AXE INSURANCE

CORRETORA DE SEGUROS

QUESTIONÁRIO

www.axeinsurance.com.br

DEVER DE INFORMAÇÃO

O Questionário de Avaliação do Risco é uma série de perguntas que a seguradora faz para definir o perfil do segurado e, desta forma, poder avaliar melhor o risco que ela irá assumir, o que tende a impactar positiva ou negativamente no valor do prêmio a ser pago, de acordo com os critérios de avaliação de risco de cada seguradora.

É dever do Segurado prestar informações verídicas e atuais e não omitir circunstâncias que possam influenciar na aceitação do risco. Poderá haver perda do direito de receber indenização em caso de sinistro, além de ficar obrigado a pagar o prêmio vencido, conforme disposto no artigo nº 766 da Lei nº 10.406/2002 (Código Civil).

Se eventualmente as informações fornecidas sofrerem alteração ao longo da vigência da apólice, o segurado deve comunicar a alteração para, se necessário, fazer o endosso, evitando assim o risco de ficar sem cobertura, em caso de sinistro.

QUESTIONÁRIO DE RESPONSABILIDADE CIVIL PARA PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

1. Razão Social:
2. Endereço:
3. CNPJ:
4. Data de início das atividades?:
5. Detalhar o ramo de atividade:
6. Número de funcionários:
7. Controle Acionário:
8. Quantidade Média de Dados e Informações sob custódia informatizada (B2B e/ou B2C):
9. Responsável pelo preenchimento (nome e telefone):
10. Faturamento médio / ANO:

	Últimos 12 meses	Estimativa dos próximos 12 meses
Faturamento Bruto		
Distribuição geográfica		
do Faturamento Bruto do Proponente (%)		
Faturamento no Brasil		
Faturamento nos EUA e Canadá		
Faturamento América Latina		
Faturamento na Europa		
Faturamento em outros continentes		
Total (100%)		
Países		

11. Existe Política de Segurança da Informação implementada na Empresa? Se sim, a Política de SI é divulgada e disponibilizada aos colaboradores, terceiros e prestadores de serviço?

- ☐ Não
- ☐ Sim, explicar

12. Existe Política de Continuidade de Negócios implementada na Empresa? Se sim, a Política de CN é divulgada e disponibilizada aos colaboradores?

- ☐ Não
- ☐ Sim, explicar

13. Quais os regimes de contratação de colaboradores de SI?

14. Existe algum programa de conscientização e treinamento em Segurança da Informação? Se sim, qual o formato de avaliação aplicado para estes treinamentos de Segurança da Informação?

- ☐ Não
- ☐ Sim, explicar

15. Existe um programa de conscientização e treinamento em Continuidade de Negócios? Se sim, qual o formato de avaliação aplicado para estes treinamentos de Continuidade de Negócio?

- ☐ Não
- ☐ Sim, explicar

16. É realizado inventário periódico, e / ou monitoração dos equipamentos e terminais dos usuários dos colaboradores (Desktops, Notebooks, Smartphones, etc)?

☐ Não
☐ Sim, explicar

17. O inventário é realizado em Planilha, Manual ou Sistema?

18. É efetuado a Instalação de antivírus e produtos de gerenciamento e segurança nas máquinas?

☐ Não
☐ Sim, explicar

19. Qual antivírus é utilizado e ou produto de gerenciamento?

20. É bloqueado o compartilhamento de diretórios corporativos da empresa para os colaboradores?

☐ Não ☐ Sim

21. É monitorado e gravado logs de ações dentro dos diretórios corporativos?

☐ Não
☐ Sim

22. É bloqueado a adição de contas de administração no grupo administrador local?

☐ Não ☐ Sim

23. É bloqueado a alteração do nome do administrador local?

☐ Não ☐ Sim

24. É bloqueado a alteração da senha do administrador local?

☐ Não ☐ Sim

25. É bloqueado o acesso ao prompt de comandos (DOS) para colaboradores comuns?

