Etapa	Frases	Menor tempo de execução	Maior tempo de execução
Etapa 0	Identificação e isolamento imediato dos sistemas afetados para conter o vazamento de dados.	Imediato	2 horas
	Notificação das equipes de segurança, jurídica e de relações públicas sobre o incidente.	1 hora	4 horas
	Início das investigações preliminares para determinar a extensão e origem do ataque.	2 horas	6 horas
Etapa 1	Configuração de isolamento/desconexão automática (SOAR) para prevenir a propagação do incidente.	4 horas	8 horas
	Comunicação aos clientes afetados informando sobre o vazamento e medidas de mitigação.	4 horas	12 horas
	Atualização das configurações de alerta para detectar qualquer atividade suspeita relacionada ao vazamento.	2 horas	6 horas
Etapa 2	Implementação de centralização dos alertas de segurança em um ponto único (SIEM).	6 horas	12 horas
	Correção e otimização das configurações de alerta para garantir respostas rápidas a novas ameaças.	4 horas	8 horas
	Início do processo de atualização dos contatos dos responsáveis por cada sistema para garantir comunicação eficiente.	2 horas	4 horas
Etapa 3	Continuação da análise forense para identificar e eliminar quaisquer backdoors ou malwares remanescentes.	12 horas	24 horas
	Reforço das medidas de segurança em todos os sistemas, incluindo patching e atualizações necessárias.	12 horas	24 horas
	Revisão e atualização da documentação dos sistemas para refletir as mudanças e melhorias implementadas.	8 horas	16 horas
Etapa 4	Orientação aos clientes sobre práticas seguras de armazenamento de dados e medidas preventivas.	4 horas	8 horas
	Oferecimento de serviços adicionais de Cyber Security para aumentar a proteção dos dados dos clientes.	6 horas	12 horas
	Desenvolvimento e implementação de indicadores de perda financeira para monitorar e avaliar futuros incidentes.	8 horas	16 horas
Etapa 5	Estabelecimento de uma operação 24/7 para monitoramento contínuo e resposta a incidentes.	1 semana	2 semanas
	Finalização da atualização e centralização das documentações dos sistemas.	1 semana	2 semanas
	Treinamento adicional das equipes internas e externas para garantir a eficácia das novas medidas de segurança.	1 semana	2 semanas
Etapa 6	Revisão completa das políticas de segurança e conformidade para prevenir futuros vazamentos.	2 semanas	4 semanas
	Testes rigorosos dos sistemas de segurança implementados para assegurar sua eficácia.	1 semana	2 semanas
	Implementação de uma campanha de conscientização de segurança entre os colaboradores e clientes.	1 semana	2 semanas
Etapa 7	Realização de auditorias regulares para garantir que todas as medidas de segurança estão sendo seguidas.	1 mês	2 meses
	Monitoramento contínuo dos sistemas para identificar e mitigar novas ameaças proativamente.	1 mês	2 meses
	Avaliação e ajuste das medidas de segurança baseadas em feedback e resultados das auditorias.	1 mês	2 meses
Etapa 8	Consolidação das lições aprendidas com o incidente e documentação das melhores práticas.	2 meses	3 meses
	Fortalecimento das parcerias com empresas de segurança cibernética para apoio contínuo.	2 meses	3 meses
	Planejamento e execução de exercícios de simulação de incidentes para testar a prontidão da equipe.	2 meses	3 meses
Etapa 9	Revisão e atualização das políticas de segurança corporativa com base nas lições aprendidas.	3 meses	6 meses
	Expansão das capacidades de segurança com novas tecnologias e estratégias.	3 meses	6 meses
	Continuidade na educação e treinamento de segurança para todos os colaboradores.	3 meses	6 meses