operações da empresa.

3.2 Os backups devem incluir, mas não se limitar a, sistemas, bancos de dados, arquivos de configuração e dados de usuários.

3.3 O cronograma de backups deve ser estabelecido com base na criticidade dos dados, sendo no mínimo 1 vez por semana.

4. Armazenamento de Backups:

4.1 Os backups devem ser armazenados em locais seguros, fora do ambiente principal de TI, para mitigar riscos como desastres naturais ou eventos que possam comprometer a infraestrutura física.

ÂNCORA
DESPACHANTE

4.2 Deve ser assegurada a proteção dos backups contra acessos não autorizados.

4.3 Periódicos testes de restauração devem ser realizados para garantir a integridade e eficácia dos backups.

5. Política de Retenção:

5.1 Será estabelecida uma política de retenção de backups para determinar o período pelo qual os dados serão mantidos.

5.2 Dados obsoletos ou não mais necessários devem ser removidos dos backups de acordo com a política de retenção.

6. Procedimentos de Recuperação:

6.1 Em caso de falhas ou incidentes que resultem em perda de dados, a equipe de TI deve atuar de maneira rápida e eficaz na recuperação dos dados.

6.2 Procedimentos documentados de recuperação devem ser mantidos e revisados regularmente.

6.3 A equipe de TI é responsável por comunicar prontamente as partes interessadas sobre qualquer incidente que envolva perda de dados.

7. Atualização e Revisão:

7.1 Esta política será revisada periodicamente para garantir sua eficácia e atualizada conforme necessário para refletir as mudanças nas operações e tecnologias.

7.2 A revisão incluirá a avaliação da eficácia dos procedimentos de backup e recuperação em resposta a incidentes recentes.

ÂNCORA
DESPACHANTE

8. Treinamento e Conscientização:

8.1 A equipe de TI fornecerá treinamento regular aos colaboradores sobre a importância da política de backup e recuperação, bem como sobre os procedimentos a serem seguidos.

9. Disposições Finais:

9.1 O não cumprimento desta política pode resultar em medidas disciplinares, incluindo rescisão de contrato e responsabilização por eventuais danos causados.

Política de Segurança da Informação

1. Introdução

1.1 A segurança da informação é um aspecto crítico para o sucesso e a continuidade dos negócios da organização. Esta política estabelece as diretrizes, regras e procedimentos para garantir a confidencialidade, integridade e disponibilidade das informações.

2. Abrangência

2.1 Esta política é aplicável a todos os colaboradores, contratados, fornecedores e demais partes que tenham acesso às informações da organização.

3. Responsabilidades

3.1 Cada colaborador é responsável por:

• Proteger informações confidenciais e sensíveis da empresa;

• Utilizar senhas de forma segura e não as compartilhar com terceiros;

• Reportar imediatamente qualquer incidente de segurança da informação à equipe

designada.

4. Senhas e Autenticação

4.1 Senhas devem ser robustas, incluindo letras maiúsculas, minúsculas, números e caracteres especiais.

4.2 Colaboradores devem utilizar senhas exclusivas para diferentes sistemas e aplicativos.

4.3 Senhas não devem ser compartilhadas, anotadas ou armazenadas em locais de fácil acesso.

4.4 A autenticação de dois fatores (2FA) deve ser habilitada sempre que possível.

5. Acesso a Sistemas e Informações

5.1 O acesso a sistemas e informações deve ser concedido com base no princípio do menor privilégio.

5.2 Colaboradores devem fazer logout de sistemas e terminar sessões de trabalho ao deixarem seus dispositivos.

5.3 O acesso remoto deve ser realizado por meio de conexões seguras, utilizando VPN quando aplicável.

6. Proteção de Dispositivos

6.1 Todos os dispositivos fornecidos pela empresa devem ser protegidos por senhas e/ou métodos de autenticação.

6.2 Atualizações de software e antivírus devem ser aplicadas regularmente.

6.3 Dispositivos móveis devem ser protegidos por PIN, senha ou biometria.

6.4 A perda ou roubo de dispositivos deve ser reportada imediatamente.

7. Manuseio de Informações Classificadas

7.1 As informações devem ser classificadas de acordo com seu nível de sensibilidade.

7.2 O compartilhamento de informações classificadas deve obedecer às políticas internas da empresa.

8. Monitoramento e Auditoria

8.1 A empresa reserva-se o direito de monitorar o uso de sistemas e redes para garantir a conformidade com esta política.

8.2 Auditorias de segurança podem ser realizadas periodicamente.

9. Treinamento e Conscientização

9.1 Colaboradores devem passar por treinamentos regulares em segurança da informação.

9.2 Campanhas de conscientização sobre ameaças cibernéticas devem ser realizadas regularmente.

10. Disposições Finais

10.1 O não cumprimento desta política pode resultar em medidas disciplinares, incluindo rescisão de contrato, bem como resultar na responsabilização cível e criminal, nos termos previstos pela legislação brasileira.

10.2 Alterações nesta política serão comunicadas aos colaboradores e demais partes interessadas.

ÂNCORA
DESPACHANTE

Política de Senhas e Autenticação

1. Objetivo:

1.1 Esta política estabelece as diretrizes para a criação, uso e proteção de senhas, bem como os requisitos de autenticação para o acesso a sistemas da organização.

2. Senhas:

2.1 As senhas são um componente essencial da segurança da informação. Para garantir a proteção adequada, as seguintes diretrizes devem ser seguidas:

• As senhas devem ter no mínimo oito caracteres.

• Devem incluir uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.

• As senhas não devem ser facilmente relacionadas a informações pessoais (como nomes, datas de nascimento, etc.).

• As senhas devem ser alteradas regularmente, a cada 6 (seis) meses.

• Senhas não devem ser compartilhadas ou divulgadas a terceiros.

3. Autenticação de Dois Fatores (2FA):

3.1 A autenticação de dois fatores (2FA) é uma camada adicional de segurança. De acordo com esta política:

• A 2FA deve ser habilitada para todos os sistemas e aplicativos que oferecem suporte a essa funcionalidade.

• O uso da 2FA é obrigatório para o acesso a sistemas e informações críticas.

ÂNCORA
DESPACHANTE

4. Proteção de Senhas:

4.1 Para garantir a segurança das senhas armazenadas e transmitidas, as seguintes medidas devem ser tomadas:

• Senhas não devem ser armazenadas em formatos legíveis. Em vez disso, devem ser adequadamente criptografadas.

• A transmissão de senhas deve ocorrer por meio de canais seguros, com protocolos de criptografia.

5. Gerenciamento de Acesso:

5.1 O acesso a sistemas e informações deve ser gerenciado de acordo com o princípio do menor privilégio:

5.1.1 Cada usuário deve receber acesso apenas às informações e recursos necessários para desempenhar suas funções.

5.1.2 O acesso deve ser revisto regularmente e ajustado conforme necessário.

6. Monitoramento e Auditoria:

6.1 A organização reserva-se o direito de monitorar o uso de senhas e conduzir auditorias de segurança para garantir a conformidade com esta política.

6.2 Tentativas suspeitas de acesso ou violações de senha devem ser relatadas imediatamente à equipe de segurança da informação.

7. Conscientização e Treinamento:

7.1 A organização fornecerá treinamentos regulares sobre boas práticas de segurança da informação, incluindo a criação e gestão de senhas seguras.

8. Disposições Finais:

8.1 O não cumprimento desta política pode resultar em medidas disciplinares, incluindo rescisão de contrato e responsabilização por eventuais danos causados.

8.2 Alterações nesta política serão comunicadas aos usuários de forma eficaz.