**FORMULÁRIO DE AMOSTRA DE QUESTIONÁRIO DE AVALIAÇÃO DE RISCO DO FORNECEDOR**

|  |  |
| --- | --- |
| NOME DO FORNECEDOR | ENDEREÇO DO FORNECEDOR |
|   |   |
| PONTO DE CONTATO | INFORMAÇÕES DE CONTATO |
|   |   |

INSTRUÇÕES: Preencha este questionário por completo, deixando anotações e anexando a documentação de suporte sempre que necessário.

**Natureza do fornecedor de dados terá acesso a** *verificar tudo o que se aplica*

|  |  |  |
| --- | --- | --- |
| **X** | **TIPO DE DADOS** | **NOTAS** |
|  | Sem troca de dados |  |
|  | Dados demográficas |  |
|  | Dados financeiros |  |
|  | Dados pessoais (por exemplo, nome, endereço, número de telefone) |  |
|  | Dados pessoais não públicos (por exemplo, SSN, médico, proprietário) |  |
|  | Outros:  |  |  |

**POLÍTICAS AND PROCESSOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | A sua organização documenta, publica e aplica políticas de segurança? |  |
|  |  |  | Sua organização documenta e aplica políticas de RH? |  |
|  |  |  | Sua organização documenta e aplica políticas de uso autorizado de serviços em rede? |  |

**POLÍTICAS AND PROCESSOS** *continuaram*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | A sua organização documenta e aplica políticas de uso autorizado de e-mail, internet e intranet da empresa? |  |
|  |  |  | Sua organização documenta e aplica políticas e padrões de criptografia? |  |
|  |  |  | A sua organização documenta e aplica políticas relativas ao armazenamento, uso e eliminação de dados confidenciais? |  |
|  |  |  | Sua organização documenta e aplica políticas relativas ao armazenamento, uso e eliminação de dados confidenciais por terceiros? |  |
|  |  |  | Sua organização terceiriza funcionalidades relacionadas ao gerenciamento de segurança? |  |
|  |  |  | As políticas e procedimentos aderem e cumprem as leis e regulamentos de privacidade relacionados à segurança, ocultação e proteção de dados de clientes? |  |
|  |  |  | As penalidades associadas à não conformidade com as políticas da sua organização estão bem documentadas? |  |
|  |  |  | [Inserir políticas e processos em questão aqui] |  |
|  |  |  | [Inserir políticas e processos em questão aqui] |  |
|  |  |  | [Inserir políticas e processos em questão aqui] |  |

**MEDIDAS DE SEGURANÇA DO DATA CENTER AND FÍSICO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | Sua organização revisa e avalia regularmente os riscos físicos e ambientais? |  |
|  |  |  | Os controles de perímetro do data center envolvem o uso de cartões de acesso? |  |
|  |  |  | Os controles de perímetro do data center envolvem o uso de controles de teclado? |  |
|  |  |  | Os controles de perímetro do Data Center envolvem o uso de seguranças? |  |
|  |  |  | Os controles de perímetro do data center envolvem o uso de \_\_[adicionar medida aqui]\_\_? |  |
|  |  |  | Existem procedimentos de continuidade de negócios se o escritório estiver inacessível por algum motivo? |  |
|  |  |  | Todos os equipamentos de rede estão fisicamente protegidos? |  |
|  |  |  | Sua organização usa provedores de data center? |  |
|  |  |  | Sua organização usa registros de visitantes? Se assim for, eles são mantidos por mais de 30 dias? |  |
|  |  |  | Sua organização mantém uma política por escrito sobre os requisitos de segurança física do escritório? |  |
|  |  |  | [Inserir questão de segurança física e do data center aqui] |  |
|  |  |  | [Inserir questão de segurança física e do data center aqui] |  |

**MEDIDAS DE SEGURANÇA DO MALWARE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | Todos os e-mails são escaneados para obter vírus? |  |
|  |  |  | O software antivírus é obrigatório e habilitado em todos os computadores de rede? |  |
|  |  |  | O software antivírus tem uma frequência estabelecida de leitura em computadores de rede? |  |
|  |  |  | Sua organização permite a instalação de software não aprovado em computadores de rede? |  |
|  |  |  | [Inserir pergunta de segurança de Phisher aqui] |  |
|  |  |  | [Inserir pergunta de segurança de Phisher aqui] |  |
|  |  |  | [Inserir pergunta de segurança de Phisher aqui] |  |

**MEDIDAS DE SEGURANÇA DA INFORMAÇÃO**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | Sua organização possui um programa de segurança da informação em vigor? (Na coluna de notas, forneça um link para todas as políticas relevantes de segurança e privacidade voltadas para o público.) |  |
|  |  |  | Se a sua organização possui um programa de segurança da informação, isso se aplica a todas as operações e sistemas que processam dados confidenciais? |  |
|  |  |  | Os funcionários e gerentes relevantes são certificados profissionalmente em segurança da informação? |  |
|  |  |  | O acesso no nível do administrador é limitado em infraestrutura de rede? |  |
|  |  |  | Existem controles rígidos para acessar os registros de segurança? |  |
|  |  |  | [Inserir pergunta de segurança das informações aqui] |  |
|  |  |  | [Inserir pergunta de segurança das informações aqui] |  |
|  |  |  | [Inserir pergunta de segurança das informações aqui] |  |

**MEDIDAS DE SEGURANÇA DE INFRAESTRUTURA DE REDE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sim** | **Não** | **N/A** | **PERGUNTA** | **NOTAS** |
|  |  |  | Sua organização mantém uma política de segurança de rede? |  |
|  |  |  | Todos os roteadores são sistematizados com listas de controle de acesso para sufocar o tráfego não autorizado? |  |
|  |  |  | Os sistemas operacionais do servidor são remendados no nível mais recente? |  |
|  |  |  | Sua organização possui um processo para rastrear e comunicar patches de vulnerabilidade? |  |
|  |  |  | Sua organização faz backup de seus dados? |  |
|  |  |  | Os backups são armazenados e testados? |  |
|  |  |  | Os dispositivos dos funcionários são criptografados? |  |
|  |  |  | Um terceiro é usado para testar a segurança da infraestrutura de rede? |  |
|  |  |  | Você emprega sistemas de detecção de intrusão? |  |
|  |  |  | [Inserir questão de segurança da infraestrutura de rede aqui] |  |
|  |  |  | [Inserir questão de segurança da infraestrutura de rede aqui] |  |
|  |  |  | [Inserir questão de segurança da infraestrutura de rede aqui] |  |

|  |
| --- |
| **INFORMAÇÕES ADICIONAIS** |
|  |

|  |  |  |
| --- | --- | --- |
| NOME DO ASSESSOR DE RISCO AND TÍTULO | ASSINATURA | DATA |
|  |  |  |

|  |
| --- |
| **DISCLAIMER**Todos os artigos, modelos ou informações fornecidos pelo Smartsheet no site são apenas para referência. Embora nos esforcemos para manter as informações atualizadas e corretas, não fazemos representações ou garantias de qualquer tipo, expressas ou implícitos, sobre a completude, precisão, confiabilidade, adequação ou disponibilidade em relação ao site ou às informações, artigos, modelos ou gráficos relacionados contidos no site. Qualquer dependência que você deposita em tais informações está, portanto, estritamente em seu próprio risco. |