Modelo de Diagnóstico de Segurança da Informação (Controles - ISO 27.001 / ISO 27.002)

- **PROPÓSITO**: O diagnóstico situacional de segurança é fundamentado nos controles da ABNT/ISO 27.001 e na ABNT/ISO 27.002, e é uma importante ferramenta para identificar pontos positivos e negativos nos processos da organização. A partir dele, é possível visualizar a situação atual da organização quanto ao cenário da segurança da informação, com objetivo de identificar pontos de atenção e melhorias que contribuam para adequação à LGPD; ao final, o diagnóstico será orientador para propostas de ações, que quando executadas, em novo diagnóstico, permitirá uma análise comparativa da evolução da organização ao longo do projeto.

DESENVOLVIMENTO

Classificação 1 - Políticas de segurança da informação.

Grupo 1 - Orientação da Direção para segurança da informação.

Propósito de Grupo 1: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Questões do Grupo 1:

- Questão 1

Pergunta: A organização possui um conjunto de políticas de segurança da informação, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes?

Peso = 3

Orientação: Norma ISO 27.002 - 5.1.1 - Políticas para segurança da informação. Controle: Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

- Questão 2

Pergunta: Na política de segurança da informação há definição de segurança da informação, objetivos e princípios relativos à segurança da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 5.1.1 - Políticas para segurança da informação. Diretrizes para implementação: Convém que a política de segurança da informação contenha declarações relativas a: a) definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;

- Questão 3

Pergunta: Na política de segurança da informação há atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos?

Peso = 1

Orientação: Norma ISO 27.002 - 5.1.1 - Políticas para segurança da informação. Diretrizes para implementação: Convém que a política de segurança da informação contenha declarações relativas a: b) atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos;

- Questão 4

Pergunta: Na política de segurança da informação há processos para o tratamento dos desvios e exceções?

Peso = 1

Orientação: Norma ISO 27.002 - 5.1.1 - Políticas para segurança da informação. Diretrizes para implementação: Convém que a política de segurança da informação contenha declarações relativas a: c) processos para o tratamento dos desvios e exceções.

- Questão 5

Pergunta: As políticas de segurança da informação são analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia?

Peso = 3

Orientação: Norma ISO 27.002 - 5.1.2 - Análise crítica das políticas para segurança da informação. Controle: Convém que as políticas de segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

- Questão 6

Pergunta: As políticas de segurança da informação são analisadas criticamente em intervalos planejados e contam com evidências?

Peso = 1

Orientação: Item de controle ISO 27.001 - A.5.1.2 - Análise crítica das políticas para segurança da informação. As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

- Questão 7

Pergunta: Na política de segurança da informação, há definição de um responsável pelo desenvolvimento, análise crítica e avaliação?

Peso = 1

Orientação: Norma ISO 27002 - 5.1.2 - Análise crítica das políticas para segurança da informação. Diretrizes para implementação: Convém que cada política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança da informação.

Classificação 2 - Organização da segurança da informação.

Grupo 1 - Organização interna

Propósito de Grupo 1: Estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

Questões do Grupo 1:

- Questão 1

Pergunta: A organização possui um responsável pelo desenvolvimento e implementação da segurança da informação, e para apoiar na identificação de controles?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.6.1.1 - Responsabilidades e papéis da segurança da informação. Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas.

- Questão 2

Pergunta: Funções conflitantes e áreas de responsabilidade são segregadas buscando reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização?

Peso = 3

Orientação: Convém que o princípio seja aplicado tanto quanto possível e praticável. Convém que sempre que seja difícil segregar, outros controles como monitoração das atividades, trilha de auditoria e supervisão da gestão sejam considerados. Convém que funções de responsabilidade sejam separadas para evitar interesses comuns.

- Questão 3

Pergunta: A organização possui procedimentos implementados que especifiquem quando e quais autoridades serão contatadas e como os incidentes de segurança da informação identificados serão reportados em tempo hábil?

Peso = 3

Orientação: Convém que estejam sendo mantidos contatos com autoridades policiais, órgãos reguladores, a fim de garantir a tomada rápida de providências e orientações em casos de incidente de segurança da informação.

- Questão 4

Pergunta: São mantidos contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação?

Peso = 3

Orientação: Convém que estejam sendo mantidos contatos apropriados com provedores de serviços de informação, fóruns especializados a fim de garantir a tomada rápida de providências e orientações em casos de incidente de segurança da informação.

- Questão 5

Pergunta: A organização conduz uma avaliação dos riscos de segurança da informação em estágios iniciais do projeto para identificar os controles que são necessários?

Peso = 3

Orientação: Convém que a segurança da informação esteja sendo considerada em todo gerenciamento de projeto adotado pela organização como princípio.

Grupo 2 - Trabalho remoto

Propósito de Grupo 2: Garantir a segurança das informações no trabalho remoto e no uso de dispositivos móveis.

Questões do Grupo 2:

- Questão 1

Pergunta: A organização possui uma política de dispositivos móveis, levando em consideração os riscos de se trabalhar com esses dispositivos em ambientes desprotegidos, a proteção física, técnicas criptográficas, proteção contra malware, backups, desativação, bloqueio e exclusão de forma remota?

Peso = 3

Orientação: Convém que esteja sendo adotada política e medidas para o gerenciamento de riscos de segurança da informação que o uso de dispositivos móveis (smartphone, tablet, notebook e outros dispositivos) podem trazer para a organização.

- Questão 2

Pergunta: A organização realiza campanhas de conscientização para os usuários quanto aos riscos adicionais decorrentes dispositivos móveis e os controles necessários?

Peso = 1

Orientação: Convém que todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados.

- Questão 3

Pergunta: A política de dispositivos móveis leva em consideração o uso de dispositivos pessoais?

Peso = 1

Orientação: Convém que a organização esteja ciente da utilização de dispositivos de uso pessoal dos colaboradores para o desenvolvimento de suas atividades e dos riscos que isso pode acarretar para a organização.

Item de controle ISO 27.001 - A.6.2.1 - Política para o uso de dispositivo móvel. Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.

- Questão 4

Pergunta: Para prover acesso às informações do negócio, a seus colaboradores, em dispositivos pessoais, a organização realiza a coleta de assinatura do Termo de Acordo de Conhecimento e Responsabilidades, pelo qual o colaborar renúncia direitos autorais dos dados do negócio ou garante a exclusão remota dos dados a ser feita pela organização?

Peso = 1

Orientação: Norma ISO 27.002 - 6.2.1 - Política para o uso de dispositivo móvel. Diretrizes para implementação: Onde a política de dispositivos móveis permite o uso de dispositivos pessoais, convém que esta política e os controles de segurança relacionados também considerem: b) prover acesso às informações do negócio somente depois que os usuários assinarem o acordo de conhecimento das suas responsabilidades(quanto a proteção física, atualização do software, entre outros), renunciando direitos autorais dos dados do negócio, permitindo a exclusão remota dos dados pela organização no caso de furto, roubo ou perda do dispositivo móvel ou, ainda, quando não mais houver autorização para o uso dos serviços. Esta política precisa levar em consideração a legislação sobre privacidade.

- Questão 5

Pergunta: É implementada política e medidas que apoiam a segurança da informação para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto?

Peso = 3

Orientação: Norma ISO 27.002 - 6.2.2 - Trabalho remoto. Diretrizes para implementação: Convém que a organização que permita a atividade de trabalho remoto publique uma política que define as condições e restrições para o uso de trabalho remoto.

- Questão 6

Pergunta: A organização possui campanhas de conscientização para orientar os usuários sobre os riscos de segurança da informação durante o uso do trabalho remoto?

Peso = 1

Orientação: Convém que todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados.

Classificação 3 - Segurança em recursos humanos.

Grupo 1 - Antes da contratação

Propósito de Grupo 1: Assegurar que funcionários e partes externas entendam as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Questões do Grupo 1:

- Questão 1

Pergunta: Durante o processo de seleção são verificados a disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal?

Peso = 3

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretrizes para a implementação: Convém que as verificações levem em consideração toda a legislação relativa à privacidade, proteção da informação de identificação de pessoal e do emprego e, onde permitido, incluam os seguintes itens: a) disponibilidades de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal.

- Questão 2

Pergunta: É realizada a confirmação das qualificações acadêmicas e profissionais no processo de seleção de colaboradores?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretrizes para a implementação: Convém que as verificações levem em consideração toda a legislação relativa à privacidade, proteção da informação de identificação de pessoal e do emprego e, onde permitido, incluam os seguintes itens: b) uma verificação (da exatidão e completeza) das informações do curriculum vitae do candidato; c) confirmação das qualificações acadêmicas e profissionais.

- Questão 3

Pergunta: É realizada uma verificação independente da identidade (através de passaporte ou documento similar)?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretrizes para a implementação: Convém que as verificações levem em consideração toda a legislação relativa à privacidade, proteção da informação de identificação de pessoal e do emprego e, onde permitido, incluam os seguintes itens: d) verificação independente da identidade(passaporte ou documento similar).

- Questão 4

Pergunta: É realizada uma verificação mais detalhada, como verificações de crédito ou registros criminais?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretrizes para a implementação: Convém que as verificações levem em consideração toda a legislação relativa à privacidade, proteção da informação de identificação de pessoal e do emprego e,

onde permitido, incluam os seguintes itens: e) verificação mais detalhadas, como verificações de crédito ou verificações de registros criminais.

