ISO 27002 by Joas

Liderança

5.1 Liderança e comprometimento

- A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão
- da segurança da informação pelos seguintes meios:
- a) assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização;
- b) garantindo a integração dos requisitos do sistema de gestão da segurança da informação dentro dos processos da organização;
- c) assegurando que os recursos necessários para o sistema de gestão da segurança da informação estão disponíveis;
- d) comunicando a importância de uma gestão efi caz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação;
- e) assegurando que o sistema de gestão da segurança da informação alcança seus resultados pretendidos;
- f) orientando e apoiando pessoas que contribuam para eficácia do sistema de gestão da segurança da informação;
- g) promovendo a melhoria contínua; e
- h) apoiando outros papéis relevantes da gerência para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade.

Conformidade

Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança

- Todos os requisitos legislativos estatutários, regulamentares e contratuais relevantes, e o enfoque da organização para atender a esses requisitos, devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.
- Procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.
- 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.
- A privacidade e proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.
- Controles de criptografia devem ser usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

Garantir que a segurança da informação está implementada e operada de acordo com as políticas e procedimentos da organização.

- O enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivos dos controles, políticas, processos e procedimentos para a segurança da informação) deve ser analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.
- Os gestores devem analisar 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.
- 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.

Aspectos da segurança da informação na gestão da continuidade do negócio

A continuidade da segurança da informação deve ser contemplada nos sistemas de gestão da continuidade do negocio da organização.

- A organização deve determinar 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.
- 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.
- A organização deve verificar os controles de continuidade da segurança da informação, estabelecidos e implementados, à intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.
- Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.

Segurança nas operações

- Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que necessitam deles.
- Mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, devem ser controladas.
- A utilização dos recursos deve ser monitorada, ajustada e as projeções devem ser feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.
- Ambientes de desenvolvimento, teste e produção devem ser separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
- Devem ser implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinado com um adequado programa de conscientização do usuário.
- 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.
- Registros de eventos (log) de eventos das atividades de usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares.
- As informações dos registros de eventos (log) e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.
- As atividades dos administradores e operadores do sistema devem ser registradas e os registros (logs) devem ser protegidos e analisados criticamente, a intervalos regulares.
- 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.
- Procedimentos para controlar a instalação de software em sistemas operacionais devem ser implementados.
- Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, devem ser obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.
- Regras definindo critérios para a instalação de software pelos usuários devem ser estabelecidas e implementadas.
- As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupção nos processos do negocio.

Criptografia

Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

- Deve ser desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
- Uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, deve ser desenvolvida e implementada ao longo de todo o seu ciclo de vida.

Aquisição, desenvolvimento e manutenção de sistemas

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.

- Os requisitos relacionados com segurança da informação devem ser incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.
- As informações envolvidas nos serviços de aplicação que transitam sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
- Informações envolvidas em transações nos 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.

Garantir que a segurança da informação está projetada e implementada no ciclo de vida de desenvolvimento dos sistemas de informação.

- Regras para o desenvolvimento de sistemas e software devem ser estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.
- Mudanças em sistemas dentro do ciclo de vida de desenvolvimento devem ser controladas utilizando procedimentos formais de controle de mudanças.
- Aplicações críticas de negócios 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.
- Modificações em pacotes de software devem ser desencorajadas e devem estar limitadas às mudanças necessárias, e todas as mudanças devem ser estritamente controladas.
- Princípios para projetar sistemas seguros devem ser estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.
- As organizações devem estabelecer e proteger adequadamente os ambientes seguros de desenvolvimento, para os esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema
- A organização deve supervisionar e monitorar as atividades de desenvolvimento de sistemas terceirizado.
- Testes de funcionalidade de segurança devem ser realizados durante o desenvolvimento de sistemas.
- Programas de testes de aceitação e critérios relacionados devem ser estabelecidos para novos sistemas de informação, atualizações e novas versões.

Assegurar a proteção dos dados usados para teste.

- Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

Gestão de ativos

Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.

- Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados e um inventário deste ativo deve ser estruturado e mantido.
- Os ativos mantidos no inventário devem ter um proprietário.
- 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.
- Todos os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.
- A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
- Um conjunto apropriado de procedimentos para rotular a informação deve ser desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.
- Procedimentos para o tratamento dos ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização
- Procedimentos devem ser implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.
- As mídias devem ser descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais.
- Mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrompida, durante o transporte.

Políticas de segurança da informação

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

- Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes.

Análise crítica das políticas para segurança da informação

Organização da segurança da informação

Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação e operação da segurança da informação dentro da organização

- Todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas.
- Funções conflitantes e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.
- Contatos apropriados com autoridades relevantes devem ser mantidos.
- Contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação devem ser mantidos.
- Segurança da informação deve ser considerada no gerenciamento de projetos, independentemente do tipo do projeto.
- Uma política e medidas que apoiam a segurança da informação devem ser adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.
- Uma política e medidas que apoiam a segurança da informação devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

Segurança nas comunicações

Assegurar a proteção das informações em redes e dos recursos de processamento da informação que os apoiam

- As redes devem ser gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
- Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, devem ser identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
- Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes.

Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

- Políticas, procedimentos e controles de transferências formais, devem ser estabelecidos para proteger a transferência de informações por meio do uso de todos os tipos de recursos de comunicação.
- Devem ser estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.
- As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas.
- Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação devem ser identificados, analisados criticamente e documentados.

Segurança física e do Ambiente

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

- Perímetros de segurança devem ser definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.
- As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
- Deve ser projetada e aplicada segurança física para escritórios, salas e instalações.
- Devem ser projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.
- Deve ser projetada e aplicada procedimentos para o trabalho em áreas seguras.
- Pontos de acesso, tais 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, isoladas das instalações de processamento da informação, para evitar o acesso não autorizado.
- Os equipamentos devem ser colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.
- Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
- O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação, interferência ou danos.
- Os equipamentos devem ter uma manutenção correta para assegurar sua disponibilidade e integridade permanente.
- Equipamentos, informações ou software não devem ser retirados do local sem autorização prévia.
- 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.
- Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança.
- Os usuários devem assegurar que os equipamentos não monitorados tenham proteção adequada.
- Deve ser adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e uma política de tela limpa para os recursos de processamento da informação.

Controle de Acesso

Limitar o acesso à informação e aos recursos de processamento da informação.

- Uma política de controle de acesso deve ser estabelecida, documentada e analisada criticamente, baseado nos requisitos de segurança da informação e dos negócios.
- Os usuários devem somente receber acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
- Um processo formal de registro e cancelamento de usuário deve ser implementado para permitir atribuição de direitos de acesso.
- Um processo formal de provisionamento de acesso do usuário deve ser implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.
- A concessão e uso de direitos e acesso privilegiado devem ser restritos e controlados.

A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal.

- Os proprietários de ativos devem analisar criticamente os direitos de acesso dos usuários, a intervalos regulares.
- 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.

Os usuários devem ser orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

O acesso à informação e as funções dos sistemas de aplicações devem ser restrito de acordo com a política de controle de acesso.

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).

- Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade.
- O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.
- O acesso ao código-fonte de programa deve ser restrito.

Demissão e Finalização de Contrato

Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

As responsabilidades e obrigações pela segurança da informação que permanecem válidas após um encerramento ou mudança da contratação devem ser definidas, comunicadas aos funcionários ou partes externas e cumpridas.

Durante a Contratação

Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

- 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.
- Todos os funcionários da organização e, onde relevante, partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

Deve existir um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.

Antes da contratação

Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

- Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.

As obrigações contratuais com funcionários e partes externas devem declarar as suas responsabilidades e a da organização para a segurança da informação.

Competência

a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;

b) assegurar que essas pessoas são competentes, com base na educação, treinamento ou experi ência apropriados;

c) onde aplicável, tomar ações para adquirir a competência necessária e avaliar a efi cácia das ações tomadas; e

d) reter informação documentada apropriada como evidência da competência.

Apoio

Recursos: A organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do sistema de gestão da segurança da informação.

Gestão de incidentes de segurança da informação

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.

- Incidentes de segurança da informação devem ser reportados de acordo com procedimentos documentados.

Os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação devem ser usados para reduzir a probabilidade ou o impacto de incidentes futuros.

A organização deve definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

Relacionamento na cadeia de suprimento

Garantir a proteção dos ativos da organização que são acessíveis pelos 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.
- 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.
- 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 das comunicações e informação.

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

A organização deve monitorar, analisar criticamente e auditar a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

Mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria 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.

Evaluation Mode

Observação

For utilizado um Template encontrado na internet para inserir as informações aqui, não existe nada relacionado a nenhum cliente ou adquirido de forma ilícita por meio de uma invasão. Google Hacking salva vidas. ISO 27001 filetype:pdf and filetype:xls

LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos