Integrantes:

Arthur Galassi | RA: 82422433

Kaue Soares | RA: 824117267

Leonardo Macedo | RA: 82422817

Luiz Washington | RA: 824148694

Lucas Felipe | RA: 824138683

George Geronimo | RA: 824148488

Políticas de segurança

Políticas de Acesso e Controle de Usuário:

Autenticação: Todos os usuários devem utilizar senhas fortes, que incluem uma combinação de letras, números e caracteres especiais ($, #@, %*). As senhas devem ser trocadas a cada 120 dias, seguindo o mesmo padrão.

Autorização: O acesso a informações e sistemas deve ser baseado em cargos hierárquicos conforme a **importância e sigilo da informação.**

Conectividade: Usuários que atuam dentro da empresa para acessar a rede devem utilizar de um dispositivo fornecido pela mesma.

Políticas de Uso de Dispositivos Móveis e Redes

Criptografia de Dados: Todos os dispositivos móveis devem obter uma criptografia atualizada para proteger informações sensíveis em caso de perda, roubo ou vazamento de dados.

Segurança de Aplicativos: É permitido instalar apenas aplicativos provenientes de fontes da própria empresa. Além disso, todos os softwares devem ser mantidos atualizados para garantir a proteção contra vulnerabilidades, incluindo o antivírus.

Conexões Seguras: Os funcionários são devidamente treinados a evitar redes Wi-Fi públicas e abrir arquivos desconhecidos para acessar informações corporativas. O uso de uma rede privada virtual (VPN) é obrigatório sempre que o acesso remoto for necessário.

Diretrizes para Resposta a Incidentes de Segurança

Identificação de Incidentes: Todos os funcionários devem ser treinados para identificar e reportar incidentes de segurança, como phishing ou acesso não autorizado.

Equipe de Resposta: Formar uma equipe técnica que responda a incidentes, responsável por investigar e resolver problemas de segurança na empresa.

Documentação: Documentar todos os registros, incidentes e as ações tomadas, para melhorar análises posteriores e dar continuidade nos processos.

Política de Backup e Recuperação de Desastres

Armazenamento de Backup: Os backups devem ser armazenados em locais físicos de preferência longe do local de atuação, utilizar do método RAID para backup em tempo real e devem separados e em serviços de nuvem confiáveis para proteção contra desastres locais.

Testes de Recuperação: Realizar simulações de recuperação de desastres regularmente para garantir que os backups possam ser restaurados rapidamente em caso de necessidade.

Documentação de Processos: Manter documentação clara e acessível sobre os procedimentos de backup e recuperação para facilitar a execução em situações de emergência.