- Questão 5

Pergunta: Se o indivíduo for contratado para desempenhar o papel de segurança da informação, a organização certifica-se que o candidato tem a competência necessária para desempenhar o papel?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretrizes para a implementação: Convém que, quando um indivíduo for contratado para desempenhar o papel de segurança da informação, a organização certifique-se de que o candidato: a) tem a competência necessária para executar o papel de segurança da informação; b) possa ser confiável para desempenhar o papel, especialmente se o papel for crítico para a organização.

- Questão 6

Pergunta: Quando da contratação de fornecedores e partes externas para atuação na área de segurança da informação, são aplicados os mesmos critérios de seleção previstos na contratação de funcionários para a área de segurança da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.1 - Seleção. Diretriz para a implementação: Convém que um processo de seleção também seja feito para fornecedores e partes externas aplicando-se os mesmos critérios utilizados para a seleção de funcionários.

- Questão 7

Pergunta: Todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinam um Termo de Confidencialidade ou de Não Divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação?

Peso = 3

Orientação: Norma ISO 27.002 - 7.1.2 - Termos e condições de contratação. Diretrizes para implementação: Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando: a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação;

- Questão 8

Pergunta: O Termo de Confidencialidade ou de Não Divulgação define as responsabilidades legais e direitos dos funcionários e partes externas, com relação às leis de direitos autorais e legislação de proteção de dados?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.2 - Termos e condições de contratação. Diretriz para implementação: Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando: b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados;

- Questão 9

Pergunta: Funcionários ou partes externas são esclarecidos em relação às responsabilidades pelo tratamento da informação na organização, recebida de outras companhias ou partes interessadas?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.2 - Termos e condições de contratação. Diretriz para implementação: Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando: d) as responsabilidades dos funcionários ou partes externas pelo tratamento da informação recebida de outras companhias ou partes interessadas;

- Questão 10

Pergunta: Funcionários ou partes externas são orientados em relação a ações a serem tomadas no caso de desrespeito aos requisitos de segurança da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.2 - Termos e condições de contratação. Diretriz para implementação: Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando: e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.

- Questão 11

Pergunta: Papéis e responsabilidades de segurança da informação são comunicados no termo de confidencialidade?

Peso = 1

Orientação: Norma ISO 27.002 - 7.1.2 - Termos e condições de contratação. Diretriz para implementação: Convém que os papéis e responsabilidades de segurança da informação sejam comunicados aos candidatos ao emprego durante o processo de pré-contratação.

Grupo 2 - Durante a contratação

Propósito de Grupo 2: Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

Questões do Grupo 2:

- Questão 1

Pergunta: Há demonstração da Direção da SIGNOVE aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.7.2.1 - Responsabilidades da Direção. A Direção deve requerer aos funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.

- Questão 2

Pergunta: Existe um programa de conscientização em segurança da informação formalizado para funcionários da organização e partes externas relevantes para suas funções?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.7.2.2 - Conscientização, educação e treinamento em segurança da informação. Todos os funcionários da organização e, onde pertinente, as partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

- Questão 3

Pergunta: Existe um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários e partes externas que tenham cometido uma violação de segurança da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.7.2.3 - Processo disciplinar. Deve existir um processo disciplinar formal, implantado e comunicado, para tomar ações

contra funcionários que tenham cometido uma violação de segurança da informação.

Grupo 3 - Encerramento e mudança da contratação

Propósito de Grupo 3: Proteger os interesses da SIGNOVE como parte do processo de mudança ou encerramento da contratação.

Questões do Grupo 3:

- Questão 1

Pergunta: Existe um processo formal e implementado para comunicação de encerramento na contratação, para realizar os devidos bloqueios de acesso?

Peso = 3

Orientação: Convém que as áreas durante do processo de encerramento da contratação comuniquem a área responsável para realizar os devidos bloqueios.

- Questão 2

Pergunta: Existe um processo formal e implementado para comunicação de mudanças na contratação, para que as devidas alterações de perfil sejam estabelecidas?

Peso = 3

Orientação: Convém que as áreas durante do processo de mudanças na contratação comunique a área responsável para realizar os devidos bloqueios.

- Questão 3

Pergunta: Existe um processo formal e implementado para comunicação e encerramento de um prestador de serviço para realizar os devidos bloqueios de acesso?

Peso = 1

Orientação: Convém que as áreas durante do processo de encerramento da contratação comuniquem a área responsável para realizar os devidos bloqueios.

Classificação 4 - Gestão de Ativos.

Grupo 1 - Responsabilidade pelos ativos

Propósito de Grupo 1: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

Questões do Grupo 1:

- Questão 1

Pergunta: A organização possui identificação e inventário de ativos de informação de forma estruturada e atualizada?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.1.1 - Inventário de ativos. Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido.

- Questão 2

Pergunta: Os ativos mantidos no inventário da organização possuem um proprietário?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.1.2 - Proprietário dos ativos. Os ativos mantidos no inventário devem ter um proprietário.

- Questão 3

Pergunta: As regras para o uso aceitável das informações, dos ativos associados com informação e os recursos de processamento da informação são identificados, documentados e implementados?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.1.3 - Uso aceitável dos ativos - Regras para o uso aceitável das informações, dos ativos associados com informação e os recursos de processamento da informação devem ser identificados, documentados e implementados.

- Questão 4

Pergunta: Todos os funcionários e partes externas devolvem todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo?

Peso = 3

Orientação: Norma ISO 27.002 - 8.1.4 - Devolução de ativos. Controle: Convém que todos os funcionários e partes externas devolvam todos os seus ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou do acordo.

- Questão 5

Pergunta: Existem procedimentos adotados para assegurar que toda a informação relevante seja transferida para a SIGNOVE em casos de uso de equipamentos pessoais ou casos em que um funcionário ou partes externas comprem o equipamento da organização?

Peso = 1

Orientação: Norma ISO 27.002 - 8.1.4 - Devolução de ativos. Diretrizes para implementação: Convém que no caso em que o funcionário ou partes externas comprem o equipamento da organização ou usem o seu próprio equipamento pessoal, procedimentos sejam adotados para assegurar que toda a informação relevante seja transferida para a organização e seja apagada de forma segura do equipamento.

Grupo 2 - Classificação da informação

Propósito de Grupo 2: Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização.

Questões do Grupo 2:

- Questão 1

Pergunta: A organização possui uma diretriz sobre classificação das informações, levando em consideração a sua sensibilidade e criticidade, em termos de confidencialidade, integridade e disponibilidade?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.2.1 - Classificação da Informação. A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

- Questão 2

Pergunta: Sabendo que algumas informações são mais sensíveis e críticas do que outras, e que alguns itens podem exigir um nível adicional de proteção ou manuseio especial, a organização utiliza um sistema de classificação para definir um conjunto apropriado de níveis de proteção?

Peso = 1

Orientação: Uma das formas mais usadas é tratar a informação como confidencial, restrita, de uso interno ou público, mas cada organização define o seu nível de controle.

- Questão 3

Pergunta: É desenvolvido e implementado um conjunto apropriado de procedimentos para rotular e tratar a informação de acordo com o esquema de classificação da informação adotado pela organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.2.2 - Rótulos e tratamento da informação. Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

- Questão 4

Pergunta: A organização possui uma diretriz sobre rotulagem da informação, tanto para os formatos físicos e eletrônicos, orientando sobre onde e como os rótulos devem ser colocados, como a informação é acessada ou ativos são manuseados, em função dos tipos de mídias?

Peso = 1

Orientação: Tipos de rotulagens: uso interno, restrita, confidencial, pública, privada, secreta.

- Questão 5

Pergunta: A organização possui uma diretriz para tratamento, processamento, armazenamento e transmissão da informação, de acordo com a sua classificação?

Peso = 3

Orientação: Norma ISO 27.002 - 8.2.3 - Tratamento dos Ativos. Diretrizes para implementação: Convém que procedimentos sejam estabelecidos para o tratamento, processamento, armazenamento e transmissão da informação, de acordo com a sua classificação.

Grupo 3 - Tratamento de mídias

Propósito de Grupo 3: Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.

Questões do Grupo 3:

- Questão 1

Pergunta: A organização possui uma diretriz implementada para o gerenciamento de mídias removíveis, levando em consideração recursos tecnológicos que permitam trilhas de auditoria em mídia removíveis?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.3.1 - Gerenciamento de mídias removíveis. Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

- Questão 2

Pergunta: A organização possui uma diretriz implementada para o gerenciamento de mídias removíveis, levando em consideração a guarda segura em um ambiente protegido da mídia removível?

Peso = 1

Orientação: Norma ISO 27.002 - 8.3.1 - Gerenciamento de mídias removíveis. Diretrizes para a implementação: Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas: c) toda mídia seja guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

- Questão 3

Pergunta: A organização possui uma diretriz implementada para o gerenciamento de mídias removíveis, levando em consideração técnicas de criptografia da informação na mídia removível?

Peso = 1

Orientação: Norma ISO 27.002 - 8.3.1 - Gerenciamento de mídias removíveis. Diretrizes para a implementação: Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas: d) convém que sejam usadas, no caso em que a integridade ou confidencialidade dos dados sejam considerações importantes, técnicas de criptografia, para proteger os dados da mídia removível;

- Questão 4

Pergunta: A organização possui uma diretriz implementada para o gerenciamento de mídias removíveis, levando em consideração a degradação na mídia removível?

Peso = 1

Orientação: Norma ISO 27.002 - 8.3.1 - Gerenciamento de mídias removíveis. Diretrizes para a implementação: Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas: e) para mitigar o risco de degradar a mídia enquanto os dados armazenados ainda são necessários, convém que os dados sejam transferidos para uma mídia nova antes de se tornarem ilegíveis;

- Questão 5

Pergunta: A organização possui uma diretriz implementada para o gerenciamento de mídias removíveis, levando em consideração a transferência da mídia removível?

