**Compliance da Empresa de Análise de Vulnerabilidade**

1. **Visão**  
   Ser referência no mercado de cibersegurança, oferecendo análises de vulnerabilidade que protejam e capacitem empresas a manterem ambientes digitais seguros, garantindo confiança em todos os níveis.
2. **Missão**  
   Capacitar empresas na identificação e mitigação de vulnerabilidades, promovendo um ambiente seguro para a operação e o crescimento dos negócios por meio de soluções precisas e confiáveis.
3. **Conformidade com a LGPD**  
   Em qualquer ação, teste ou análise, a empresa está totalmente alinhada à Lei Geral de Proteção de Dados (LGPD), que regula o tratamento de dados pessoais e garante a proteção da privacidade.

3.1 **Confidencialidade e LGPD**

* + **Proteção e Tratamento de Dados Pessoais**: Em conformidade com a LGPD, garantimos que todas as operações e acessos a dados pessoais dos clientes estejam protegidos. Cada acesso a dados sensíveis passa por uma verificação de conformidade com a LGPD.
  + **Termos de Confidencialidade e Controle de Acesso**: Todos os colaboradores e parceiros são obrigados a assinar termos de confidencialidade, e o acesso é limitado ao mínimo necessário para proteger a privacidade e a confidencialidade, conforme exigido pela LGPD.

3.2 **Integridade**

* + **Controle e Validação de Alterações em Conformidade com a LGPD**: Qualquer modificação ou intervenção em sistemas e dados é feita com análise prévia, conforme a LGPD. Em descobertas de vulnerabilidade, seguimos uma abordagem de Remoção, Retração e Jurídico para mitigar riscos, isolar sistemas afetados e garantir a integridade dos dados, respeitando sempre a legislação.

3.3 **Disponibilidade e Conformidade**

* + **Planos de Continuidade e Backup Seguros**: Qualquer vulnerabilidade que ameace a continuidade dos serviços é tratada conforme a LGPD, priorizando a segurança dos dados pessoais. Realizamos backups com criptografia e acesso controlado, em conformidade com a LGPD, para assegurar a disponibilidade e proteção dos dados.

1. **Política de Jornada de Trabalho**  
   4.1 **Modalidades de Trabalho**
   * **Remoto**: A empresa opera em um modelo de trabalho remoto, possibilitando flexibilidade e acessibilidade para todos os colaboradores. Cada colaborador tem horários de trabalho definidos, de acordo com as demandas de cada função e a necessidade de interação com a equipe.
   * **Presencial (opcional)**: Caso necessário, os colaboradores podem utilizar o escritório da empresa para reuniões estratégicas, treinamentos e atualizações de equipamentos.

4.2 **Ferramentas e Equipamentos**

* + A empresa fornece as ferramentas e equipamentos essenciais (computadores, VPNs, softwares de segurança) para garantir que as atividades possam ser desempenhadas remotamente de forma segura e eficiente.

4.3 **Horário Flexível e Disponibilidade**

* + A flexibilidade de horários é oferecida, respeitando as entregas e prazos acordados com os clientes. Cada colaborador deve garantir a disponibilidade para reuniões de equipe e sessões de atualização semanais.

1. **Política de Acesso e Segurança**  
   5.1 **Políticas de Acesso**
   * **Autenticação de Múltiplos Fatores (MFA)**: Todos os colaboradores devem utilizar MFA para acessar sistemas internos e plataformas que contenham dados sensíveis.
   * **Acesso Segmentado por Função**: Os acessos aos dados e sistemas da empresa são concedidos com base no perfil e nas funções de cada colaborador, garantindo um controle restrito e monitorado.
   * **Sistema de Logs**: Todas as atividades, acessos e modificações nos sistemas são registradas automaticamente em logs de segurança, com monitoramento constante para detectar atividades incomuns.

5.2 **VPN e Segurança de Rede**

* + **Acesso Exclusivo por VPN**: Todos os acessos aos sistemas internos devem ser feitos por VPN, com criptografia de ponta a ponta, assegurando a proteção da comunicação de dados.
  + **Monitoramento e Auditorias Regulares**: Realização de auditorias e verificações regulares de segurança para garantir o cumprimento das políticas e identificar melhorias contínuas.

5.3 **Política de Segurança Contra Ameaças Externas**

* + **Atualizações de Segurança**: Todos os equipamentos e softwares devem estar atualizados com os últimos patches e correções de segurança.
  + **Treinamento de Conscientização em Segurança**: A empresa realiza treinamentos mensais de conscientização, reforçando boas práticas de cibersegurança e prevenção contra ameaças, como phishing e engenharia social.

1. **Política de Resposta a Cenários de Ataque aos Dados dos Clientes**  
   Ao identificar um cenário de ataque ou vulnerabilidade crítica que envolva dados pessoais, seguimos os protocolos da LGPD. Qualquer teste de invasão será executado somente após a autorização expressa do CEO da empresa, assegurando a retraçabilidade da ação. Caso sejam encontradas vulnerabilidades relacionadas ao comportamento de colaboradores, o setor Jurídico será acionado para as notificações necessárias.

6.1 **Detecção e Avaliação de Ameaça**

* Realizamos uma análise de impacto imediato sobre a privacidade e integridade dos dados, conforme previsto na LGPD.

6.2 **Comunicação e Transparência**

* Transparência e prontidão são fundamentais. Em caso de incidentes que afetem dados pessoais, as informações são comunicadas ao cliente e às autoridades, mantendo a conformidade com a LGPD.