☐ Não ☐ Sim

26. É bloqueada a adição de componentes do Sistema Operacional (SO) para colaboradores que são de SI?

☐ Não ☐ Sim

27. É bloqueado o uso de ferramentas de edição do Registro para colaboradores que de SI?

☐ Não ☐ Sim

28. É bloqueada a alteração do nome da máquina para colaboradores que são de SI?

☐ Não ☐ Sim

29. É bloqueada ou controlado o download de arquivos e softwares da internet?

☐ Não ☐ Sim

30. As portas USB das máquinas são bloqueadas ou desativadas?

☐ Não ☐ Sim

31. Caso efetuem o bloqueio das portas USB, existe algum controle e/ou monitoramento das mesmas?

- [ ] Não
- [ ] Sim, explicar

32. Existe procedimento seguro de eliminação dos dados das máquinas ou mídias quando são substituídos, descartados ou cedidos?

- [ ] Não
- [ ] Sim, explicar

33. Os equipamentos (desktops e notebooks) possuem senha para acesso a BIOS, ou serviço de BITLocker?

- [ ] Não
- [ ] Sim, explicar

34. É efetuado a atualização do Antivírus nos desktops e notebooks de forma automática?

- [ ] Não
- [ ] Sim, explicar

35. São monitorados e controlados os softwares instalados nos desktops e notebooks?

- [ ] Não
- [ ] Sim, explicar

36. Os softwares instalados nos equipamentos (desktops e notebooks) passam por um processo de homologação?

- ☐ Não
- ☐ Sim, explicar

37. É bloqueado mais de um login na rede pelo mesmo usuário?

- ☐ Não
- ☐ Sim, explicar para quais áreas?

38. Os materiais e documentos físicos se existentes e confidenciais são armazenados de forma segura?

- ☐ Não
- ☐ Sim, explicar

39. Existe uma política de descarte de materiais confidenciais na empresa? (exemplo: HDs, Computadores e afins).

- ☐ Não
- ☐ Sim, explicar

40. É utilizado shredder no caso de cópias impressas? Se sim, por favor detalhar como é feito e quais os registros.

- ☐ Não
- ☐ Sim, explicar

41. A empresa possui política de desligar ou bloquear estações de trabalho e notebooks ao final do expediente automaticamente?

☐ Não
☐ Sim, explicar

42. Existe um mecanismo de travar as sessões inativas de usuários na rede?

☐ Não
☐ Sim, explicar

43. Máquinas copiadoras estão com a função e-mail externo desabilitada?

☐ Não ☐ Sim

44. Qual o tipo de Datacenter a empresa possui?

45. O Datacenter está localizado no Brasil ou no exterior? Em sendo no exterior, favor especificar qual o país.

46. Existe controle de acesso físico ao Data Center (Crachá, Biometria, etc)?

☐ Não ☐ Sim

47. É controlado e/ou registrado quem possui acesso ao Data Center?

☐ Não ☐ Sim

48. É efetuada revisão periódica da lista de pessoas com acesso físico ao Datacenter?

☐ Não
☐ Sim, explicar

49. Somente as áreas competentes as atividades de Infraestrutura que possuem acesso ao Datacenter?

☐ Não ☐ Sim

50. É efetuado o registro de visitantes e pessoal de manutenção no acesso ao Datacenter?

☐ Não ☐ Sim

51. Existe um Plano de Continuidade de Negócios que abrange a recuperação do ambiente de TI total ou parcial do Data Center principal?

☐ Não
☐ Sim, explicar

52. Em relação às capacidades de recuperação de desastres do Proponente, selecione todas as opções que se aplicam:

☐ Existe um processo para execução de backups, mas não é documentado e estruturado.
☐ O Proponente possui uma política documentada de recuperação de desastres, incluindo padrões para realização de backups de acordo com a criticidade da informação
☐ Pelo menos duas vezes ao ano, o Proponente testa sua capacidade de restaurar diferentes sistemas e dados críticos de seus backups
☐ Nenhuma das opções anteriores.

