Prime

ISF – A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Informação Como **Fator De Produção**

Capital | **Mão de Obra** | **Matéria-Prima** | **Tecnologia da Informação**

As empresas não podem existir sem a informação. Será?

Exemplo:

- Banco;
- Siderúrgica;
- PMG Prime;
- Pastelaria;
- Artesão.

Informação

A informação é um ativo como qualquer outro ativo importante;

A informação é essencial para os negócios de uma organização, por isso necessita de proteção;

Ficou ainda mais importante nos negócios por conta da interconexão;

Resultado na exposição a um crescente número e variedade de ameaças e vulnerabilidades.

A informação pode existir em diversas formas:

- Impressa;
- Escrita em papel;
- Armazenada eletronicamente;
- Transmitida pelo correio;
- Transmitida por meios eletrônicos;
- Apresentada em vídeos;
- Faladas em conversas.

Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Segurança

“Estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais; situação em que nada há a temer.”

Oxford

- Investir em soluções de TI cria valor ao consumidor;
- Investir em segurança evita reduzir o valor ao consumidor.

Desafios

- Segurança de TI, normalmente, é encarado como custo ou gasto, e não investimento;
- É como um seguro. Ninguém quer ser roubado ou morrer. Dinheiro jogado fora.

Sistema Da Informação

Responsável pela transformação de dados em informações.

No contexto da SI, é a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional.

Estação de Trabalho, Impressora, SO, software etc.

Conexão, wireless, bluetooth, cabos, roteador, etc.

Servidores, nuvem, apps, Sistemas etc.

Armazenamento, Storage, e-mail, etc.

Smartphone, tablet, IoT, Pabx etc.

- Muitos desses sistemas de informação não foram projetados para serem seguros;
- O nível de segurança alcançado apenas por meio de medidas tecnológicas é limitado;
- Deve ser apoiado por atividades de gerenciamento;
- Apoiados por processos organizacionais apropriados;
- Essencial identificar quais controles usar;
- E atenção aos detalhes ao realizar o tratamento de riscos.

Relação **Informação E Segurança**

Segurança é um termo relativamente:

- Pesado;
- Negativo.

Diz respeito a:

- Proteção;
- Redução de problemas e riscos;
- Seguro ou backup.

A informação pode:

- Ser criada por alguém;
- Ser processada por outro;
- Acessado por muitos.

A informação desempenha um papel:

- Importante:
  - Nos negócios;
  - E na vida pessoal;
- Mas, quase todas as organizações tratam de dados pessoais.

Há uma conexão entre: Risco e Segurança

- Uma não existe sem a outra;
- Riscos levam a consequências não aceitáveis;
- Para isso, há medidas a serem tomadas.

Precisaremos destes tipos de controles

- Físicos;
- Técnicos;
- Organizacionais;
- Recursos Humanos.

Valor da Informação

O valor é atribuído à informação segundo os seus interesses

A informação tem valor para:

- Negócios públicos;
- Setor privado;
- Pequenas empresas;
- Departamentos;
- Indivíduos.

Ou seja, para aqueles que:

- Criam;
- Coletam;
- Processam;
- Armazenam;
- Transmitem;
- Descartam.

Que manipulam informações de várias formas, incluindo:

- Eletrônica;
- Física;
- Verbal.

O valor da informação vai além das palavras escritas, números e imagens. São provenientes de informações intangíveis, como:

- Conhecimento;
- Conceitos;
- Ideias;
- Marcas.

Por isso as informações merecem proteção contra riscos:

- Naturais;
- Acidentais;
- Intencionais.

Importância Da Proteção

Para:

- Obter vantagem competitiva;
- Manter o fluxo de caixa;
- Ter rentabilidade;
- Estar dentro da lei;
- Preservar a imagem da empresa.

É preciso definir:

- O que proteger;
- O que deseja alcançar da SI;
- O que manter na SI;
- O que melhorar da SI;
- O valor da informação.

Contra:

- Vazamento de informação;
- Espionagem;
- Sabotagem;
- Vandalismo;
- Incêndio ou inundação.