Peso = 1

Orientação: Norma ISO 27.002 - 8.3.1 - Gerenciamento de mídias removíveis. Diretrizes para a implementação: Convém que as seguintes diretrizes para o gerenciamento de mídias removíveis sejam consideradas: i) onde houver a necessidade para o uso de mídia removível, a transferência da informação contida na mídia seja monitorada.

- Questão 6

Pergunta: A organização possui um procedimento formal para o descarte seguro de mídias para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.3.2 - Descarte de mídias. As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.

Norma ISO 27.002 - 8.3.2 - Descarte de mídias. Diretrizes para implementação: Convém que procedimentos formais para o descarte seguro das mídias sejam definidos para minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas. Os procedimentos para descarte seguro das mídias, contendo informações confidenciais, sejam proporcionais à sensibilidade das informações.

- Questão 7

Pergunta: As mídias que possuem informações são protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte entre organizações ou setores?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.8.3.3 - Transferência física de mídias. Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrompida, durante o transporte.

Classificação 5 - Controle de acesso.

Grupo 1 - Requisitos do negócio para controle de acesso.

Propósito de Grupo 1: Limitar o acesso à informação e aos recursos de processamento da informação.

Questões do Grupo 1:

- Questão 1

Pergunta: A política de controle de acesso define requisitos para autorização formal de pedidos de acesso?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.1.1 - Política de controle de acesso. Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

Norma ISO 27.002 - 9.1.1 - Política de controle de acesso. Diretrizes para implementação: Convém que a política leve em consideração os seguintes itens: g) requisitos para autorização formal de pedidos de acesso;

- Questão 2

Pergunta: A política de controle de acesso define requisitos para análise crítica periódica de direitos de acesso e remoção dos direitos de acesso?

Peso = 1

Orientação: Norma ISO 27.002 - 9.1.1 - Política de controle de acesso. Diretrizes para implementação: Convém que a política leve em consideração os seguintes itens: h) requisitos para análise crítica periódica de direitos de acesso;

- Questão 3

Pergunta: A política de controle de acesso define regras para o acesso privilegiado?

Peso = 1

Orientação: Norma ISO 27.002 - 9.1.1 - Política de controle de acesso. Diretrizes para implementação: Convém que a política leve em consideração os seguintes itens: k) regras para o acesso privilegiado.

- Questão 4

Pergunta: A política de acesso define regras para os usuários de férias ou afastados?

Peso = 1

Orientação: Convém que a política leve em consideração regras para os usuários de férias e afastados.

- Questão 5

Pergunta: Os usuários somente recebem acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar?

Peso = 3

Orientação: Convém que uma política seja formulada com relação ao uso de redes e serviços de rede. Item de controle ISO 27.001 - A.9.1.2 - Acesso às redes e aos serviços de rede. Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

Grupo 2 - Gerenciamento de acesso do usuário

Propósito de Grupo 2: Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.

Questões do Grupo 2:

- Questão 1

Pergunta: O uso de ID de usuário é único e que esses estejam aprovados e documentados?

Peso = 3

Orientação: Norma ISO 27.002 - 9.2.1 - Registro e cancelamento de usuário. Diretrizes para implementação: Convém que o processo para gerenciar o ID de usuário inclua: a) o uso de um ID único, para permitir relacionar os usuários às suas responsabilidades e ações; convém que o uso compartilhado dos ID de usuário somente seja permitido onde eles são necessários por razões operacionais ou de negócios, e convém que seja aprovado e documentado.

- Questão 2

Pergunta: O uso de ID de usuário compartilhado é permitido somente onde necessários por razões operacionais ou de negócios, e que esses estejam aprovados e documentados?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.1 - Registro e cancelamento de usuário. Diretrizes para implementação: Convém que o processo para gerenciar o ID de usuário inclua: a) o uso de um ID único, para permitir relacionar os usuários às suas responsabilidades e ações; convém que o uso compartilhado dos ID de usuário

somente seja permitido onde eles são necessários por razões operacionais ou de negócios, e convém que seja aprovado e documentado.

- Questão 3

Pergunta: É implementado um processo formal de provisionamento de acesso do usuário para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços?

Peso = 3

Orientação: Provisionamento de usuários é a criação e gerenciamento de acesso aos recursos da empresa. O acesso pode variar de contas de TI (Sistema, e-mail, rede, etc.) para equipamentos e recursos que NÃO sejam de TI (crachá de acesso, telefone, carro, etc.), de acordo com a função exercida. Devendo levar em consideração a mudança de setor e até mesmo a revogação no caso de dispensa do usuário. Item de controle ISO 27.001 - A.9.2.2 - Provisionamento para acesso de usuário. Um processo formal de provisionamento de acesso ao usuário deve ser implementado para conceder ou revogar os direitos de acesso para todos os tipos de usuários em todos os tipos de sistemas e serviços.

- Questão 4

Pergunta: Os direitos de acessos privilegiados são atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio?

Peso = 3

Orientação: Norma ISO 27.002 - 9.2.3 - Gerenciamento de direitos de acesso privilegiado. Diretrizes para implementação: Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um processo de autorização formal, de acordo com a política de controle de acesso pertinente. Convém que os seguintes passos sejam considerados: e) os direitos de acesso privilegiado sejam atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio. As atividades normais do negócio não sejam desempenhadas usando ID privilegiados;

- Questão 5

Pergunta: Os direitos de acessos privilegiados são analisados criticamente a intervalos regulares?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.3 - Gerenciamento de direitos de acesso privilegiado sejam restritos e controlados. Diretrizes para implementação: Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um processo de autorização formal, de acordo com a política de controle de acesso

pertinente: f) as competências dos usuários com direitos de acesso privilegiado sejam analisadas criticamente a intervalos regulares, para verificar se eles estão alinhados com as suas obrigações;

- Questão 6

Pergunta: Os direitos de acessos privilegiados estabelecem que o usuário administrador genérico seja evitado?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.3 - Gerenciamento de direitos de acesso privilegiado sejam restritos e controlados. Diretrizes para implementação: Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um processo de autorização formal, de acordo com a política de controle de acesso pertinente: g) procedimentos específicos sejam estabelecidos e mantidos para evitar o uso não autorizado dos ID de usuário de administrador genérico, de acordo com as capacidades de configuração dos sistemas;

- Questão 7

Pergunta: Os direitos de acessos privilegiados estabelece que um usuário ao deixar a organização e que utilize ID de usuário administrador genérico, tenha sua senha alterada?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.3 - Gerenciamento de direitos de acesso privilegiado sejam restritos e controlados. Diretrizes para implementação: Convém que a alocação de direitos de acesso privilegiado seja controlada por meio de um processo de autorização formal, de acordo com a política de controle de acesso pertinente: h) para os ID de usuário de administrador genéricos, a confidencialidade da informação de autenticação secreta seja mantida quando for compartilhada (por exemplo, mudanças de senhas com frequência e tão logo quanto possível, quando um usuário privilegiado deixa a organização ou muda de função, comunicação entre os usuários privilegiados por meio de mecanismos apropriados).

- Questão 8

Pergunta: Os usuários assinam uma declaração, orientando manter a confidencialidade da informação de autenticação secreta e as senhas de grupos de trabalho?

Peso = 3

Orientação: Norma ISO 27.002 - 9.2.4 - Gerenciamento da informação de autenticação secreta de usuários. Diretrizes para implementação: Convém que o processo inclua os seguintes requisitos: a) solicitar aos usuários a assinatura de

uma declaração, para manter a confidencialidade da informação de autenticação secreta e para manter as senhas de grupos de trabalho, exclusivamente com os membros do grupo; esta declaração assinada pode ser incluída nos termos e condições de contratação. Item de controle ISO 27.001 - A.9.2.4 - Gerenciamento da informação de autenticação secreta de usuários. A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal.

- Questão 9

Pergunta: A organização estabelece uma autenticação secreta temporária, a qual o usuário é obrigado a alterar no primeiro uso?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.4 - Gerenciamento da informação de autenticação secreta de usuários. Diretrizes para implementação: Convém que o processo inclua os seguintes requisitos: b) garantir, onde os usuários necessitam manter suas próprias informações de autenticação secreta, que lhes seja fornecida uma informação de autenticação secreta temporária, a qual o usuário é obrigado a alterar no primeiro uso;

- Questão 10

Pergunta: A informação de autenticação secreta temporária é única para uma pessoa e não é fácil de ser adivinhada?

Peso = 1

Orientação: Norma ISO 27.002 - 9.2.4 - Gerenciamento da informação de autenticação secreta de usuários. Diretrizes para implementação: Convém que o processo inclua os seguintes requisitos: e) informação de autenticação secreta temporária seja única para uma pessoa e não seja fácil de ser adivinhada;

- Questão 11

Pergunta: Os proprietários de ativos analisam criticamente os direitos de acesso dos usuários, a intervalos regulares?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.2.5 - Análise crítica dos direitos de acesso do usuário. Os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários a intervalos regulares.

- Questão 12

Pergunta: Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação são retirados após o

encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.2.6 - Retirada ou ajuste dos direitos de acesso. Os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.

Grupo 3 - Responsabilidades dos usuários

Propósito de Grupo 3: Tornar os usuários responsáveis pela proteção das suas informações de autenticação.