53. Em relação a autenticação de funcionários que acessam remotamente a rede corporativa e serviços baseados em nuvem que armazenem dados sensíveis (incluindo acesso VPN, e-mail baseado em nuvem e soluções de CRM), selecione a descrição que melhor representa a postura

atual do Proponente. Inclua comentários adicionais sobre requisitos de autenticação adotados pela companhia.

('Autenticação multi fator' no contexto abaixo significa autenticação que utiliza pelo menos dois fatores diferentes de autenticação (algo que você sabe, algo que você tem, e algo que você é);

☐ Acesso remoto à recursos corporativos requer uma combinação válida de usuário e senha (único fator de autenticação).

☐ Autenticação multi fator está implantada para acesso remoto a alguns tipos de recursos corporativos, mas não todos

☐ Autenticação multi fator é requerida por política para acesso remoto a qualquer recurso corporativo; todas as exceções à esta política são documentadas

☐ O Proponente não fornece acesso remoto aos funcionários.

54. A implementação de autenticação multi fator também atende a critérios de que o comprometimento de algum dispositivo isolado somente comprometa um fator de autenticação?
(Por exemplo: onde a autenticação requer uma senha (algo que você sabe) e um token (algo que você tem), a configuração não atenderia ao critério, se o token é armazenado no mesmo dispositivo em que a senha é inputada, o que poderia expor os dois fatores de autenticação caso o dispositivo fosse comprometido)

☐ Não

☐ Sim, explicar

55. Quando liberado o acesso remoto o mesmo é feito através de um terminal padronizado e exclusivo da empresa?

☐ Não

☐ Sim, explicar

56. A empresa possui políticas de multifatorial implantado?

☐ Não

☐ Sim, explicar

57. São revisados semanalmente os acessos remotos da empresa?

☐ Não ☐ Sim

58. Os acessos remotos são monitorados?

☐ Não

☐ Sim, explicar

59. Os dados transferidos são criptografados?

☐ Não ☐ Sim

60. O processo de solicitação de concessão de acessos é feito por e-mail ou sistema?

61. Os acessos são baseados e concedidos através do perfil por função?

62. São bloqueadas cópias e impressões das informações?

☐ Não ☐ Sim

63. Quem possui acesso a dados de clientes e a outros dados sensíveis são apenas colaboradores específicos a função?

☐ Não ☐ Sim

64. Esses acessos são monitorados e/ou registrados?

☐ Não ☐ Sim

65. Existe política de alteração de senha por tempo determinado?

☐ Não

☐ Sim, explicar

66. Possuem regras de Segurança da informação aplicadas como política de senhas, políticas de acessos, etc?

☐ Não

☐ Sim, explicar

67. Com qual frequência os dados passam por backup?

68. Os dados de backup são mantidos por no mínimo 5 anos?

69. É realizado o monitoramento das rotinas de backup?

☐ Não

☐ Sim, explicar

70. Cópias de backup são armazenadas em locais externos?

- [ ] Não
- [ ] Sim, explicar

71. Os testes de restore são efetuados pelo menos a cada 1 ano?

- [ ] Não
- [ ] Sim, explicar

72. Em quanto tempo o backup pode ser recuperado a partir do momento de ocorrência do ponto de falha?

73. Qual é a perda máxima de dados tolerável para a retomada dos processos da Empresa, após um incidente (RPO)?

74. O acesso ao serviço é realizado por conexão criptografada, preferencialmente via HTTPS usando TLS?

- [ ] Não
- [ ] Sim, explicar

75. Existe processo de Gestão de Vulnerabilidades no ambiente de TI?

- [ ] Não
- [ ] Sim, explicar

76. Os registros de eventos(log) são armazenados por um período?

- [ ] Não
- [ ] Sim, explicar

77. Os sistemas de desenvolvimento próprio da empresa possuem ambiente segregados DEV / Homologação/ QA /Produção?

- [ ] Não
- [ ] Sim, explicar

78. São realizados testes periódicos de intrusão (EHT) no ambiente/serviço?

- [ ] Não
- [ ] Sim, explicar

79. Existem padrões, processos e/ou ferramentas utilizadas para detectar ataque em sistema de rede (Network IDS, Firewall, WAF)?

