INFORMAÇÕES BÁSICAS

Informações Cadastrais:

Razão Social:

CNPJ:

Informações Para análise:

1) Poderia nos informar o **domínio principal** de internet da empresa?

Importante: Essa informação é relevante para podermos rodar o scan de vulnerabilidade do seguro.
“https//www.empresa.com.br”

2) Caso você precise informar mais algum domínio, só digitar abaixo?

Os domínios precisam estar separados por "," (vírgula);
“www.dominio2.com.br,www.dominio3.com.br,www.dominio4.com.br”.

3) Qual seria o ramo da atuação da empresa?

Escolha uma das opções da lista.

4) Qual o faturamento da empresa?

Min. R$ 100.000,00 - Max. R$ 300.000.000,00

R$

5) Qual seria o limite pretendido para a importância segurada?

Min. R$ 100.000,00 - Max. R$ 300.000.000,00

R$

6) Você informar uma segunda opção de importância segurada?

Caso não queira, deixe a opção em vazia.

R$

7) Você informar uma terceira opção de importância segurada?

Caso não queira, deixe a opção em vazia.

R$

Informações do Corretor:

Nome e Sobrenome:	
Corretora:	
E-mail:	
Telefone:	

20.00 % Comissionamento desejado

☐ O Proponente abaixo declara que todas as informações constantes neste questionário são verdadeiras.

QUESTIONÁRIO TÉCNICO

Dados da empresa:

Razão Social:

CNPJ:

Informações para Análise:

1) Quanto do faturamento em percentual da empresa representa as vendas online?

2) Na sua empresa existe alguém responsável pela Segurança da Informação, como por exemplo um (Chief Information Security Officer "CISO")?

Sim ☐ Não ☐

3) A Empresa possui um Encarregado dos Dados, ou, Data Protection Officer (DPO)?

O Encarregado dos Dados, ou Data Protection Officer (DPO) garante, de forma independente, que uma determinada organização segue as leis que protegem os dados pessoais dos indivíduos.

4) Qual o tipo de dados que a sua empresa guarda sobre os seus clientes?

Pode selecionar várias opções

- ☐ Informação Pessoal Identificável (PII)
- ☐ Informação Pessoal de Saúde (PHI)
- ☐ Informações de Cartão de Crédito (PCI)
- ☐ Propriedade Intelectual (IP)

5) Estime o número de registros únicos (PII/PHI/PCI) que são guardados.

Sabendo que Informação Pessoal Identificável (PII), Informação Pessoal de Saúde (PHI) ou Informações de Cartão de Crédito (PCI).

6) Estime a quantidade de dispositivos (smartphone, desktop, notebook ou tablet) existem na sua empresa.

7) Estime a quantidade de funcionários que trabalham diretamente para a sua empresa.

Entende-se que funcionários são: Estagiários, Terceiros, CLT e Autônomos.

8) A empresa executa algum tipo de treinamento com os seus colaboradores sobre phishing?

Definição de Phishing: É um tipo de engenharia social que necessariamente se utiliza de links falsos para sites falsos na internet projetados para coletar dados pessoais dentro do referido site falso. Tais links são comumente enviados por e-mail, SMS, WhatsApp ou similares.

Entende-se que "recorrentemente" aos treinamentos executados de forma trimestral. Logo, pontualmente seria 1 vez ao ano.

9) A Empresa possui um time responsável pelo controle e a manutenção de acesso dos usuários?

Um time dedicado as alterações de permissões e retirada de usuários inativos.

Sim ☐ Não ☐

10) Sobre os usuários inativos: estes são retirados do sistema quando após sua inatividade?

Usuários que não acessam mais o sistema por meio de suas credenciais.

11) Com relação as políticas de acesso aos sistemas e dispositivos, selecione quais se aplicam ao seu negócio:

Pode selecionar várias opções

- [ ] Perfil de acesso distinto para colaboradores, administradores e terceiros que contemplem níveis de acessos diferentes e respeitem as devidas alçadas.
- [ ] Exigência de níveis de segurança compatíveis com o próprio padrão de segurança da informação para prestadores de serviços terceirizados.
- [ ] Perfil de administrador restrito ao time de Tecnologia.
- [ ] Criptografia das informações confidenciais armazenadas em dispositivos móveis (por exemplo, smartphones e laptops) e em seus servidores web (por exemplo, HTTPS)
- [ ] Monitoramento de rede e identificação de eventos de segurança.
- [ ] Servidores de internet, e-mail segregados de sua rede confiável (por exemplo, em um provedor terceirizado ou dentro de uma zona desmilitarizada (DMZ).
- [ ] Confidencialidade de dados operacionais de testes com o objetivo de garantir que todos os detalhes confidenciais sejam protegidos por remoção ou modificação.
- [ ] Redundância nos servidores e processo de informações (ou seja, qualquer sistema, serviço ou infraestrutura, ou local físico que o abrigue).

12) A empresa tem algum tipo de regra exigindo senhas fortes para acesso de sistemas críticos?

Entende-se que senha forte é uma senha com 8 ou mais caracteres sem palavras do dicionário, ou repetição de caracteres. Normalmente, uma senha é considerada forte quando tem um comprimento considerável e contém símbolos, letras maiúsculas e minúsculas e, inclusive, números.

Sim	Não
☐	☐

13) Quais dos itens abaixo são adotados pela empresa em **TODOS** os dispositivos e/ou ambientes digitais?

Pode selecionar várias opções

- [ ] Antivírus
- [ ] Firewall
- [ ] Backup semanal na nuvem em outra localidade separada da produção
- [ ] Sistema anti-phishing
- [ ] VPN
- [ ] Autenticação de Múltiplos Fatores (MFA)
- [ ] Outro

14) Na sua empresa existe um Plano de Ação em resposta a um incidente cibernético?

Detalhando as funções e procedimentos a serem adotados em caso de um ataque ou incidente cibernético.

Sim	Não
☐	☐

15) A empresa costuma fazer atualizações críticas de software ("Patch") sempre que recomendado pelo fabricante?

Entende-se que "recorrentemente" se aplica quando a atualização é feita em até 1 semana da liberação do patch. Logo, pontualmente seria qualquer período após 1 semana.

16) Em Compliance, a Empresa realizou as alterações necessárias para se adaptar as regras de LGPD?

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais.

Sim	Não
☐	☐

17) Sua empresa tem ciência de algum fato, circunstância, problema que possa causar alguma perda ou sinistro dentro do contexto de cibersegurança?

Sim ☐ Não ☐

Descreva o ocorrido...

18) Sua empresa já teve algum incidente, interrupção não planejada de negócios e/ou processos judiciais envolvendo problemas de privacidade ou ataques cibernéticos?

Sim ☐ Não ☐

Descreva o ocorrido...

19) Em caso de um incidente cibernético, a empresa possui:

Pode selecionar várias opções

- ☐ Análise de Impacto ao négocio
- ☐ Plano de recuperação de dados em caso de desastre
- ☐ Plano de continuidade de negócios
- ☐ Nenhuma das alternativas anteriores

22) A empresa tem ou já teve seguro de riscos cibernéticos?

Sim ☐ Não ☐

Informações para contato:

Nome e Sobrenome:	
E-mail:	
Telefone:	

☐ O Proponente abaixo declara que todas as informações constantes neste questionário são verdadeiras.