Questões do Grupo 3:

- Questão 1

Pergunta: Os usuários são orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta (senha)?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.3.1 - Uso de informação de autenticação secreta. Os usuários devem ser orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

Grupo 4 - Controle de acesso ao sistema e à aplicação

Propósito de Grupo 4: Prevenir o acesso não autorizado aos sistemas e aplicações

Questões do Grupo 4:

- Questão 1

Pergunta: O acesso à informação e às funções dos sistemas de aplicações são restritos de acordo com a Política de Controle de Acesso?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.4.1 - Restrição de acesso à informação. O acesso à informação e às funções dos sistemas de aplicações deve ser restrito de acordo com a política de controle de acesso.

- Questão 2

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como não mostrar identificadores de sistema até que o processo tenha sido concluído com sucesso?

Peso = 3

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Diretrizes para implementação: Convém que um bom procedimento de entrada no sistema (log-on): a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso;

- Questão 3

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como não fornecer mensagens de ajuda durante o procedimento de entrada que poderiam auxiliar um usuário não autorizado?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Diretrizes para implementação: Convém que um bom procedimento de entrada no sistema (log-on): c) não forneça mensagens de ajuda durante o procedimento de entrada (log-on) que poderiam auxiliar um usuário não autorizado;

- Questão 4

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como, por exemplo, em condição de erro o sistema não indicar qual parte do dado de entrada está correta ou incorreta?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Diretrizes para implementação: Convém que um bom procedimento de entrada no sistema (log-on): d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correta ou incorreta;

- Questão 5

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como registro de tentativas de acesso ao sistema?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): e) proteja contra tentativas forçadas de entrada no sistema (log-on); f) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida;

- Questão 6

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, sejam elas, sem sucesso e bem sucedidas?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): f) registre tentativas de acesso ao sistema, sem sucesso e bem sucedida; Item de controle ISO 27.001 - A.9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on).

- Questão 7

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como não mostrar a senha que está sendo informada?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): i) não mostre a senha que está sendo informada;

- Questão 8

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como não transmitir senhas em texto claro pela rede?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): j) não transmita a senha em texto claro pela rede;

- Questão 9

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como encerrar sessões inativas após um período definido de inatividade?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): k) encerre sessões inativas após um período definido de inatividade, especialmente em locais de alto risco, como locais públicos, ou áreas externas ao gerenciamento de segurança da organização ou quando do uso de dispositivos móveis;

- Questão 10

Pergunta: A organização possui procedimentos para minimizar a oportunidade de acessos não autorizados em sistemas e aplicações, como registros de data e hora de log-on com sucesso e tentativas sem sucesso de entrada?

Peso = 1

Orientação: Norma ISO 27.002 - 9.4.2 - Procedimentos seguros de entrada no sistema (log-on). Convém que um bom procedimento de entrada no sistema (log-on): h) mostre as seguintes informações quando o procedimento de entrada no sistema de (log-on) finalizar com sucesso: 1) data e hora da última entrada no sistema (log-on) com sucesso; 2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (log-on) desde o última acesso com sucesso;

- Questão 11

Pergunta: Sistemas para gerenciamento de senhas são interativos e asseguram senhas de qualidade?

Peso = 3

Orientação: Norma ISO 27.002 - 9.4.3 - Sistema de Gerenciamento de Senha. Diretrizes para implementação: Obrigue o uso individual de ID de usuário e senha para manter responsabilidades; Permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros; Obrigue a escolha de senhas de qualidade; Obrigue os usuários a mudarem as senhas temporárias no primeiro acesso ao sistema; Force as mudanças de senha a intervalos regulares.

- Questão 12

Pergunta: A SIGNOVE possui diretrizes para o uso de programas utilitários que possam ser capazes de sobrepor os controles dos sistemas?

Peso = 3

Orientação: Convém que a organização tenha diretrizes no gerenciamento de instalações de programas utilitários que sobreponham ou entrem em conflito com as aplicações já instaladas, seja no servidor ou desktop. Item de controle ISO 27.001 - A.9.4.4 - Uso de programas utilitários privilegiados. O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.

- Questão 13

Pergunta: A organização possui bibliotecas de programa-fonte para controle de código-fonte de programa e de itens associados, com a finalidade de prevenir a introdução de funcionalidade não autorizada e para evitar mudanças não intencionais e manter a confidencialidade de propriedade intelectual?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.9.4.5 - Controle de acesso ao código-fonte de programas. O acesso ao código-fonte do programa deve ser restrito.

Classificação 6 - Criptografia.

Grupo 1 - Controles criptográficos

Propósito de Grupo 1: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Questões do Grupo 1:

- Questão 1

Pergunta: São desenvolvidas e implementadas políticas para o uso de controles criptográficos para a proteção da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.10.1.1 - Política para o uso de controles criptográficos. Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.

- Questão 2

Pergunta: São desenvolvidas e implementadas políticas sobre o uso, proteção e tempo de vida das chaves criptográficas ao longo de todo o seu ciclo de vida?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.10.1.2 - Gerenciamento de chaves. Uma política sobre o uso, proteção e tempo de vida das chaves criptográficas deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida.

Classificação 7 - Segurança física e do ambiente

Grupo 1 - Áreas seguras

Propósito de Grupo 1: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.

Questões do Grupo 1:

- Questão 1

Pergunta: Nas instalações onde há o processamento da informação existe um estudo do perímetro para se evitar brecha de segurança? (Ex: paredes externas do local sejam de construção robusta, portas externas sejam adequadamente protegidas contra acesso não autorizado, proteção externa para janelas).

Peso = 3

Orientação: Item de controle ISO 27.001 - A.11.1.1 - Perímetro de segurança física. Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.

- Questão 2

Pergunta: Existe uma recepção ou outro meio para controlar o acesso físico ao local ou edifício?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.1 - Perímetro de segurança física. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física: c) convém que seja implementada uma área de recepção, ou outro meio para controlar o acesso físico ao local ou ao edifício; convém que o acesso aos locais ou edifícios fique restrito somente ao pessoal autorizado;

- Questão 3

Pergunta: Existem outras barreiras físicas para impedir o acesso físico não autorizado?

Peso = 1

Orientação: Normas ISO 27.002 - 11.1.1 - Perímetro de segurança física. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física: d) convém que sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;

- Questão 4

Pergunta: A organização possui portas corta-fogo providas de alarme, monitoradas e testadas?

Peso = 1

Orientação: Normas ISO 27.002 - 11.1.1 - Perímetro de segurança física. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física: e) convém que todas as portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; convém que elas funcionem de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas.

- Questão 5

Pergunta: Existem sistemas de detecção de intrusos no perímetro físico instalados e testados em intervalos regulares? E que cubram todas as portas externas e janelas acessíveis?

Peso = 1

Orientação: Normas ISO 27.002 - 11.1.1 - Perímetro de segurança física. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física: f) convém que sistemas de detecção de intrusos, de acordo com normas regionais, nacionais e internacionais aceitáveis, sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis;

- Questão 6

Pergunta: As áreas seguras são protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.11.1.2 - Controles de entrada física. As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

- Questão 7

Pergunta: Existe um registro de data e a hora da entrada e saída de visitantes, assim como a validação de identidade dos visitantes?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: a) convém que a data e a hora da entrada e saída dos visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado. Convém que a identidade dos visitantes seja autenticada por meios apropriados.

- Questão 8

Pergunta: É mantida uma trilha de auditoria eletrônica ou um livro de registro dos acessos físicos?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: c) convém que uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos sejam mantida e monitorada de forma segura;

- Questão 9

Pergunta: Existe um procedimento formal exigindo que colaboradores, fornecedores, partes externas e visitantes tenham alguma forma visível de identificação?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: d) convém que seja exigido de todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação;

- Questão 10

Pergunta: Existe um procedimento formal orientando colaboradores no caso de encontrarem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes

diretrizes: d) convém que seja exigido de todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação e que eles avisem imediatamente ao pessoal de segurança, caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;

- Questão 11

Pergunta: Terceiros que realizam serviço de suporte em área segura, possuem acesso somente sob autorização e são monitorados?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: e) às partes externas que realizam serviços de suporte, convém que seja concedido acesso restrito às áreas seguras ou as instalações de processamento de informações sensíveis somente quando necessário; convém que este acesso seja autorizado e monitorado;

- Questão 12

Pergunta: Existe uma revisão de acesso a áreas seguras em intervalos regulares?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.2 - Controles de entrada física. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: f) convém que os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário.

- Questão 13

Pergunta: É projetada e aplicada segurança física para escritórios, salas e instalações?

Peso = 3

Orientação: Item de controle ISO 27.001 - 11.1.3 - Segurança em escritórios, salas e instalações. Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.

- Questão 14

Pergunta: As salas que possuem processamento de informações estão localizadas em local que evite o acesso do público?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.3 - Segurança em escritórios, salas e instalações. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para proteger escritórios, salas e instalações: a) convém que as instalações-chave sejam localizadas de maneira a evitar o acesso do público;

- Questão 15

Pergunta: A sala de processamento de informações possui a menor indicação possível da sua finalidade ou que identifique a presença de atividades de processamento de informações?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.3 - Segurança em escritórios, salas e instalações. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para proteger escritórios, salas e instalações: b) quando for aplicável, convém que os edifícios sejam discretos com a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações.

- Questão 16

Pergunta: É projetada e aplicada proteção física contra desastres naturais (alagamentos), ataques maliciosos ou acidentes?

Peso = 3

Orientação: Norma ISO 27.002 - 11.1.4 - Proteção contra ameaças externas e do meio ambiente. Diretrizes para implementação: Convém que orientações de especialistas sejam obtidas sobre como evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.