- [ ] Não
- [ ] Sim, explicar

80. Qual modelo do equipamento (L3)?

81. Qual versão (Build) encontra-se?

82. Há Switchs internos na empresa?

- [ ] Não
- [ ] Sim, explicar quantos e quais modelos?

83. Os switchs são gerenciáveis? Se sim, sua gerência está separada em alguma DMZ ou na mesma rede?

- [ ] Não
- [ ] Sim, explicar

84. Os equipamentos de Wi-fi estão separados em uma DMZ ou estão na mesma LAN?

85. Existe bloqueio de portas livres e ou novas portas alocadas?

- [ ] Não
- [ ] Sim, explicar

86. A atualização do Firmware dos dispositivos Wi-fi é realizada quando disponível?

☐ Não
☐ Sim, explicar

87. O backup do Firewall e Switchs, se existentes, são guardados em locais seguros que apenas a equipe de SI tem acesso?

☐ Não
☐ Sim, explicar

88. Os backups são criptografados?

☐ Não ☐ Sim

89. Possuem solução implementada e configurada para monitoramento de e-mails (Ex.: DLP)?

☐ Não
☐ Sim, explicar

90. Os colaboradores foram orientados a utilizar o e-mail da empresa para fins pessoais?

☐ Não
☐ Sim, explicar

91. É bloqueado o recurso de Webmail ao sistema de correio eletrônico em funcionamento? Caso negativo, são monitorados os acessos e utilização do mesmo?

- [ ] Sim
- [ ] Não, explicar

92. Utilizam algum software de criptografia de e-mails enviados para Internet?

- [ ] Não
- [ ] Sim, explicar

93. Possui solução de backup efetuando a gravação de todos os tipos de mensagens das caixas de e-mail (enviadas, recebidas, excluídas)?

- [ ] Não
- [ ] Sim, explicar

94. É bloqueado o acesso do e-mail pessoal através da internet da empresa? Caso negativo, são monitorados a utilização do mesmo?

- [ ] Sim
- [ ] Não, explicar

95. Possui sistema de gravação telefônica instalado nos ramais? Caso afirmativo, as áreas críticas de negócios estão inseridas na gravação telefônica?

- [ ] Não
- [ ] Sim, explicar

96. A empresa utiliza acordos de conformidade e divulgação e conscientiza seus colaboradores a respeito?

- [ ] Não
- [ ] Sim, explicar

97. A empresa adota alguma metodologia de desenvolvimento seguro para os seus sistemas?

- [ ] Não
- [ ] Sim, explicar

98. Existem controles que assegurem a aderência à metodologia adotada?

- [ ] Não
- [ ] Sim, explicar

99. O desenvolvimento de sistemas é realizado por terceiro, é interno ou ambos?

100. Há algum colaborador e/ou equipe designados para esta posição de "gestão da segurança da informação"?

- [ ] Não
- [ ] Sim, explicar

101. Existe um "SOC" (Security Operations Center) ou um método de monitoramento de incidentes?

☐ Não

☐ Sim, explicar

102. Fornece um serviço de quarentena aos seus utilizadores?

☐ Não

☐ Sim, explicar

103. Tem a capacidade de excluir e avaliar automaticamente os anexos numa caixa de entrada para determinar se é malicioso antes da entrega ao utilizador final?

