**📝 Formulário de Pré-Análise: Maturidade em Segurança da Informação, Cibersegurança e TI**

**Objetivo:** Avaliar a situação atual da sua empresa em relação à proteção de dados, segurança da informação e infraestrutura de TI, como etapa inicial para um projeto de adequação à LGPD.

**Instruções:** Responda cada pergunta escolhendo a alternativa que mais representa a realidade da sua empresa hoje.

**🔐 SEGURANÇA DA INFORMAÇÃO**

1. **A empresa possui políticas claras sobre proteção de dados?**
   * (1) Não temos nenhuma política.
   * (2) Temos algumas orientações informais.
   * (3) Existe uma política, mas poucos conhecem.
   * (4) Política escrita e comunicada, mas sem revisão.
   * (5) Política atualizada, documentada e aplicada com treinamentos.
2. **Existe controle de acesso aos arquivos e sistemas da empresa?**
   * (1) Não há controle.
   * (2) Alguns documentos têm senha.
   * (3) Usamos logins, mas sem controle de acesso.
   * (4) Acesso com permissões por área/setor.
   * (5) Controle completo por usuário, com registros e auditoria.
3. **Os funcionários recebem treinamento sobre como proteger os dados?**
   * (1) Nunca receberam.
   * (2) Apenas no início do trabalho.
   * (3) Já houve treinamento, mas sem frequência.
   * (4) Ocasionalmente fazemos treinamentos.
   * (5) Treinamentos frequentes e obrigatórios.
4. **Existe um responsável formal pela segurança da informação?**
   * (1) Não.
   * (2) Alguém cuida informalmente.
   * (3) Pessoa da TI assume a função parcialmente.
   * (4) Responsável nomeado, mas sem dedicação exclusiva.
   * (5) Responsável dedicado, com autonomia e rotina definida.
5. **Como é feito o descarte de documentos físicos e digitais?**
   * (1) Não há nenhum critério.
   * (2) Cada setor faz como acha melhor.
   * (3) Há orientação, mas não é seguida.
   * (4) Processo definido, mas sem controle.
   * (5) Processo padronizado, com segurança e rastreabilidade.
6. **Os dados pessoais são protegidos por mecanismos técnicos (ex: criptografia)?**
   * (1) Não utilizamos nenhuma proteção técnica.
   * (2) Apenas alguns arquivos são protegidos.
   * (3) Usamos senhas básicas.
   * (4) Dados críticos têm proteção adequada.
   * (5) Dados pessoais são protegidos com múltiplas camadas (ex: criptografia + controle de acesso).
7. **As informações sensíveis (ex: dados de clientes) têm controle de quem acessa?**
   * (1) Qualquer pessoa pode acessar.
   * (2) Alguns dados têm acesso restrito.
   * (3) Acesso controlado em algumas áreas.
   * (4) Acesso por setor com registro parcial.
   * (5) Acesso restrito por usuário com registro e autorização.
8. **Há controle de onde os dados pessoais estão armazenados?**
   * (1) Não sabemos onde estão.
   * (2) Sabemos parcialmente.
   * (3) Sabemos, mas não temos organização.
   * (4) Documentado, mas desatualizado.
   * (5) Totalmente mapeado e controlado.
9. **Em caso de incidente de segurança, existe um plano de ação?**
   * (1) Não sabemos o que fazer.
   * (2) Resolveríamos por tentativa e erro.
   * (3) Temos uma ideia geral.
   * (4) Plano documentado, mas sem testes.
   * (5) Plano testado, conhecido e revisado regularmente.
10. **Com que frequência as políticas de segurança são revisadas?**

* (1) Nunca foram revisadas.
* (2) Apenas quando há problemas.
* (3) Revisamos de forma eventual.
* (4) Há calendário anual, mas sem revisão formal.
* (5) Revisadas periodicamente com participação dos gestores.

**🛡️ CIBERSEGURANÇA**

1. **A empresa utiliza antivírus ou ferramentas de proteção contra ameaças?**
   * (1) Nenhuma proteção.
   * (2) Apenas antivírus gratuito.
   * (3) Antivírus pago em alguns dispositivos.
   * (4) Antivírus pago em todos os dispositivos.
   * (5) Antivírus com gestão centralizada e relatórios.
2. **Existe firewall configurado na rede da empresa?**
   * (1) Não usamos firewall.
   * (2) Apenas o firewall padrão do roteador.
   * (3) Firewall com regras básicas.
   * (4) Firewall com regras definidas e segmentação.
   * (5) Firewall com monitoramento e atualização frequente.
3. **A empresa realiza backups dos dados importantes?**
   * (1) Não fazemos backup.
   * (2) Backup manual e irregular.
   * (3) Backup automático, mas sem validação.
   * (4) Backup periódico com validação ocasional.
   * (5) Backup automático, testado e armazenado em local seguro.
4. **Os sistemas da empresa são atualizados com frequência?**
   * (1) Nunca atualizamos.
   * (2) Só quando há falha.
   * (3) Atualizamos manualmente, sem controle.
   * (4) Atualização periódica, mas sem política formal.
   * (5) Atualizações automatizadas e controladas.
5. **Existe proteção contra golpes por e-mail (phishing, spam)?**
   * (1) Não há proteção.
   * (2) Apenas filtro básico do e-mail.
   * (3) Filtro de spam ativo, sem gestão.
   * (4) Solução de proteção ativa em todos os e-mails.
   * (5) Filtro avançado, com monitoramento e treinamento de usuários.
6. **Os dispositivos móveis usados (celulares, notebooks) têm segurança adequada?**
   * (1) Nenhuma proteção.
   * (2) Apenas senha de acesso.
   * (3) Antivírus ou bloqueio de tela.
   * (4) Dispositivos gerenciados pela TI.
   * (5) Dispositivos criptografados, monitorados e com controle remoto.
7. **Já houve algum incidente de segurança digital na empresa?**
   * (1) Sim, e não sabemos a causa.
   * (2) Sim, resolvemos sem medidas preventivas.
   * (3) Sim, e tomamos medidas depois.
   * (4) Não, mas não temos plano de ação.
   * (5) Não, e temos plano de resposta implementado.
8. **A empresa possui plano de resposta a incidentes cibernéticos?**
   * (1) Não temos plano.
   * (2) Temos ideia geral.
   * (3) Plano informal.
   * (4) Plano documentado, mas sem testes.
   * (5) Plano testado, revisado e com responsáveis definidos.

**🖥️ TECNOLOGIA DA INFORMAÇÃO (TI)**

1. **Existe alguém responsável pela área de TI?**
   * (1) Não há ninguém responsável.
   * (2) Um funcionário ajuda ocasionalmente.
   * (3) Um colaborador atua, mas sem processo.
   * (4) Terceirizamos para empresa de TI.
   * (5) Profissional ou equipe dedicada, com processos documentados.
2. **A rede está organizada e protegida?**
   * (1) Totalmente desorganizada.
   * (2) Uso de Wi-Fi aberto ou sem senha forte.
   * (3) Wi-Fi com senha simples e equipamentos misturados.
   * (4) Wi-Fi com separação por setor e senha forte.
   * (5) Rede segmentada com equipamentos gerenciados.
3. **As senhas são trocadas regularmente?**
   * (1) Nunca são trocadas.
   * (2) Trocadas apenas quando há problema.
   * (3) Trocadas esporadicamente.
   * (4) Política informal de troca.
   * (5) Política obrigatória de troca periódica.
4. **Os softwares são originais e licenciados?**
   * (1) Usamos softwares piratas.
   * (2) Alguns são originais, outros não.
   * (3) Usamos apenas o que veio nos equipamentos.
   * (4) Usamos software livre ou com licenças organizadas.
   * (5) Todos são licenciados e com controle centralizado.
5. **Os dados estão centralizados e organizados?**
   * (1) Estão espalhados em diversos computadores.
   * (2) Estão em pen drives ou HDs externos.
   * (3) Centralizamos em pastas, mas sem organização.
   * (4) Usamos servidor ou nuvem, mas sem controle.
   * (5) Dados centralizados, organizados e com backup.
6. **Os equipamentos seguem padrão de compra e configuração?**
   * (1) Cada setor compra o que quer.
   * (2) Compramos conforme necessidade, sem padrão.
   * (3) Temos preferência por algumas marcas.
   * (4) Compramos conforme padrão, mas sem documentação.
   * (5) Equipamentos padronizados e documentados.
7. **Há controle de quem acessa os sistemas?**
   * (1) Não há controle.
   * (2) Login compartilhado.
   * (3) Logins individuais sem controle de permissões.
   * (4) Logins com permissões, mas sem histórico.
   * (5) Logins controlados, com permissões e auditoria.
8. **Existe inventário de equipamentos e softwares?**
   * (1) Não temos inventário.
   * (2) Temos lista informal.
   * (3) Lista desatualizada.
   * (4) Lista organizada, mas manual.
   * (5) Inventário digital e atualizado.
9. **A empresa tem plano de continuidade em caso de falhas?**
   * (1) Não temos plano.
   * (2) Apenas uma ideia informal.
   * (3) Documentado, mas desatualizado.
   * (4) Plano atualizado, mas nunca testado.
   * (5) Plano documentado, testado e revisado periodicamente.