Plano de aulas 7 - Tema 3

NORMAS DE SEGURANÇA DA INFORMAÇÃO

Identificação das aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

Link importante: https://www.diegomacedo.com.br/conheca-a-nbr-isoiec-27002/

Plano de aula 7

94

Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002

Hans Baars; Kees Hintzbergen; Jule Hint...

Páginas: 0
Editora: Editora Brasport
Edição: 1ª

Idioma: Português
ISBN: 9788574528670

Descrição

Prático e de fácil leitura explica de forma clara as abordagens, ou políticas, de gerenciamento de segurança da informação que muitas organizações podem analisar e implementar nos seus negócios. Ele aborda: Os requisitos de qualidade que uma organização pode ter para informações. Os riscos associados com os requisitos de qualidade no uso das informações. As medidas defensivas que são necessárias para mitigar os riscos associados. Como garantir a continuidade do negócio em caso de desastre. Se e quando reportar acidentes para fora da organização.

95

Identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002

As normas ISO/IEC 27001 e ISO/IEC 27002 são duas das normas mais importantes na área de segurança da informação. A ISO/IEC 27001 estabelece os requisitos para um sistema de gestão de segurança da informação, enquanto a ISO/IEC 27002 fornece diretrizes para a implementação e gestão de controles de segurança da informação.

Algumas das aplicações das normas ISO/IEC 27001 e ISO/IEC 27002 são:

1- Implementação de um sistema de gestão de segurança da informação em organizações públicas e privadas;

2- Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes;

3- Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações;

4- Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação;

5- Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis.

96

Aplicação 1

1- Implementação de um sistema de gestão de segurança da informação (SGSI) em organizações públicas e privadas

A ideia principal dessa aplicação é fornecer um conjunto de controles e boas práticas que permitam garantir a segurança das informações de uma organização, protegendo-as contra ameaças internas e externas, incluindo fraudes, espionagem, invasões e roubo de informações.

97

Aplicação 1

O SGSI deve ser adaptado às necessidades específicas de cada organização, levando em consideração seus objetivos de negócios, suas atividades, seus riscos, suas ameaças e vulnerabilidades. Alguns dos elementos que devem ser considerados na implementação do SGSI incluem:

- Identificação dos ativos de informação críticos da organização;
- Avaliação dos riscos associados a cada ativo de informação;
- Estabelecimento de políticas, procedimentos e processos de segurança da informação;
- Identificação de medidas de segurança adequadas para mitigar os riscos;
- Implementação de controles de segurança da informação;
- Monitoramento e revisão do SGSI para garantir sua eficácia e conformidade com as normas aplicáveis.

98

O que é Um Sistema de Gestão de Segurança da Informação (SGSI) ?

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de políticas, procedimentos, processos e práticas organizacionais que têm como objetivo garantir a segurança da informação em uma organização. Ele é baseado em padrões e normas reconhecidos internacionalmente, como a ISO/IEC 27001, e visa identificar, avaliar e gerenciar os riscos de segurança da informação em uma organização.

O SGSI inclui a implementação de medidas de segurança técnica, como firewalls, criptografia e sistemas de detecção de intrusão, bem como medidas organizacionais, como treinamento de funcionários, revisões de segurança e auditorias. Além disso, o SGSI estabelece um processo contínuo de monitoramento e melhoria da segurança da informação na organização.

O SGSI é uma abordagem sistemática e abrangente para a gestão da segurança da informação e ajuda as organizações a protegerem seus ativos de informação, reduzir riscos e garantir a conformidade com as regulamentações aplicáveis.

99

O que são ativos de informação?

Ativos de informação são quaisquer informações, sistemas, dispositivos ou recursos relacionados à tecnologia da informação que possuem valor para a organização, e que necessitam ser protegidos contra ameaças, riscos e vulnerabilidades. Esses ativos incluem dados de clientes, informações financeiras, propriedade intelectual, software, hardware, redes, servidores, dispositivos móveis, entre outros. A identificação e classificação correta dos ativos de informação é fundamental para a elaboração de uma política de segurança da informação eficiente, que possibilite uma gestão adequada dos riscos associados a esses ativos.

100

como se faz a identificação e classificação dos ativos de informação ?

A identificação e classificação correta dos ativos de informação é uma etapa importante para a gestão da segurança da informação em uma organização. O processo envolve os seguintes passos:

1. Identificação dos ativos: o primeiro passo é identificar os ativos de informação da organização, que podem incluir informações em papel, informações eletrônicas, hardware, software, redes, sistemas e serviços.

2. Categorização dos ativos: depois que os ativos são identificados, é necessário categorizá-los com base em seu valor e sensibilidade para a organização. Isso pode ser feito usando critérios como o impacto potencial de uma falha de segurança, o nível de confidencialidade exigido para os dados, a disponibilidade necessária dos sistemas e informações, entre outros.

101

como se faz a identificação e classificação dos ativos de informação ?

3. Avaliação de riscos: a partir da categorização dos ativos, é possível avaliar os riscos associados a cada um deles. Isso envolve a análise de ameaças potenciais, vulnerabilidades e o impacto potencial de uma violação de segurança.

4. Seleção de controles de segurança: com base na avaliação de riscos, é possível selecionar os controles de segurança apropriados para proteger cada ativo de informação. Esses controles podem incluir medidas técnicas, como criptografia e firewalls, bem como políticas e procedimentos organizacionais, como controles de acesso e treinamento de conscientização em segurança.

5. Documentação: por fim, é importante documentar todas as etapas do processo de identificação e classificação dos ativos de informação. Isso ajuda a garantir a consistência e a eficácia da gestão de segurança da informação em toda a organização.

102

Aplicação 2

2- Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes;

A aplicação "Proteção das informações confidenciais de uma organização, tais como informações financeiras, de propriedade intelectual e de clientes" é uma das principais aplicações das normas ISO/IEC 27001 e ISO/IEC 27002. Ela visa garantir que todas as informações confidenciais da organização sejam protegidas de possíveis ameaças, tais como vazamento, roubo ou violação.

103

Aplicação 2

Para atingir este objetivo, as normas propõem a adoção de medidas de segurança em diferentes áreas, incluindo tecnologia da informação, políticas de segurança, processos internos e treinamento de funcionários. Algumas das medidas recomendadas pelas normas incluem:

- Identificação das informações confidenciais da organização e sua classificação de acordo com o nível de sensibilidade;
- Definição de políticas de segurança claras e objetivas, que estabeleçam as responsabilidades de cada funcionário em relação à proteção das informações;
- Implementação de controles de acesso a sistemas e informações, utilizando mecanismos como senhas, autenticação biométrica e criptografia;
- Realização de testes de vulnerabilidade e análises de riscos para identificar possíveis falhas nos sistemas e processos da organização;

104

Aplicação 2

- Monitoramento constante das informações confidenciais da organização, para identificar possíveis violações ou acessos não autorizados;
- Treinamento e conscientização dos funcionários em relação à importância da segurança da informação e das políticas estabelecidas pela organização.
- Com a aplicação das normas ISO/IEC 27001 e ISO/IEC 27002, as organizações podem garantir a proteção das suas informações confidenciais e minimizar o risco de perdas financeiras, danos à reputação e violação de leis e regulamentações. Além disso, a adoção das normas também pode aumentar a confiança dos clientes e parceiros em relação à organização, tornando-a mais competitiva no mercado.

105

Aplicação 3

3- Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações;

Esta aplicação está diretamente relacionada à norma ISO/IEC 27001, que define os requisitos para um sistema de gestão de segurança da informação (SGSI) em uma organização. O objetivo principal é ajudar as empresas a proteger seus ativos de informação, tais como dados financeiros, informações de propriedade intelectual e informações dos clientes.

Para alcançar esse objetivo, a norma estabelece que a empresa deve implementar controles de segurança adequados, que sejam apropriados para os riscos que a organização enfrenta. Esses controles incluem medidas preventivas, como firewalls e criptografia, bem como medidas corretivas, como backups e planos de contingência em caso de incidentes de segurança.

106

Aplicação 3

A norma também requer que a empresa desenvolva uma política de segurança da informação, que descreva os objetivos e metas da segurança da informação e os procedimentos para alcançá-los. A política deve ser clara e comunicada a todos os funcionários da empresa, para garantir que eles compreendam a importância da segurança da informação e estejam cientes de suas responsabilidades.

Outro aspecto importante é o estabelecimento de um processo de avaliação de riscos, que deve ser realizado regularmente para identificar novas ameaças e vulnerabilidades que possam surgir. Com base nessa avaliação, a empresa pode implementar medidas de segurança adicionais ou atualizar as existentes.