Como:

- Códigos maliciosos;
- Vírus;
- Hacking;
- Fraude e roubos;
- Ataques de negação de serviço (DDOS);

Precisamos proteger também os ativos:

- Instalações:
- Informação;
- Software;
- Hardware;
- Serviços impressos (papéis);
- Pessoas;
- Habilidades;
- Experiências;
- Reputação e imagem da empresa.

Visão Geral da Segurança da Informação

A segurança da informação é a disciplina que se concentra na qualidade (confiabilidade)

Baseado na tríade de requisitos

Disponibilidade;

Confidencialidade;

Integridade;

Quem está envolvido no contexto da SI?

- Todos que manipulam informação;
- Todos envolvidos na SI, por meio de contramedidas:
  - Impostas por leis;
  - Impostas por normas internas.

O truque para execução da SI é equilibrar estes aspectos:

- Os requisitos de qualidade que uma organização pode ter para a informação;
- Os riscos que estão associados a estes requisitos de qualidade;
- As contramedidas que são necessárias para minimizar esses riscos;
- Assegurar a continuidade da organização no caso de um desastre.

Segurança da Informação

Segurança da informação:

- É a proteção da informação de vários tipos de ameaças;
- Garante a continuidade do negócio;
- Minimiza o risco ao negócio;
- Maximiza o retorno sobre os investimentos;
- Maximiza oportunidades de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo:

- Políticas;
- Processos;
- Procedimentos;
- Estruturas organizacionais;
- Software;
- Hardware.

Estes controles precisam ser:

- Estabelecidos;
- Implementados;
- Monitorados;
- Analisados criticamente;
- Melhorados, onde necessário

Para garantir que os objetivos do negócio e de segurança da organização sejam atendidos, convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Começando do Começo

Antes de iniciar uma estratégia de segurança, precisamos:

- Saber o que queremos proteger;
- Do que ou de quem queremos proteger;
- Para isso, vamos iniciar uma análise de risco.

Ao analisar os riscos:

- Identificamos os requisitos;
- Os custos;
- Nos guiará e determinará as ações.

A análise (ou avaliação de risco) deve:

- Feita periodicamente;
- Lidar com as mudanças.

“A Segurança é alcançada por meio da aplicação de controles (contramedidas)”

Normas ISO/IEC 27000

A família da norma ISO 27000 contém os padrões relacionados a Segurança da Informação, sendo:

- 27001 – Requisitos base para certificação;
- 27002 – Detalhes dos controles “Código de Práticas”;
- 27003 – Guia de Implementação;
- 27004 – Define métricas, monitoramento, análise e avaliação;
- 27005 – Gerenciamento de Riscos;
- 27006 – Requisitos para órgãos que realizam auditoria;
- 27007 – Diretrizes para auditoria;
- 27008 – Orientação para auditores;
- 27009 – Documento reservado para o comitê que desenvolve variantes para a ISO27k;

E mais 50 outras normas, indo de Segurança da Informação das áreas de Telecomunicações, até:

- Investigação;
- Prevenção de intrusão;
- Fornecedores;
- SI na indústria de energia;
- SI na área de Saúde;
- Segurança cibernética;

Código De Prática Para a **Segurança Da Informação**

A família da norma ISO 27000 contém algumas partes com códigos de práticas que nos ajuda a:

- Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação;
- Implementar e operar controles para gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização.
- Monitorar e revisar o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (Information Security Management System – ISMS).
- Melhorar continuamente com base nas medições objetivas.

Códigos de Práticas da série ISO 27000:

- 27002:2013, "Código de prática para a segurança da informação";
- 27002:2022, com o título alterado para "Segurança da Informação, Segurança Cibernética e Proteção da Privacidade, Controles de Segurança da Informação".