☐ Não

☐ Sim, explicar

104. Cumpri rigorosamente o Sender Policy Framework (SPF) nas mensagens de e-mail recebidas?

☐ Não

☐ Sim, explicar

105. O Proponente possui procedimentos documentados para responder a campanhas de Phishing (que tenham ou não a companhia como alvo)? Se sim, descreva os principais passos para responder a este tipo de incidente e com qual frequência é realizado o treinamento em Phishing para todo o pessoal (por exemplo, mensalmente, trimestralmente, anualmente)?

☐ Não

☐ Sim, explicar

106. Utiliza o Office 365 na sua organização? Se sim, utiliza o 365 Advanced Threat Protection nele?

☐ Não

☐ Sim, explicar

107. Utiliza o AMF para proteger contas de usuário administrativos?

☐ Não

☐ Sim, explicar

108. Uma configuração de base de hardware é estendida através de servidores, computadores portáteis, desktops e dispositivos móveis geridos?

☐ Não

☐ Sim, explicar

109. Que % da empresa é coberta pelas suas varreduras de vulnerabilidade programadas?

110. Qual é o tempo máximo para aplicação de patches críticos de segurança? (conforme determinado na política de aplicação de patches de segurança do Proponente)

- ☐ Não há política definida para aplicação de patches críticos de segurança.
- ☐ Dentro de 24h
- ☐ Entre 24 e 72 horas
- ☐ Entre 3 e 7 dias
- ☐ Mais de 7 dias

111. Qual o percentual de compliance do Proponente com seus padrões para deploy de patches críticos de segurança?

O Proponente não acompanha esta métrica

- ☐ >95%
- ☐ 90-95%
- ☐ 80-90%
- ☐ <80%

112. Se tiver algum software em fim de vida ou de suporte, está segregado do resto da rede?

- ☐ Não
- ☐ Sim, explicar

113. Configurou firewalls de rede e host-based para proibir as ligações de entrada padrão?

- ☐ Não
- ☐ Sim, explicar

114. Utiliza um serviço DNS protetor (por exemplo, Quad9, OpenDNS ou o PDNS do setor público)?

- ☐ Não
- ☐ Sim, explicar

115. Os utilizadores podem executar documentos MS Office Macro ativados no seu sistema padrão?

- [ ] Não
- [ ] Sim, explicar

116. A empresa utiliza contas privilegiadas utilizando ferramentas? E.g. CyberArk

- [ ] Não
- [ ] Sim, explicar

117. Tem um centro de operações de segurança estabelecido, seja internamente ou subcontratado?

- [ ] Não
- [ ] Sim, explicar

118. Utiliza um serviço de sincronização em nuvem (por exemplo, Dropbox, OneDrive, SharePoint, Google Drive) para efetuar cópias de segurança?

- [ ] Não
- [ ] Sim, explicar

119. Testou com sucesso a restauração e recuperação de configurações de servidores chave e dados de cópias de segurança nos últimos 6 meses?

- [ ] Não
- [ ] Sim, explicar

120. É capaz de testar a integridade das cópias de segurança antes da restauração para ter a certeza de que está livre de malware?

☐ Não

☐ Sim, explicar

121. Utiliza tecnologia de isolamento e contenção de aplicações finais? Os utilizadores podem executar documentos MS Office Macro ativados nos seus sistemas padrão?

☐ Não

☐ Sim, explicar

122. Fornecem aos seus funcionários um software de gestão de senhas?

☐ Não

☐ Sim, explicar

123. Em relação à segurança de endpoints e estações de trabalho, selecione todas as opções válida. Acrescentar quaisquer comentários adicionais sobre a segurança de endpoints:

☐ Todas as estações de trabalho possuem soluções de antivírus com capacidades de heurística.

☐ O Proponente utiliza soluções de segurança de endpoints com detecção de comportamento malicioso e capacidades de mitigação de exploits

☐ O Proponente possui um grupo interno que monitora o output das soluções de segurança de endpoint e investiga as anomalias.

☐ O Proponente possui um grupo interno que monitora o output das soluções de segurança de endpoint e investiga as anomalias.

