1. Políticas de Acesso e Controle de Usuários

Objetivo: Garantir que apenas usuários autorizados acessem recursos e dados sensíveis da empresa, minimizando os riscos de acessos não autorizados ou mal-intencionados.

Política proposta:

- **Autenticação Multifatorial (MFA):** Todos os usuários devem utilizar autenticação multifatorial (MFA) para acessar sistemas críticos e dados sensíveis. Isso proporciona uma camada extra de segurança, além da senha, dificultando o acesso por meio de credenciais comprometidas.
- **Privilégios Mínimos:** O acesso a sistemas e dados deve ser baseado no princípio de "privilégios mínimos", ou seja, os usuários devem ter acesso apenas aos recursos necessários para desempenhar suas funções. Isso limita os danos em caso de comprometimento de uma conta.
- **Controle de Acesso Baseado em Funções (RBAC):** O acesso será concedido com base nas funções do colaborador dentro da empresa, garantindo que um usuário com responsabilidades limitadas não tenha acesso a informações que não são relevantes para sua função.
- **Gerenciamento de Senhas:** Senhas devem ser alteradas a cada 90 dias. A empresa deve implementar políticas rigorosas para a criação de senhas seguras (mínimo de 8 caracteres, contendo letras maiúsculas, minúsculas, números e caracteres especiais).
- **Revisão Periódica de Acessos:** Os acessos dos funcionários devem ser revistos periodicamente para garantir que aqueles que não desempenham mais determinadas funções ou que saíram da empresa não mantenham acessos ativos aos sistemas.

Justificativa:

Essas políticas visam proteger a integridade e confidencialidade das informações da empresa, assegurando que o acesso seja restrito e monitorado de acordo com as necessidades e responsabilidades dos colaboradores.

2. Política de Uso de Dispositivos Móveis e Redes

Objetivo: Proteger os dados da empresa contra vazamentos ou acessos não autorizados, especialmente quando acessados por dispositivos móveis ou redes externas.

Política proposta:

- **Uso de VPN (Rede Privada Virtual):** Todos os funcionários que acessarem a rede corporativa remotamente, de fora da empresa, devem utilizar uma VPN. A VPN criptografa a comunicação, tornando mais difícil para atacantes interceptarem dados sensíveis.
- **Controle de Dispositivos Móveis (BYOD):** Se a empresa permitir o uso de dispositivos pessoais para acessar sistemas corporativos (BYOD – Bring Your Own Device), esses dispositivos devem ser configurados com criptografia de dados e autenticação forte. Além disso, o acesso será monitorado e restrito a aplicativos corporativos.
- **Bloqueio de Tela e Senhas em Dispositivos:** Todos os dispositivos móveis, como smartphones e tablets, devem ser configurados para bloquear a tela automaticamente após 5 minutos de inatividade e exigir uma senha ou biometria para desbloqueio.
- **Proibição de Uso de Redes Públicas:** O acesso a sistemas da empresa via redes Wi-Fi públicas (como em cafés ou aeroportos) é estritamente proibido, a menos que seja feito por meio da VPN corporativa.
- **Monitoramento e Controle de Aplicativos:** O uso de aplicativos móveis não autorizados ou não corporativos deve ser evitado. Apenas aplicativos relacionados ao trabalho devem ser instalados e monitorados pela equipe de TI.

Justificativa:

Essas medidas são cruciais para proteger dados sensíveis contra roubo ou interceptação, especialmente em um ambiente em que dispositivos móveis e conexões à distância se tornam cada vez mais comuns.

3. Diretrizes para Resposta a Incidentes de Segurança

Objetivo: Estabelecer um protocolo claro para a gestão de incidentes de segurança, garantindo que a empresa possa reagir rapidamente a eventos que possam comprometer a segurança da informação.

Política proposta:

- **Notificação Imediata:** Todos os colaboradores devem ser orientados a reportar imediatamente qualquer incidente de segurança ao departamento de TI ou equipe de segurança. A empresa deve fornecer canais de comunicação seguros e dedicados a essas notificações.
- **Plano de Resposta a Incidentes:** A empresa deve ter um plano estruturado para responder a incidentes de segurança, que inclua as etapas de identificação, contenção, erradicação, e recuperação. Esse plano deve ser revisado e testado periodicamente.
- **Investigação e Documentação de Incidentes:** Todos os incidentes de segurança devem ser documentados em detalhes e analisados para identificar a causa raiz e evitar ocorrências futuras. A análise pós-incidente deve ser realizada com o objetivo de melhorar continuamente as práticas de segurança.
- **Treinamento Contínuo:** A empresa deve oferecer treinamentos periódicos para os colaboradores sobre como identificar e reagir a incidentes de segurança, como phishing e vazamento de dados, além de manter a equipe de TI treinada em técnicas de resposta a incidentes.

Justificativa:

Essas diretrizes permitem que a empresa se recupere rapidamente de incidentes de segurança, minimizando danos e melhorando a postura de segurança com base em experiências passadas.

4. Política de Backup e Recuperação de Desastres

Objetivo: Garantir que dados críticos possam ser recuperados em caso de falhas nos sistemas, ataques de ransomware ou desastres naturais, protegendo a continuidade dos negócios.

Política proposta:

- **Backup Regular:** A empresa deve realizar backups diários de todos os dados essenciais, incluindo documentos, banco de dados e configurações do sistema. Esses backups devem ser armazenados tanto localmente quanto em uma solução de armazenamento em nuvem segura.
- **Testes de Recuperação:** A empresa deve testar a recuperação dos dados a cada seis meses para garantir que o processo de backup esteja funcionando corretamente e que a restauração seja possível em caso de falha.

- **Armazenamento Seguro e Criptografado:** Todos os backups devem ser criptografados e armazenados de forma segura. O acesso a esses backups deve ser restrito a pessoal autorizado apenas.
- **Plano de Continuidade de Negócios (BCP):** A empresa deve ter um plano de continuidade de negócios, que defina ações claras para a recuperação de sistemas e dados após eventos catastróficos, com a priorização de processos críticos.
- **Monitoramento de Backups:** O status dos backups deve ser monitorado em tempo real e qualquer falha no processo deve gerar alertas imediatos para os administradores de TI.

Justificativa:

A implementação de backups regulares e a definição de um plano claro de recuperação garantem que a empresa consiga se recuperar de falhas graves ou desastres, minimizando o tempo de inatividade e a perda de dados importantes.