- Questão 17

Pergunta: Existe uma política ou procedimento para o trabalho em áreas seguras, considerando que não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio, salvo se autorizado, que seja evitado o trabalho nesses ambientes sem a devida supervisão e que sejam fisicamente trancadas quando não ocupadas?

Peso = 3

Orientação: Norma ISO 27.002 - 11.1.5 - Trabalhando em áreas seguras. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes: d) não sejam permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudios ou de outros equipamentos de gravação, como câmeras em

dispositivos móveis, salvo se for autorizado. Item de controle ISO 27.001 - A.11.1.5 - Trabalhando em áreas seguras. Devem ser projetados e aplicados procedimentos para o trabalho em áreas seguras.

- Questão 18

Pergunta: O acesso a uma área de entrega e carregamento a partir do exterior do prédio fica restrito ao pessoal identificado e autorizado?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.11.1.6 - Áreas de entrega e carregamento. Pontos de acesso, como áreas de entrega e de carregamento, e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

- Questão 19

Pergunta: As áreas de entrega e carregamento são projetadas de tal maneira que seja possível carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício?

Peso = 1

Orientação: Item de controle ISO 27.001 - A.11.1.6 - Áreas de entrega e carregamento. Pontos de acesso, como áreas de entrega e de carregamento, e outros pontos em que pessoas não autorizadas possam entrar nas instalações, devem ser controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

- Questão 20

Pergunta: Os materiais entregues são inspecionados para evidenciar alguma alteração indevida?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.6 - Áreas de entrega e carregamento. Diretrizes para implementação: Convém que sejam levados em consideração as seguintes diretrizes: g) convém que os materiais entregues sejam inspecionados para evidenciar alteração indevida. Caso alguma alteração indevida seja descoberta, ela deve ser imediatamente notificada ao pessoal da segurança.

- Questão 21

Pergunta: Os materiais entregues são inspecionados e examinados para detectar a presença de explosivos, materiais químicos ou outros materiais perigosos antes do carregamento para o local de utilização?

Peso = 1

Orientação: Norma ISO 27.002 - 11.1.6 - Áreas de entrega e carregamento. Diretrizes para implementação: Convém que sejam levados em consideração as seguintes diretrizes: d) convém que os materiais entregues sejam inspecionados e examinados para detectar a presença de explosivos, materiais químicos ou outros materiais perigosos, antes de serem transportados da área de entrega e carregamento para o local de utilização;

Grupo 2 - Equipamentos

Propósito de Grupo 2: Impedir perdas, danos, furto ou roubo, ou comprometimento de ativos e interrupção das operações da organização.

Questões do Grupo 2:

- Questão 1

Pergunta: Os equipamentos de processamento de informação classificados como sensíveis são protegidos e colocados em locais com o intuito de reduzir os riscos de ameaças e perigos ambientais?

Peso = 3

Orientação: Norma ISO 27.002 - 11.2.1 - Localização e proteção do equipamento. Diretrizes para implementação: e) convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água(ou falha no suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo.

- Questão 2

Pergunta: As instalações de processamento da informação que manuseiam dados sensíveis são posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.1 - Localização e proteção do equipamento. Diretrizes para implementação: b) convém que as instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização;

- Questão 3

Pergunta: São estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.1 - Localização e proteção do equipamento. Diretrizes para implementação: f) convém que sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação.

- Questão 4

Pergunta: As condições ambientais, como temperatura e umidade são monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.1 - Localização e proteção do equipamento. Diretrizes para implementação: g) convém que as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação.

- Questão 5

Pergunta: Os edifícios são dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações possuem filtros de proteção contra raios?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.1 - Localização e proteção do equipamento. Diretrizes para implementação: h) convém que todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;

- Questão 6

Pergunta: Existe uma avaliação regular quanto a capacidade das utilidades (suprimento de energia elétrica, telecomunicações, ventilação e ar condicionado) de atender ao crescimento do negócio?

Peso = 3

Orientação: Norma ISO 27.002 - 11.2.2 - Utilidades. Diretrizes para implementação: Convém que todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, ventilação e ar-condicionado): b) sejam avaliadas regularmente quanto à sua capacidade de atender ao crescimento do negócio e às interações com outras utilidades;

- Questão 7

Pergunta: As utilidades (suprimento de energia elétrica, telecomunicações, ventilação e ar condicionado) são inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.2 - Utilidades. Diretrizes para implementação: Convém que todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, ventilação e ar-condicionado): c) sejam inspecionadas e testadas regularmente para assegurar o seu adequado funcionamento.

- Questão 8

Pergunta: Existe um monitoramento e alarmes para detectar o mau funcionamento do suprimento de energia elétrica, ou de telecomunicações, ventilação e ar condicionado?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.2 - Utilidades. Diretrizes para implementação: Convém que todas as utilidades (como suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, ventilação e ar-condicionado): d) sejam alarmadas para detectar o mau funcionamento, quando necessário.

- Questão 9

Pergunta: As linhas de energia e de telecomunicações são subterrâneas (ou abaixo do piso) sempre que possível, ou recebem uma proteção alternativa adequada?

Peso = 3

Orientação: Norma ISO 27.002 - 11.2.3 - Segurança do cabeamento. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento: a) convém que as linhas de energia e de telecomunicações sejam subterrâneas (ou fiquem abaixo do piso) sempre que possível, ou recebam uma proteção alternativa adequada;

- Questão 10

Pergunta: Os cabos de energia são segregados dos cabos de comunicações para evitar interferências?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.3 - Segurança do cabeamento. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento: b) convém que os cabos de energia sejam segregados dos cabos de comunicações, para evitar interferências;

- Questão 11

Pergunta: Existe acesso controlado aos painéis de conexões (rack) e às salas de cabos?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.3 - Segurança do cabeamento. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento: c) para sistemas sensíveis ou críticos, convém que os seguintes controles adicionais sejam considerados: 4) acesso controlado aos painéis de conexões e às salas de cabos.

- Questão 12

Pergunta: É utilizado blindagem eletromagnética para a proteção dos cabos?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.3 - Segurança do cabeamento. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a segurança do cabeamento: c) para sistemas sensíveis ou críticos, convém que os seguintes controles adicionais sejam considerados: 2) utilização de blindagem eletromagnética para a proteção dos cabos;

- Questão 13

Pergunta: É assegurado que os equipamentos tenham manutenção correta que assegure a sua contínua integridade e disponibilidade?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.11.2.4 - Manutenção de equipamentos. Os equipamentos devem ter uma manutenção correta para assegurar a sua contínua integridade e disponibilidade.

- Questão 14

Pergunta: Existe uma manutenção em intervalos recomendados pelo fornecedor e de acordo com as suas especificações?

Peso = 3

Orientação: Norma ISO 27.002 - 11.2.4 - Manutenção de equipamentos. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a manutenção dos equipamentos: a) convém que a manutenção dos equipamentos seja realizada nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

- Questão 15

Pergunta: Existem registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas?

Peso = 1

Orientação: Norma ISO 27.002 - 11.2.4 - Manutenção de equipamentos. Diretrizes para implementação: Convém que sejam levadas em consideração as seguintes diretrizes para a manutenção dos equipamentos: c) convém que sejam mantidos registros de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas;

- Questão 16

Pergunta: Existe política para equipamentos, informações ou software que são retirados do local (seja por funcionários ou terceiros), observando-se o armazenamento de informações?

Peso = 3

Orientação: Item de controle ISO 27.001 - 11.2.5 - Remoção dos ativos. Equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.

- Questão 17

Pergunta: São tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A11.2.6 - Segurança de equipamentos a ativos fora das dependências da organização. Devem ser tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

- Questão 18

Pergunta: Todos os equipamentos que contenham mídias de armazenamento de dados são examinados antes da reutilização, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.11.2.7 - Reutilização ou descarte seguro de equipamentos. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes da reutilização, para

assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

- Questão 19

Pergunta: A organização possui uma campanha de conscientização para informar usuários da necessidade de proteger equipamentos, assim como suas responsabilidades por implementar estas proteções?

Peso = 3

Orientação: Norma ISO 27.002 - 11.2.8 - Equipamento de usuário sem monitoração. Diretrizes para implementação: Convém que todos os usuários estejam cientes dos requisitos de segurança da informação e procedimentos para proteger equipamentos desacompanhados, assim como suas responsabilidades por implementar estas proteções.

- Questão 20

Pergunta: É adotada uma política de mesa limpa para papéis e mídias de armazenamento removíveis?

Peso = 3

Orientação: Item de controle ISO 27.001 - 11.2.9 - Política de mesa limpa e tela limpa. Devem ser adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

- Questão 21

Pergunta: É adotada uma política de tela limpa para os recursos de processamento da informação?

Peso = 1

Orientação: Item de controle ISO 27.001 - 11.2.9 - Política de mesa limpa e tela limpa. Devem ser adotadas uma política de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

Classificação 9 - Segurança nas operações

Grupo 1 - Responsabilidades e procedimentos operacionais

Propósito de Grupo 1: Garantir a operação segura e correta dos recursos de processamento da informação.

Questões do Grupo 1:

- Questão 1

Pergunta: São documentados e disponibilizados os procedimentos de operação para todos os usuários que necessitam deles?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.12.1.1 - Documentação dos procedimentos da operação. Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitam deles.

Norma ISO 27.002 - 12.1.1 - Documentação dos procedimentos da operação. Diretrizes para implementação: Convém que os procedimentos de operação especifiquem as instruções, incluindo: Instalação e configuração de sistemas; Cópias de segurança; Instruções para tratamento de erros ou outras condições excepcionais; Instruções quanto ao manuseio de mídias e saídas impressões) de dados especiais.

