**QUESTÕES PARA SEREM RESPONDIDAS EM GRUPO SOBRE A NORMA NBR ISO/IEC 17799**

Integrantes:

Alisson Soares Pais

Carlos Eduardo Rabelo Souza

Camilly Vitoria Balduino Silva

Eduardo Galindo de Oliveira

Kawã Augusto Nascimento Dias

3C

* O que é a informação e como ela pode existir dentro de uma organização? Por que é importante protege-la?

Informação é um conjunto organizado de dados que pode constituir uma referência a um fato ou fenômeno. Por meio dela, podemos resolver problemas e tomar decisões, pois seu uso racional é a base do conhecimento.

Assim, pode-se compreender o papel relativo da informação no sucesso organizacional. Eles estão diretamente relacionados à organização de processos, à construção de um negócio e à tomada de decisões nos níveis estratégico, tático e operacional. Portanto, a informação é considerada o ativo mais importante de uma organização.

* Quando falamos de segurança da informação o que significa os termos: confidencialidade, integridade e disponibilidade?

Confidencialidade: Acesso a informação somente para aqueles que possuem autorização; Integridade: Garantia de que o conteúdo está inalterado, sem ter sido alterado; Disponibilidade: Garantia de que os usuários autorizados terão acesso a informação sempre que necessário.

* Como podemos obter Segurança da Informação?

Criando um diagnóstico dos fatores que podem deixar a informação vulnerável; desenvolver políticas de segurança, para o controle da forma que as informações são acessadas, além do desenvolvimento de princípios para o processamento da informação.

* Quais são os principais tipos de ameaças à segurança da informação?

Ao avaliar os riscos dos ativos da organização; a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender; conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações

* Como uma organização pode identificar os seus requisitos de segurança?

A organização deve estabelecer, implementar, operar, monitorar, revisar, manter e melhorar

Um SGSI documentado no contexto das atividades gerais de negócios de uma organização e seus riscos

Face.

A organização deve:

a) Definir o escopo e os limites do SGSI em termos de negócio, organização e suas características

localização, propriedade e tecnologia, incluindo detalhes e justificativa;

b) Definir a estratégia de ISMS de acordo com as características do negócio, organização, localização, ativos

E Tecnologia:

1) Incluir uma estrutura para definir metas e estabelecer uma direção geral e princípios de ação

relacionados à segurança da informação;

2) Considerar requisitos comerciais, legais e/ou regulatórios e obrigações contratuais de segurança;

3) Alinhar com o ambiente de gerenciamento de risco estratégico estabelecido da organização

O ISMS será mantido;

4) estabelecer critérios para avaliar o risco;

5) tenha sido aprovada pela direção.

* Como realizar análises críticas periódicas dos riscos de segurança e dos controles?

O processo de “Diagnóstico de Risco” consiste numa investigação destinada a identificar riscos internos e externos, analisando a probabilidade de ocorrência de ameaças, identificando e abordando vulnerabilidades, tendo em conta os mecanismos de segurança implementados. Ele é projetado para minimizar o risco de perda de confidencialidade, integridade e disponibilidade que podem afetar os negócios. Os diagnósticos de segurança apresentam uma "imagem" do sistema analisado de forma razoável. O sistema de referência pode ser industrial, comercial, apartamento, residencial ou qualquer outra estrutura. No diagnóstico, são analisadas as ameaças e vulnerabilidades, definidos os riscos e consideradas as variáveis ​​externas e internas. O diagnóstico responde às seguintes perguntas: Quão seguro é? Qual plano de ação deve ser seguido para atingir o nível desejado? Uma revisão regular dos riscos de segurança e dos controles implementados é necessária para considerar mudanças nos requisitos e prioridades de negócios, para considerar novas ameaças e vulnerabilidades e para confirmar que os controles permanecem eficazes e adequados.

As análises devem ser realizadas em diferentes níveis de profundidade, dependendo dos resultados das análises de risco realizadas anteriormente e das mudanças nos níveis de risco que a administração considera aceitáveis ​​para o negócio.