124. Em relação ao monitoramento de logs das soluções de segurança, selecione a descrição que melhor reflete as capacidades do Proponente. (maiores detalhes podem ser fornecidos abaixo)

☐ O Proponente não possui equipe dedicada a monitorar as operações de segurança (Security Operations Center).

☐ O Proponente possui um Security Operations Center, mas não atua 24/7.

☐ O Proponente possui um Security Operations Center executado por um provedor de serviço (MSSP).

☐ O Proponente possui Security Operations Center 24/7 interno.

125. Qual é o tempo médio para o Proponente detectar e conter incidentes de segurança em estações de trabalho?

☐ O Proponente não mede este indicador

☐ Menor que 30 minutos.

☐ Entre 30 minutos e 2 horas

☐ O Proponente não mede este indicador.

☐ Mais de 8 horas

126. Com relação a controle de acessos a estações de trabalho, selecione a descrição abaixo que melhor reflete a postura do Proponente.

☐ Nenhum funcionário está no grupo de administradores ou possui privilégios de administrador local da estação de trabalho

☐ A política padrão é que nenhum funcionário seja membro do grupo de administradores e não tenham privilégios de administrador local; todas as exceções à política são documentadas.

☐ Alguns funcionários estão no grupo de administradores ou possuem privilégios de administrador local nas estações de trabalho.

☐ Não sabemos

127. Em relação à proteção de credenciais de acesso privilegiado, selecione todas as opções que se aplicam sobre a postura do Proponente.

☐ Administradores de sistemas possuem uma credencial única para acessos privilegiados para tarefas administrativas (separada da conta de usuário para o dia-a-dia de trabalho normal).

☐ Acessos privilegiados (incluindo administradores de domínio) requerem autenticação multi fator

☐ Credenciais de acesso privilegiado são mantidas em uma solução de cofre de senha que requer o registro de uso da credencial (com a rotação automática da senha posteriormente).

☐ Existem logs do uso de todas as contas de acesso privilegiado. Estes são mantidos por pelo menos 30 dias.

☐ Estações de trabalho privilegiadas (estações que não possuem acesso a internet e a e-mails) são utilizadas para administração de sistemas críticos (incluindo servidores de autenticação / controladores de domínio)

☐ Nenhuma das anteriores.

128. Em relação a segurança de sistemas acessíveis via internet, selecione todas as opções que se aplicam ao Proponente.

☐ O Proponente realiza testes de invasão pelo menos anualmente para avaliar a segurança dos sistemas acessíveis via internet

☐ O Proponente possui Web Application Firewall (WAF) configurado no modo bloqueio para proteção das aplicações acessíveis via internet

☐ O Proponente utiliza algum serviço externo para monitorar sua superfície de ataque (sistemas externos/acessíveis via internet).

☐ Nenhuma das opções acima

129. Inclua a data do último exercício de Ransomware, ou seja, teste das ações de resposta em um eventual incidente real de Ransomware, realizado pelo Proponente.

130. O Proponente possui um plano documentado para responder a um incidente de Ransomware? Em caso positivo, favor descrever os principais passos abaixo.

☐ Não

☐ Sim, explicar

131. Descreva quaisquer passos adicionais que a sua organização tome para detectar e prevenir ataques de resgate (por exemplo, segmentação da sua rede, ferramentas de software adicionais, serviços de segurança externos, etc.).

132. Descrever as ações futuras relativas a Segurança da Informação que serão implementadas no futuro.

133. O Proponente possui um plano documentado para responder a um incidente de ransomware? Em caso positivo, favor descrever os principais passos abaixo.

- ☐ Não
- ☐ Sim, explicar

134. Descreva quaisquer passos adicionais que a sua organização tome para detectar e prevenir ataques de resgate (por exemplo, segmentação da sua rede, ferramentas de software adicionais, serviços de segurança externos, etc.).

Nome e cargo do responsável

Local e data