- Questão 2

Pergunta: Mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação estão controladas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.12.1.2 - Gestão de mudanças. Mudanças na organização, nos processos de negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação devem ser controladas.

- Questão 3

Pergunta: A utilização dos recursos são monitoradas e ajustadas, e as projeções são realizadas para necessidades de capacidade futura a fim de garantir o desempenho requerido do sistema?

Peso = 3

Orientação: Norma ISO 27.002 - 12.1.3 - Gestão da capacidade. Diretrizes para implementação: O fornecimento da capacidade suficiente pode ser obtido por meio do aumento de capacidade ou redução da demanda. Exemplos de gerenciamento da demanda de capacidade incluem: a) exclusão de dados obsoletos (espaço em disco); b) desativação de aplicações, sistemas, bases de dados ou ambientes; c) otimização das programações e dos processos de lote; d) otimização da lógica de aplicação ou das consultas à base de dados; e) negar ou restringir o uso da banda larga para serviços que demandam muitos recursos, se estes não forem críticos ao negócio (por exemplo, streaming de vídeo).

- Questão 4

Pergunta: Os ambientes de desenvolvimento, teste e produção estão separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção?

Peso = 3

Orientação: Norma ISO 27.002 - 12.4.4 - Separação do ambientes de desenvolvimento, teste e produção. Informações adicionais: As atividades de desenvolvimento e teste podem causar sérios problemas, como, por exemplo, modificações inesperadas em arquivos ou no ambiente dos sistemas, ou falhas de sistemas. Nesse caso, é necessária a manutenção de um ambiente conhecido e estável, no qual possam ser executados testes significativos e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento ao ambiente operacional.

Grupo 2 - Proteção contra malware

Propósito de Grupo 2: Assegurar que as informações e os recursos de processamento da informação estão protegidos contra malware.

Questões do Grupo 2:

- Questão 1

Pergunta: A organização possui uma política formal proibindo o uso de software não autorizado?

Peso = 1

Orientação: Norma ISO 27.002 - 12.2.1 - Controles contra malware. Diretrizes para implementação: Convém que a proteção contra malware seja baseada em software de detecção de resposta a malware, na conscientização da segurança da informação, no controle de acessos adequado e nos controles de gerenciamento de mudanças. Recomenda-se que os seguintes controles sejam considerados: a) estabelecer uma política formal proibindo o uso de software não autorizados;

- Questão 2

Pergunta: A organização possui um controle para prevenir ou detectar o uso de software não autorizado, como whitelisting ou lista de softwares permitidos?

Peso = 1

Orientação: Norma ISO 27.002 - 12.2.1 - Controles contra malware. Diretrizes para implementação: Convém que a proteção contra malware seja baseada em software de detecção de resposta a malware, na conscientização da segurança da informação, no controle de acessos adequado e nos controles de gerenciamento de

mudanças. Recomenda-se que os seguintes controles sejam considerados: b) implementar controles para prevenir ou detectar o uso de software não autorizado (por exemplo whitelisting, ou seja, uma lista de softwares permitidos a acessar o sistema);

- Questão 3

Pergunta: São implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário?

Peso = 1

Orientação: Norma ISO 27.002 - 12.2.1 - Controles contra malware. Diretrizes para implementação: Convém que a proteção contra malware seja baseada em software de detecção de resposta a malware, na conscientização da segurança da informação, no controle de acessos adequado e nos controles de gerenciamento de mudanças.

- Questão 4

Pergunta: A organização possui instalado e atualizado regularmente software para detecção e remoção de malware?

Peso = 1

Orientação: Norma ISO 27.002 - 12.2.1 - Controles contra malware. Diretrizes para implementação: Convém que a proteção contra malware seja baseada em software de detecção de resposta a malware, na conscientização da segurança da informação, no controle de acessos adequado e nos controles de gerenciamento de mudanças . Recomenda-se que os seguintes controles sejam considerados: g) instalar e atualizar regularmente software de detecção e remoção de malware de computadores e mídias magnéticas, de forma preventiva ou rotineira.

Grupo 3 - Cópias de segurança

Propósito de Grupo 3: Proteger contra a perda de dados.

Questões do Grupo 3:

- Questão 1

Pergunta: A organização possui política para cópias de segurança das informações, softwares e das imagens do sistema?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.12.3.1 - Cópias de segurança das informações. Cópias de segurança das informações, softwares e das imagens do

sistema devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

- Questão 2

Pergunta: As cópias de segurança são testadas regularmente, inclusive checando o tempo de restauração requerido?

Peso = 1

Orientação: Norma ISO 27.002 - 12.3.1 - Cópias de segurança das informações. Diretrizes para implementação: Quando da da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração: e) convém que as mídias de backup sejam regularmente testadas para garantir que elas sejam confiáveis no caso de uso emergencial; convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido.

- Questão 3

Pergunta: A organização mantém registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração?

Peso = 1

Orientação: Norma ISO 27.002 - 12.3.1 - Cópias de segurança das informações. Diretrizes para implementação: Quando da da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração: a) registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;

- Questão 4

Pergunta: As cópias de segurança são armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal?

Peso = 1

Orientação: Norma ISO 27.002 - 12.3.1 - Cópias de segurança das informações. Diretrizes para implementação: Quando da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração: c) convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

- Questão 5

Pergunta: As cópias de segurança possuem um nível apropriado de proteção física e ambiental (exposição às intempéries do tempo)?

Peso = 1

Orientação: Norma ISO 27.002 - 12.3.1 - Cópias de segurança das informações. Diretrizes para implementação: Quando da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração: d) convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança, consistentes com as normas aplicadas na instalação principal;

- Questão 6

Pergunta: As cópias de backup são protegidas através de encriptação?

Peso = 1

Orientação: Norma ISO 27.002 - 12.3.1 - Cópias de segurança das informações. Diretrizes para implementação: Quando da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração: f) em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Grupo 4 - Registros e monitoramento

Propósito de Grupo 4: Registrar eventos e gerar evidências.

Questões do Grupo 4:

- Questão 1

Pergunta: Registros de eventos (log) das atividades do usuário, exceções, falhas e eventos de segurança da informação são produzidos, mantidos e analisados criticamente, a intervalos regulares?

Peso = 3

Orientação: Item de controle A.12.4.1 - ISO 27.001 - Registro de eventos. Registros de eventos (log) das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente a intervalos regulares.

- Questão 2

Pergunta: As informações dos registros de eventos (log) e seus recursos estão protegidos contra acesso não autorizado e adulteração?

Peso = 3

Orientação: Item de controle A.12.4.2 - ISO 27.001 - Proteção das informações dos registros de eventos (logs) . As informações dos registros de eventos (log) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.

- Questão 3

Pergunta: As atividades dos administradores e operadores do sistema estão registradas e os registros (logs) estão protegidos e analisados criticamente, a intervalos regulares?

Peso = 3

Orientação: Item de controle A.12.4.3 - ISO 27.001 - Registro de eventos (logs) de administrador e operador. As atividades dos administradores e operadores do sistema devem ser registradas e os registros (logs) devem ser protegidos e analisados criticamente, a intervalos regulares.

- Questão 4

Pergunta: Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, estão sincronizados com uma fonte de tempo precisa?

Peso = 3

Orientação: Item de controle A.12.4.4 - ISO 27.001 - Sincronização dos relógios. Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, devem ser sincronizados com uma fonte de tempo precisa.

Grupo 5 - Controle de software operacional

Propósito de Grupo 5: Assegurar a integridade dos sistemas operacionais.

Questões do Grupo 5:

- Questão 1

Pergunta: Instalações e atualizações do software operacional, aplicativos e bibliotecas de programas são executadas apenas por administradores e com autorização apropriada?

Peso = 3

Orientação: Norma ISO 27.002 - 12.5.1 - Instalação de software nos sistemas operacionais. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de software em sistemas operacionais: a) convém que as atualizações do software operacional, aplicativos e

bibliotecas de programas sejam executadas por administradores treinados e com autorização gerencial apropriada;

- Questão 2

Pergunta: Sistemas operacionais e aplicativos são implementados somente após testes extensivos e bem sucedidos?

Peso = 1

Orientação: Norma ISO 27.002 - 12.5.1 - Instalação de software nos sistemas operacionais. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de software em sistemas operacionais: c) convém que sistemas operacionais e aplicativos somente sejam implementados após testes extensivos e bem-sucedidos;

- Questão 3

Pergunta: A organização possui um controle da implementação do software, assim como da documentação do sistema?

Peso = 1

Orientação: Norma ISO 27.002 - 12.5.1 - Instalação de software nos sistemas operacionais. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de software em sistemas operacionais: d) convém que um sistema de controle de configuração seja utilizado para manter o controle da implementação do software, assim como da documentação do sistema;

- Questão 4

Pergunta: As versões anteriores dos softwares aplicativos são mantidas como medida de contingência?

Peso = 1

Orientação: Norma ISO 27.002 - 12.5.1 - Instalação de software nos sistemas operacionais. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para controlar as mudanças de software em sistemas operacionais: g) convém que versões anteriores dos softwares aplicativos sejam mantidas como medida de contingência;

Grupo 6 - Gestão de vulnerabilidades técnicas

Propósito de Grupo 6: Prevenir a exploração de vulnerabilidades técnicas.

Questões do Grupo 6:

- Questão 1

Pergunta: A SIGNOVE possui definido as funções e responsabilidades associadas à gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida?

Peso = 3

Orientação: Norma ISO 27.002 - 12.6.1 - Gestão de vulnerabilidades técnicas. Diretrizes para implementação: É recomendável que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas: a) convém que a organização estabeleça as funções e responsabilidades associadas à gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida;

- Questão 2

Pergunta: A SIGNOVE possui recursos de informação a serem usados para identificar vulnerabilidades técnicas relevantes, que sejam mantidos atualizados com base nas mudanças no inventários de ativos, ou quando outros recursos novos ou úteis forem encontrados?

Peso = 1

Orientação: Norma ISO 27.002 - 12.6.1 - Gestão de vulnerabilidades técnicas. Diretrizes para implementação: É recomendável que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas: b) convém que os recursos a serem usados para identificar vulnerabilidades técnicas relevantes para manter a conscientização sobre eles sejam identificados, para software e outras tecnologias; convém que esses recursos de informação sejam mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis forem encontrados;

- Questão 3

Pergunta: A SIGNOVE possui um prazo definido para execução da análise de vulnerabilidades, e definição de tratamentos em casos de urgências?

Peso = 1

Orientação: Norma ISO 27.002 - 12.6.1 - Gestão de vulnerabilidades técnicas. Diretrizes para implementação: É recomendável que as seguintes diretrizes sejam seguidas para o estabelecimento de um processo de gestão efetivo de vulnerabilidades técnicas: c) convém que seja definido um prazo para reação a notificações de potenciais vulnerabilidades técnicas relevantes;

- Questão 4

Pergunta: São definidos e implementados critérios para a instalação de software pelos usuários?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.12.6.2 - Restrições quanto à instalação de software. Regras definindo critérios para a instalação de software pelos usuários devem ser estabelecidas e implementadas.

Grupo 6 - Considerações quanto à auditoria de sistemas de informação

Propósito de Grupo 6: Minimizar o impacto das atividades de auditoria nos sistemas operacionais.

Questões do Grupo 7:

- Questão 1

Pergunta: As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais são planejados e acordados para minimizar a interrupção nos processos do negócio?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.12.7.1 - Controles de auditoria de sistemas de informação. As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar a interrupção nos processos do negócio.

Classificação 10 - Aquisição, desenvolvimento e manutenção de sistemas

Grupo 1 - Requisitos de segurança de sistemas de informação

Propósito de Grupo 1: Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas.

Questões do Grupo 1:

- Questão 1

Pergunta: Os requisitos relacionados com segurança da informação são incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.1.1 - Análise e especificação dos requisitos de segurança da informação. Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informações existentes.

- Questão 2

Pergunta: As informações envolvidas nos serviços de aplicação que transitam em redes públicas são protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.1.2 - Serviços de aplicação seguros sobre redes públicas. As informações envolvidas nos serviços de aplicação que transitam em redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais e divulgações e modificações não autorizadas. Por exemplo: autenticação por dois fatores em serviços de rede mais sensíveis.

- Questão 3

Pergunta: A organização possui uma avaliação de riscos detalhada e uma seleção de controles apropriados para serviços de aplicação em redes públicas?

Peso = 1

Orientação: Norma ISO 27.002 - 14.1.2 - Serviços de aplicação seguros em redes públicas. Informações adicionais: Aplicações acessadas através de redes públicas são suscetíveis a uma variedade de ameaças de rede, como atividades fraudulentas, disputas contratuais ou divulgação de informação para o público. Por esses motivos, uma avaliação de riscos detalhada e uma seleção de controles apropriada são indispensáveis.

- Questão 4

Pergunta: A organização possui procedimentos para proteger as informações envolvidas em transações nos aplicativos de serviços, e que são protegidas (estejam íntegras) para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.1.3 - Protegendo as transações nos aplicativos de serviços. Informações envolvidas em transações em aplicativos de serviços devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.

Grupo 2 - Segurança em processos de desenvolvimento e de suporte.

Propósito de Grupo 2: Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação

Questões do Grupo 2:

- Questão 1

Pergunta: A organização possui uma política de desenvolvimento seguro, considerando segurança no ambiente de desenvolvimento, segurança na metodologia de desenvolvimento do software, repositórios seguros, detectar e corrigir vulnerabilidades e segurança no controle de versões?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.1 - Política de desenvolvimento seguro. Regras para o desenvolvimento de sistemas e software devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

- Questão 2

Pergunta: A organização possui uma diretriz para controle de mudanças em sistemas, considerando que as mudanças sejam submetidas por usuários autorizados, análise crítica dos procedimentos de controle e integridade, aprovações e documentação antes e após mudanças, controle de versão e trilha de auditoria?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.2 - Procedimentos para controles de mudanças de sistemas. Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças.

- Questão 3

Pergunta: Aplicações críticas de negócios são analisadas criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.3 - Análise crítica técnica das aplicações após mudanças nas plataformas operacionais. Aplicações críticas de negócio devem ser analisadas criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança.

- Questão 4

Pergunta: Modificações em pacotes de software são desencorajadas e estão limitadas às mudanças necessárias, e essas mudanças são estritamente controladas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.4 - Restrições sobre mudanças em pacotes de software. Modificações em pacotes de software devem ser desencorajadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.

- Questão 5

Pergunta: A organização estabelece princípios para projetar sistemas seguros, documentados, e estes mantidos e aplicados para qualquer implementação de sistemas de informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.5 - Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

- Questão 6

Pergunta: A organização estabelece e protege adequadamente os ambientes seguros de desenvolvimento, como esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.6 - Ambiente seguro para desenvolvimento. As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistemas.

- Questão 7

Pergunta: A SIGNOVE supervisiona e monitora se as atividades de desenvolvimento de sistemas terceirizados contemplam a segurança da informação em todas as suas fases?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.7 - Desenvolvimento terceirizado. A organização deve supervisionar e monitorar as atividades de desenvolvimento de sistemas, terceirizado.

- Questão 8

Pergunta: As terceirizadas documentam e comunicar ao contratante sobre a segurança da informação utilizada em suas fases de desenvolvimento e implementação?

Peso = 1

Orientação: Norma ISO 27.002 - 14.2.7 - Desenvolvimento terceirizado. Diretrizes para implementação: Quando o desenvolvimento de sistemas for terceirizado, convém que os seguintes pontos sejam considerados ao longo de toda a cadeia de suprimento externo da organização: e) fornecimentos de evidência de que os princípios de segurança foram usados para estabelecer um nível mínimo de segurança aceitável e a qualidade da privacidade; j) documentação efetiva da construção do ambiente usado para realizar as entregas;

- Questão 9

Pergunta: Testes de funcionalidade de segurança são realizados durante o desenvolvimento de sistemas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.2.8 - Teste de segurança do sistema. Testes de funcionalidade de segurança devem ser realizados durante o desenvolvimento de sistemas.

- Questão 10

Pergunta: A organização utiliza procedimentos para testes de aceitação para novos sistemas de informação, atualizações e novas versões?

Peso = 3

Orientação: Norma ISO 27.002 - 14.2.9 - Teste de aceitação de sistemas. Controle: Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.

Grupo 3 - Dados para teste

Propósito de Grupo 3: Assegurar a proteção dos dados usados para teste.

Questões do Grupo 3:

- Questão 1

Pergunta: A organização utiliza procedimentos para o uso de dados em testes de novos sistemas ou novas funcionalidades são selecionados com cuidado, protegidos e controlados?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.14.3.1 - Proteção dos dados para teste. Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

Classificação 11 - Relacionamento na cadeia de suprimento

Grupo 1 - Segurança da informação na cadeia de suprimento

Propósito de Grupo 1: Garantir a proteção dos ativos da organização que são acessados pelos fornecedores.

Questões do Grupo 1:

- Questão 1

Pergunta: Todos os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização são acordados com o fornecedor e documentados?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.15.1.1 - Política de segurança da informação no relacionamento com os fornecedores. Requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização devem ser acordados com o fornecedor e documentados.

- Questão 2

Pergunta: Todos os requisitos de segurança da informação relevantes são estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.15.1.2 - Identificando segurança da informação nos acordos com fornecedores. Todos os requisitos de segurança da informação relevantes devem ser estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da organização.

- Questão 3

Pergunta: Acordos com fornecedores incluem requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.15.1.3. Cadeia de suprimento na tecnologia da informação e comunicação. Acordos com fornecedores devem incluir requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia da informação e comunicação.

Grupo 2 - Gerenciamento da entrega do serviço do fornecedor

Propósito de Grupo 2: Manter um nível acordado de segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Questões do Grupo 2:

- Questão 1

Pergunta: A organização monitora e analisa criticamente a entrega dos serviços executados pelos fornecedores, avaliando o seu desempenho, serviços produzidos, trilhas de auditoria, registros de eventos de segurança e as condições dos acordos de segurança da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.15.2.1 - Monitoramento e análise crítica de serviços com fornecedores. A organização deve monitorar, analisar criticamente e auditar, a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

- Questão 2

Pergunta: Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, são gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos e a reavaliação de riscos?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.15.2.2 - Gerenciamento de mudanças para serviços com fornecedores. Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhorias das políticas de segurança da informação, dos procedimentos e controles existentes, devem ser gerenciadas levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos e a reavaliação de riscos.

Classificação 12 - Gestão de incidentes de segurança da informação

Grupo 1 - Gestão de incidentes de segurança da informação e melhorias

Propósito de Grupo 1: Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Questões do Grupo 1:

- Questão 1

Pergunta: Os procedimentos estabelecidos asseguram um ponto de contato para notificação e detecção de incidentes de segurança, contatos com autoridades e pessoal competente para tratar as questões relativas aos incidentes?