Em resumo, a aplicação "Estabelecimento de controles de segurança da informação para prevenir ou minimizar incidentes de segurança, tais como invasões, perda ou roubo de informações" tem como objetivo garantir que a empresa tenha medidas adequadas de segurança da informação para proteger seus ativos mais valiosos e minimizar o risco de incidentes de segurança.

107

Aplicação 4

4- Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação;

Esta aplicação é uma das principais aplicações das normas ISO/IEC 27001 e ISO/IEC 27002.

A segurança da informação envolve a proteção dos dados e informações de uma organização, incluindo informações confidenciais, financeiras, de propriedade intelectual e de clientes. Para garantir a segurança dessas informações, é fundamental identificar e avaliar os riscos de segurança da informação a que a organização está exposta.

A mitigação de riscos é o processo de reduzir o nível de risco associado às informações da organização. Ela envolve a implementação de medidas de segurança, como controles de acesso, criptografia de dados, backups regulares, entre outras. A mitigação de riscos é importante para garantir que as informações da organização estejam protegidas contra ameaças.

108

Aplicação 4

O processo de identificação e avaliação de riscos envolve a análise de ameaças, vulnerabilidades e impactos potenciais. É necessário avaliar as ameaças que podem afetar a organização, como ataques cibernéticos, vírus, fraudes, roubo de informações, entre outros. Também é importante avaliar as vulnerabilidades existentes, como sistemas desatualizados, falta de controles de acesso, falta de backups regulares, entre outros. Além disso, é preciso avaliar o impacto potencial que uma violação de segurança da informação pode ter sobre a organização, seus clientes e parceiros.

Com base na análise de riscos, é possível estabelecer medidas para mitigar esses riscos, como controles de segurança da informação, políticas de segurança, treinamentos, entre outros. A implementação dessas medidas pode ajudar a prevenir ou minimizar incidentes de segurança, como invasões, perda ou roubo de informações.

Assim, a aplicação "Identificação e avaliação de riscos de segurança da informação em uma organização, a fim de estabelecer medidas para sua mitigação" é fundamental para garantir a segurança da informação em uma organização, protegendo seus dados e informações contra ameaças potenciais.

109

Aplicação 5

5- Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis.

A aplicação "Estabelecimento de políticas, procedimentos e diretrizes para a gestão de segurança da informação em uma organização, visando garantir a conformidade com leis e regulamentos aplicáveis" refere-se à implementação das normas ISO/IEC 27001 e ISO/IEC 27002 na criação de políticas de segurança da informação e na definição de processos e diretrizes para garantir que as informações sejam gerenciadas de forma segura e em conformidade com as leis e regulamentações aplicáveis.

Para implementar essa aplicação, é necessário definir políticas e procedimentos claros para lidar com os dados confidenciais da organização, tais como informações financeiras, de propriedade intelectual e de clientes. Essas políticas devem incluir medidas para proteger essas informações, incluindo criptografia, autenticação de usuários e controle de acesso.

110

Aplicação 5

Além disso, é importante estabelecer diretrizes para o gerenciamento de incidentes de segurança da informação, tais como invasões, perda ou roubo de informações. Essas diretrizes devem incluir medidas para detectar, responder e relatar incidentes de segurança da informação.

Por fim, a conformidade com as leis e regulamentos aplicáveis é essencial. Isso significa que a organização deve estar em conformidade com as leis e regulamentos de privacidade de dados, segurança da informação, proteção de dados pessoais, entre outros. As políticas e procedimentos da organização devem ser projetados para garantir que todas as leis e regulamentos aplicáveis sejam cumpridos.

111

Questão sugerida

Quando o Deutsche Bank perdeu seus escritórios nos ataques de 11 de setembro, os funcionários puderam acessar o email corporativo no dia seguinte para que pudessem se conectar com clientes e colegas de trabalho em casa. "Tivemos acesso aos nossos arquivos, embora a TI estivesse na Torre Dois do World Trade Center", diz uma fonte. "Tínhamos backup em Jersey City. Não perdemos nada".

Este relato de adoção de medidas de proteção, nestes termos, poderá ser melhor enquadrado no item da norma ISO/IEC 27002:2013:

a) 7.1: Antes da contratação, dentro do item 7, Segurança em Recursos Humanos.
b) 9.2: Gerenciamento de acesso do usuário, dentro do item 9, Controle de Acesso.
c) 10.1: Controles criptográficos, dentro do item 10, Criptografia.
d) 17.1: Continuidade da segurança da informação, dentro do item 17, Aspectos da segurança da informação na Gestão da Continuidade do Negócio.

112

Fim

113