* Quais são os controles considerados essenciais para uma organização?

De acordo com o ponto de vista legal, os controles considerados essenciais são:

Proteção de dados e privacidade de informações pessoais ;

Salvaguarda de registros organizacionais;

Direitos de propriedade intelectual;

* Quais são os controles considerados como melhores práticas para a segurança da informação?

Os controles considerados como melhores práticas para a segurança da informação incluem:

a) documento da política de segurança da informação (ver 3.1);

b) definição das responsabilidades na segurança da informação (ver 4.1.3);

c) educação e treinamento em segurança da informação (ver 6.2.1);

d) relatório dos incidentes de segurança (ver 6.3.1);

e) gestão da continuidade do negócio (ver 11.1).

Esses controles se aplicam à maioria das organizações e na maioria dos ambientes. Deve ser notado

Embora todos os controles desta Norma sejam importantes, a relevância de cada controle é determinada à luz desta

riscos específicos aos quais a organização está exposta. Por esta razão, a abordagem acima é considerada um bom ponto

Como ponto de partida, não substitui a seleção de controles com base em uma avaliação de risco.

* 9 Quais são os fatores críticos para o sucesso da implementação da segurança da informação dentro de uma organização?

Política de segurança, objetivos e atividades, que reflitam os objetivos do negócio;

Um enfoque para a implementação da segurança que seja consistente com a cultura organizacional;

Comprometimento e apoio visível da direção;

Um bom entendimento dos requisitos de segurança, avaliação de risco e gerenciamento de risco;

Divulgação eficiente da segurança para todos os gestores e funcionários;

Distribuição das diretrizes sobre as normas e política de segurança da informação para todos os funcionários e fornecedores;

Proporcionar educação e treinamento adequados;

Um abrangente e balanceado sistema de medição, que é usado para avaliar o desempenho da gestão de segurança da informação e obtenção de sugestões para a melhoria.

* As empresas podem criar suas próprias recomendações de segurança

Esta Norma pode servir como um ponto de partida para a empresa criar suas normas com objetivos mais específicos. Nem todas as recomendações e controles desta Norma são aplicadas. Além disso, controles de dados adicionais não incluídos nesta norma podem ser necessários. Quando isso acontece, pode ser útil manter uma referência cruzada para facilitar a verificação de conformidade por auditores e parceiros de negócios.

* Qual a diferença entre avaliação de risco e gerenciamento de risco?

Avaliação de risco é a análise de ameaças, impactos e vulnerabilidades da informação e instalações de processamento da informação e da probabilidade de sua ocorrência. Já o gerenciamento de riscos são processos de indentificão, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação.

* Qual o objetivo de uma Política de segurança da informação e o que deve conter este documento?

O objetivo é guiar a direção e dar apoio em relação a segurança da informação, de forma geralmente padronizada.

De acordo com a norma 3.1.1, deve conter no documento:

Definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação (ver introdução);

Declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação;

Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização;

Definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança;

Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que convém que os usuários sigam.

* Como deve ser feita a Análise crítica e avaliação da Política de Segurança de uma empresa?

A análise crítica deve ser feita pela alta direção, que deve analisar criticamente o sistema de política de segurança, em intervalos planejados, para assegurar a sua pertinência, adequação e eficácia.

* Com relação a Segurança organizacional de uma empresa, porque é importante a criação de uma Infraestrutura da segurança da informação?

Além de eliminar vulnerabilidades e proteger sistemas do negócio contra-ataques, a segurança da informação também contribui para a longevidade da organização. Afinal, o roubo e vazamento de dados também compromete a reputação da empresa no mercado, já que pode causar danos diretos aos seus clientes.

* Quais são as responsabilidades dos gestores de um fórum de segurança da informação?

É da responsabilidade dos gestores de garantir a existência de controles para que o Processo Organizacional de Segurança da Informação existe, seja efetivo, se mantenha ao longo do tempo e possibilite que a organização atinja seus objetivos no que depende do recurso informação.