Peso = 3

Orientação: Norma ISO 27.002 - 16.1.1 - Responsabilidades e procedimentos. Diretrizes para implementação: a) convém que responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização: 2) procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação; b) convém que os procedimentos estabelecidos assegurem que: 1) pessoal competente trate as questões relativas a incidentes de segurança dentro da organização; 2) um ponto de contato para notificação e detecção de incidentes de segurança esteja implementado; 3) contatos apropriados sejam mantidos com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação;

- Questão 2

Pergunta: A organização possui diretrizes sobre responsabilidades e procedimentos em relação à gestão de incidentes de segurança da informação?

Peso = 1

Orientação: Item de controle ISO 27.001 - A.16.1.1 - Responsabilidades e procedimentos. Responsabilidades e procedimentos de gestão devem ser estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

- Questão 3

Pergunta: As diretrizes para gestão de incidentes incluem procedimentos para preparação e planejamento da resposta a incidentes?

Peso = 1

Orientação: Norma ISO 27.002 - 16.1.1 - Responsabilidades e procedimentos. Diretrizes para implementação: a) convém que responsabilidades pelo

gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização: 1) procedimentos para preparação e planejamento a resposta a incidente;

- Questão 4

Pergunta: As diretrizes incluem procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação?

Peso = 1

Orientação: Norma ISO 27.002 - 16.1.1 - Responsabilidades e procedimentos. Diretrizes para implementação: a) convém que responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização: 2) procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação;

- Questão 5

Pergunta: Existe uma campanha para alertar funcionários e partes externas sobre sua responsabilidade em notificar qualquer evento de segurança da informação o mais breve possível?

Peso = 3

Orientação: Norma ISO 27.002 - 16.1.2 - Notificação de eventos de segurança da informação. Diretrizes para implementação: Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível.

- Questão 6

Pergunta: Essa campanha define os procedimentos de como notificar os eventos, ponto de contato e quais os eventos devem ser notificados?

Peso = 1

Orientação: Norma ISO 27.002 - 16.1.2 - Notificação de eventos de segurança da informação. Diretrizes para implementação: Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato, ao qual os eventos devem ser modificados.

- Questão 7

Pergunta: A organização possui diretriz orientando funcionários e partes externas que usam os sistemas de informação e serviços da organização a notificar e

registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.16.1.3 - Notificando fragilidades de segurança da informação. Os funcionários e partes externas que usam os sistemas de informação e serviços da organização devem ser instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

- Questão 8

Pergunta: A organização possui um ponto de contato para notificação e registro de quaisquer fragilidades de segurança da informação observada ou suspeita?

Peso = 1

Orientação: Norma ISO 27.002 - 16.1.3 - Notificando fragilidades de segurança da informação. Diretrizes para implementação: Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido possível, de forma a prevenir incidentes de segurança da informação. O mecanismo de notificação deve ser fácil, acessível e disponível, sempre que possível.

- Questão 9

Pergunta: A organização possui uma escala de classificação de incidentes e eventos de segurança da informação, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.16.4.1 - Avaliação e decisão de eventos de segurança da informação. Os eventos de segurança da informação devem ser avaliados, e deve ser decidido se eles são classificados como incidentes de segurança da informação.

- Questão 10

Pergunta: Incidentes de segurança da informação são reportados de acordo com procedimentos documentados?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.16.1.5 - Resposta aos incidentes de segurança da informação. Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados.

- Questão 11

Pergunta: Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação são documentados e são usados para reduzir a probabilidade ou o impacto de incidentes futuros?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.16.1.6 - Aprendendo com os incidentes de segurança da informação. Os conhecimentos obtidos da análise e resolução de incidentes de segurança da informação devem ser usados para reduzir a probabilidade ou o impacto de incidentes futuros.

- Questão 12

Pergunta: A organização define e aplica procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.16.1.7 - Coleta de evidências. A organização deve definir e aplicar procedimentos para identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Classificação 13 - Aspectos da segurança da informação na gestão da continuidade do negócio

Grupo 1 - Continuidade da segurança da informação.

Propósito de Grupo 1: A continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negócio da organização.

Questões do Grupo 1:

- Questão 1

Pergunta: A organização determina seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.17.1.1 - Planejando a continuidade da segurança da informação. A organização deve determinar seus requisitos para a segurança da informação e a continuidade da gestão da informação em situações adversas, por exemplo, durante uma crise ou desastre.

- Questão 2

Pergunta: A organização estabelece, documenta, implementa e mantém processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.17.1.2 - Implementando a continuidade da segurança da informação. A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa.

- Questão 3

Pergunta: A organização verifica os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.17.1.3 - Verificação, análise crítica e avaliação da continuidade da segurança da informação. A organização deve verificar os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

Grupo 2 - Redundâncias

Propósito de Grupo 2: Assegurar a disponibilidade dos recursos de processamento da informação.

Questões do Grupo 2:

- Questão 1

Pergunta: São implementados recursos de processamento da informação com redundância suficiente para atender aos requisitos de disponibilidade?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.17.2.1 - Disponibilidade dos recursos de processamento da informação. Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade. Por exemplo: Para garantir a continuidade dos processos, existe redundância para: servidores e links.

- Questão 2

Pergunta: Os componentes de redundância são testados para assegurar o funcionamento conforme esperado?

Peso = 1

Orientação: Norma ISO 27.002 - 17.2.1 - Disponibilidade dos recursos de processamento da informação. Diretrizes para implementação: onde aplicável, convém que sistemas de informação redundantes sejam testados para assegurar que a transferência de um componente para outro componente, funcione conforme o esperado.

Classificação 14 - Conformidade

Grupo 1 - Conformidade com requisitos legais e contratuais

Propósito de Grupo 1: Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

Questões do Grupo 1:

- Questão 1

Pergunta: Os requisitos legislativos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, são explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.1.1 - Identificação da legislação aplicável e de requisitos contratuais. Todos os requisitos legislativos estatutários, regulamentares e contratuais relevantes, e enfoque da organização para atender a esses requisitos, devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

- Questão 2

Pergunta: A organização possui uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: a) divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação;

- Questão 3

Pergunta: A organização adquire software somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não esteja sendo violado?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: b) adquirir software somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não esteja sendo violado;

- Questão 4

Pergunta: A organização mantém um programa de conscientização das políticas para proteger os direitos de propriedade intelectual e a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: c) manter a conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;

- Questão 5

Pergunta: A organização mantém, de forma adequada, os registros de ativos e identificação desses para proteger os direitos de propriedade intelectual?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: d) manter, de forma adequada, os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;

- Questão 6

Pergunta: A organização mantém provas e evidências da propriedade de licenças, discos-mestres, manuais, etc?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam

consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: e) manter provas e evidências da propriedade de licenças, discos-mestres, manuais etc.;

- Questão 7

Pergunta: A organização possui controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não esteja excedido?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: f) implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não esteja excedido;

- Questão 8

Pergunta: A organização conduz verificações para que somente produtos de software autorizados e licenciados sejam instalados?

Peso = 1

Orientação: Norma ISO 27.002 - 18.1.2 - Direitos de propriedade intelectual. Diretrizes para implementação: Convém que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado propriedade intelectual: g) conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados;

- Questão 9

Pergunta: Existem diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações (seja qual for o tipo de mídia de armazenamento, como, por exemplo, papel, microficha, meio magnético ou óptico)?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.1.3 - Proteção de registros. Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado, e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio;

Norma ISO 27.002 - 18.1.3 - Proteção de registros. Diretrizes para implementação: Para atender aos objetivos de proteção dos registros, convém que os seguintes passos sejam tomados pela organização: a) emitir diretrizes gerais para retenção, armazenamento, tratamento e disposição de registros e informações;

- Questão 10

Pergunta: Existe uma política de dados da organização para proteção e privacidade da informação, desenvolvida e implementada requerida por legislação e regulamentação pertinente?

Peso = 3

Orientação: Norma ISO 27.002 - 18.1.4 - Proteção e privacidade de informações de identificação pessoal. Diretrizes para implementação: Convém que uma política de dados da organização para proteção e privacidade da informação de identificação pessoal seja desenvolvida e implementada. Esta política deve ser comunicada a todas as pessoas envolvidas no processamento de informação de identificação pessoal.

- Questão 11

Pergunta: São usados controles de criptografia em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.1.5 - Regulamentação de controles de criptografia. Controles de criptografia devem ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

Grupo 2 - Análise crítica da segurança da informação

Propósito de Grupo 1: Assegurar que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

Questões do Grupo 1:

- Questão 1

Pergunta: A organização analisa, criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas, seu enfoque para gerenciar a segurança da informação e a sua implementação?

Peso = 3

Orientação: Norma ISO 27.002 - 18.2.1 - Análise crítica independente da segurança da informação. Controle: Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, objetivos dos controles, controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

- Questão 2

Pergunta: Os gestores analisam criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.2.2 - Conformidade com as políticas e normas da segurança da informação. Os gestores analisam criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

- Questão 2

Pergunta: Os gestores analisam criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.2.2 - Conformidade com as políticas e normas da segurança da informação. Os gestores analisam criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

- Questão 3

Pergunta: Os sistemas de informação são analisados criticamente (através de testes de invasão e avaliações de vulnerabilidade), a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização?

Peso = 3

Orientação: Item de controle ISO 27.001 - A.18.2.3 - Análise crítica da conformidade técnica. Os sistemas de informação devem ser analisados criticamente, a intervalos regulares para verificar a conformidade com as normas e políticas de segurança da informação da organização.