Além de:

- Nas organizações de Telecomunicações: ISO/IEC 27011, Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations;
- Serviços na Nuvem: ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- Para Privacidade e Proteção (PII): ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

Requisitos da **Segurança da Informação**

a) Avaliação de riscos para a organização identificar:

- Ameaças;
- Vulnerabilidades dos ativos;
- Probabilidade de ocorrência das ameaças;
- Impacto potencial ao negócio;
- Os controles necessários;
- Que o risco residual atenda aos seus critérios de aceitação de risco.

b) Requisitos legais, como:

- Legislação vigente;
- Estatutos;
- Regulamentação;
- Cláusulas contratuais com seus parceiros, prestadores de serviços, etc.
- Cumprimento do seu ambiente sociocultural.

c) Iniciativas da própria organização, como um conjunto de:

- Princípios;
- Objetivos;
- Requisitos inerentes ao negócios;
- Tudo aquilo que a organização precise para desenvolver e apoiar suas operações.

Contramedidas

O que são Contramedidas?

- Sinônimo para salvaguarda ou controles;
- Um controle é um conjunto de medidas para gerenciar riscos incluindo:
  - Políticas;
  - Regras;
  - Processos;
  - Procedimentos;
  - Diretrizes;
  - Práticas.

Exemplo de controles definidos pela norma:

- Barreiras (catracas, portas);
- Senhas;
- Políticas de segurança;
- Backup;
- Controle de acesso lógico.

Em resumo, as contramedidas de segurança são os controles usados para proteger os dados e sistemas de informação quanto a:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Seleção de Controles

A ISO 27002 tem uma série de controles!
Então, primeiro eu faço o levantamento dos riscos.

E aí, o riscos identificados devem ser baseados:

- Nos critérios de aceitação de riscos;
- Opções de tratamento de riscos;
- Abordagem de gerenciamento de riscos.

A seleção dos controles leva em consideração:

- As decisões da organização após uma avaliação de riscos;
- Todas as legislações e regulamentações nacionais e internacionais relevantes;
- Maneira pela qual os controles interagem uns com os outros;
- Recursos e investimentos;
- O equilíbrio entre os controles e o potencial impacto nos negócios;
- Impacto resultante de incidentes de segurança na ausência desses controles;
- Encare os controles como princípios orientadores para o gerenciamento de SI;
- Pode ser um ponto de partida para o desenvolvimento de diretrizes da organização;
- Nem todos os controles podem ser aplicáveis a todas as organizações;
- Pesquisar mais opções de tratamento de risco na ISO/IEC 27005.

Ciclo de Vida **da Informação**

- A informação tem um ciclo de vida, desde a criação até o descarte;
- O valor e os riscos das informações podem variar ao longo deste ciclo de vida;
  - Por exemplo, o valor de uma informação antes e depois de ser roubada e divulgada, ou os riscos na criação e no armazenamento na nuvem, e por fim, depois que dados são descartados;
  - Mas a integridade permanece crítica;
  - Portanto, a segurança da informação permanece importante até certo ponto da etapa do ciclo.
- Já os sistemas de informação têm os seus ciclos:
  - Concepção;
  - Especificação;
  - Projeto;
  - Desenvolvimento;
  - Testes;
  - Implementação;
  - Utilização;
  - Manutenção;
  - E eventualmente, os serviços são retirados e descartados.

- A segurança da informação deve ser considerada em todas essas etapas;
- Oportunidades são geradas em:
  - Novos projetos de desenvolvimento de sistemas;
  - Mudanças nos sistemas existentes;
  - Lições aprendidas com incidentes.

Sistema de Gerenciamento de **Segurança da Informação**

A ISO/IEC 27001 especifica um SGSI, ela é a referência!

Um Sistema de Gerenciamento de Segurança da Informação SGSI (ISMS) deve adotar:

- Uma visão holística e coordenação dos riscos;
- Implementação de um conjunto abrangente de controles.

Um SGSI bem-sucedido requer:

- Apoio de todo o pessoal da organização;
- Pode exigir a participação de outras partes interessadas, como:
  - Acionistas;
  - Fornecedores.;
  - O conselho de especialistas.
- Um SGSI adequado traz garantias à organização e partes interessadas;
- Garantias que suas informações e ativos serão mantidos razoavelmente:
  - Seguros;
  - Protegidos contra ameaças;
  - Protegidos contra danos.

OBRIGADO

ISF – A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO