EXIN INFORMATION SECURITY

Apostila Preparatória para Certificação

ISO/IEC 27002 Foundation

Área de Aprendizagem

PMG academy

www.pmgacademy.com

Official Course

www.pmgacademy.com

Design: By Freepik

Instrutor - Prof. Adriano Martins Antonio

ISO 27002

Esta apostila está dividida em quatro partes.

I – Atualização de Conceitos:

Este material é complementar ao curso oficial ISO 27002 Foundation.

Ele foi desenvolvido com o objetivo de alinhar este curso aos novos conceitos que são utilizados em nossa área. Adicionalmente, alguns destes conceitos ou termos são exigidos pela própria EXIN previamente, pois ela julga fazer parte do conhecimento geral dos alunos, porém entendemos que nem todos os alunos tem conhecimento prévio de tudo que é solicitado no exame, independente se é básico ou atual.

Os próximos conteúdos podem ser cobrados ou mencionados no exame de certificação por isso é importante estudá-los com dedicação e atenção.

II – Conteúdo do Curso:

Este material é complementar ao curso oficial da ISO/IEC 27002 Foundation (ISFS) e tem o objetivo apresentar os conceitos de segurança da informação sob a ótica da própria norma, cujo texto foi extraído.

Este conteúdo não só te ajudará a entender mais sob os assuntos abordados no curso, como também te proporcionará maior segurança no exame de certificação internacional da EXIN, por isso, leia e releia quantas vezes achar necessário.

III – Guia Preparatório:

Os requisitos do exame são os principais temas de um módulo. O candidato deve ter o domínio completo sobre estes temas. Os requisitos do exame são elaborados na especificação do exame. Neste tópico você terá uma visão do peso de cada tópico e os itens cobrado no exame.

IV – Glossário

ISO 27002

I – Atualização de conceitos:

Este material é complementar ao curso oficial ISO 27002 Foundation. Ele foi desenvolvido com o objetivo de alinhar este curso aos novos conceitos que são utilizados em nossa área. Adicionalmente, alguns destes conceitos ou termos são exigidos pela própria EXIN previamente, pois ela julga fazer parte do conhecimento geral dos alunos, porém entendemos que nem todos os alunos tem conhecimento prévio de tudo que é solicitado no exame, independente se é básico ou atual.

Os próximos conteúdos podem ser cobrados ou mencionados no exame de certificação por isso é importante estudá-los com dedicação e atenção.

Política de Segurança para Equipamentos Móveis

Como é difícil fazer um seguro contra perdas e roubo de Equipamentos Móveis, é aconselhável adote uma política de segurança que contenha as seguintes técnicas:

- Zero Footprint, ou seja, técnica que possibilita o acesso seguro as informações a partir de dispositivos móveis, já que não há a necessidade de instalação de nenhum software;
- Tunneling, que funciona como empacotamento dos dados trafegados;
- Proteção contra malware;
- Controle de acesso;
- Restrição da instalação do software;
- Registro de dispositivos;
- Criptografia;
- Backups;
- Aplicação de patches;
- Endurecimento (hardening), técnica e processo de proteção do sistema do servidor que impede riscos aos dispositivos;
- Treinamento de usuários;

Os usuários não devem usar seus dispositivos móveis em locais públicos e outras áreas desprotegidas.

Teletrabalho

O objetivo de uma política de teletrabalho é garantir que os benefícios do teletrabalho possam ser alcançados sem aumentar indevidamente o risco para ativos de informação da organização.

ISO 27002

Muitos dos controles de segurança existentes que são construídos para serem usados internamente em um ambiente de trabalho estão suscetíveis de se perderem a partir do teletrabalho, então, os controles devem ser substituídos por políticas e procedimentos adequados. A necessidade de políticas formais aumenta se o teletrabalho for da casa do funcionário, pois pode haver uma tentação de inverter o comportamento profissional pelo pessoal.

Qualquer organização que permite o teletrabalho para a sua equipe deve fazê-lo com base numa avaliação de riscos. As medidas de controle adequadas podem exigir o fornecimento de equipamento, tanto na empresa quanto no local do teletrabalho, em particular para garantir a segurança das comunicações. Então, software e equipamentos precisam ser licenciados e mantidos, as licenças precisam ser verificadas para garantir que cubram o trabalho remoto e alguns meios adequados de manutenção destes equipamentos, além de continuar o trabalho se os equipamentos não estiverem disponíveis. Também será necessário garantir instalações apropriadas de um escritório no local do teletrabalho, incluindo pelo menos o armazenamento seguro para documentos sensíveis e meios de comunicação e, possivelmente, outros equipamentos como trituradores.

Embora os requisitos gerais de uma política de teletrabalho possam ser aplicados a todos os teletrabalhadores da empresa, os riscos podem ser muito diferentes em cada caso, dependendo da localização e a criticidade dos ativos de TI que o membro da equipe irá utilizar, portanto, é provável que o acordo de teletrabalho com cada pessoa possa exigir a sua própria avaliação de risco, e com isso, cada contrato pode ser diferente em algum detalhe.

Os quatro elementos a seguir devem ser considerados no desenvolvimento de uma política de teletrabalho:

- Autorização;
- Provisão de equipamentos;
- Segurança da informação, enquanto do teletrabalho;
- Utilização de equipamentos no teletrabalho.

BYOD

Em relação à propriedade dos ativos, BYOD: Bring Your Own Device (Traga seu próprio aparelho) é um termo que não deve ser esquecido jamais. BYOD é seu próprio dispositivo, pois normalmente as empresas dão aos funcionários a possibilidade de usar seus próprios dispositivos para o trabalho dentro da empresa. Se for esse o caso, os bens pessoais (um tablet, laptop ou telefone celular) contêm informações de negócios e essas informações devem ser protegidas como tal.

Por isso deve haver uma política para o BYOD dentro da empresa e as informações sobre os ativos BYOD devem ser protegidas.

ISO 27002

Acordos de Confidencialidade ou de Não Divulgação (NDA) na Cloud Computing

As informações confidenciais devem ser devidamente identificadas e protegidas adequadamente, mas as pessoas dentro e fora da empresa não precisam ter acesso às informações confidenciais, por exemplo, como um administrador de banco de dados, devido à natureza do seu trabalho.

Se empresa decidir que o novo sistema de TI deva ficar localizado na nuvem(Cloud Computing), o que potencialmente significa que o fornecedor da nuvem pode ter acesso aos dados confidenciais da empresa, ela então deve proteger a informação e criar uma estrutura jurídica com acordos de confidencialidade ou de não divulgação.

Nesses acordos deve constar a propriedade dos dados, a permissão de acesso aos dados e também as ações que devem ser tomadas em caso de uma violação da confidencialidade. Estes acordos devem ser elaborados com a ajuda de um conselheiro legal, tal como um advogado.

O Cumprimento das Normas Legais

As regulamentações específicas do governo são geralmente específicas de cada país e podem incluir regras de segurança para informações especiais (sensíveis ou classificadas). Informações especiais é um termo para as informações que precisam de proteção extra com base na natureza sensível que decorre de seu potencial impacto ou do risco para a segurança nacional.

Revisões de Segurança de Informação

Revisões são úteis como um meio de avaliar periodicamente as medidas de segurança, processos e procedimentos. Dependendo do escopo de uma avaliação, pode ser utilizado para diferentes fins. Revisões podem ser aplicadas para testar se as medidas de segurança estão em conformidade com os requisitos definidos, tais como os padrões da empresa, legislação e regulamentos. Elas são aplicadas para avaliar se as medidas de segurança estão em conformidade com os requisitos específicos de segurança identificados por um sistema de informação e que estas medidas sejam implementadas e mantidas de forma eficaz. Finalmente, as revisões também ajudam a verificar que estas medidas estão funcionando como especificado e esperado.

Para garantir a importância das revisões, elas devem fazer parte de um programa de revisão. Os elementos deste programa incluem, entre outras coisas:

- O escopo das revisões
- Critérios de revisão
- Frequência
- Revisões de metodologias.

O plano deve indicar quais áreas precisam ser revistas juntamente com os resultados das avaliações anteriores. É importante prestar atenção na seleção dos auditores, pois deve haver a garantia de uma imparcialidade no processo de revisão. Uma regra de ouro é que um auditor nunca deva avaliar seu próprio trabalho. O gerente responsável deve assegurar que quaisquer não conformidades identificadas sejam resolvidas e que suas causas sejam investigadas, além disso, ele deve assegurar que quaisquer ações necessárias sejam tomadas e deve verificar os resultados dessas ações.

Segurança no Desenvolvimento de Programas

Na ISO 27002:2005 era chamado de "terceirização do desenvolvimento de programas", mas na ISO 27001:2013 foi alterado para "Fornecedor de Gerenciamento de Prestação de Serviços". Quando o desenvolvimento de programas for terceirizado, é importante que este desenvolvimento seja supervisionado e controlado pela organização, e se possível, o cliente deve ter os direitos de propriedade intelectual.

Ao monitorar regularmente, rever a prestação de serviços dos fornecedores, a empresa deve assegurar que os termos de segurança da informação e as condições dos acordos estão sendo cumpridos e que os incidentes de segurança da informação e os problemas estão sendo geridos de forma adequada.

Outra maneira de assegurar o serviço dos fornecedores é através da certificação por um organismo independente. O organismo independente pode usar ISO 27001, por exemplo, para certificar sistema de gestão de segurança da informação dos fornecedores e ISO 9001 para seu sistema de gestão da qualidade.

Mudanças nos serviços dos fornecedores devem ser geridas, tendo na criticidade da informação de negócio, sistemas e processos envolvidos quanto na reavaliação dos riscos. Quando uma organização está mudando os serviços oferecidos, a modificação ou atualização de produtos (aplicações, sistemas, etc.) ou desenvolvimento de novos sistemas, levará às mudanças ou atualizações dos SLAs também. Nestes acordos devem constar também as responsabilidades e obrigações dos subempreiteiros.

Evento de Segurança da Informação

É uma ocorrência identificada em um sistema, serviço ou rede indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possam ser relevantes na segurança.

ISO 27002

Big Data

Big Data é um termo amplamente utilizado para nomear conjuntos de dados muito grandes ou complexos, porém é essencial entender a diferença entre dados e informações. Os dados podem ser processados pela tecnologia da informação, mas tornam-se informações, após ter adquirido certo significado. Em se tratando de segurança da informação, é indiferente a forma como a informação é apresentada, no entanto, há algumas restrições sobre as medidas que são necessárias para proteger essas informações.

É a Informática que converter os dados em informações, ela que desenvolve novos usos para a tecnologia da informação, está interessada em como as pessoas transformam a tecnologia, e como a tecnologia nos transforma.

Os dados podem ter grande significados - dependendo de como ele é usado - mesmo se ele não está no formato de "informação". Não haveria necessidade de "proteção de dados" e, portanto, "a segurança do computador" se os dados, por definição, não tivesse nenhum significado. O valor dos dados é determinado principalmente pelo usuário.

Conformidade com as Políticas e Normas de Segurança

Há muitas organizações e normas sobre segurança da informação. Os padrões mais importantes são desenvolvidos pela ISO, NIST e ANSI. Na Europa, a norma ISO é a mais comum em uso. Nos EUA, os padrões NIST e ANSI são mais comuns. A maioria das normas abrangem os mesmos objetivos de segurança. Cada norma dá mais atenção a um determinado elemento dentro da disciplina que o diferencia de outros padrões.

ISO: Fundada em 1947, é uma federação mundial de órgãos nacionais de padronização em torno de 100 países, com um corpo de padrões representando cada país membro. A American National Standards Institute (ANSI), por exemplo, representa os Estados Unidos. As organizações membros colaboram no desenvolvimento e na promoção de normas internacionais. Entre os padrões que a ISO promove, existe a Interconexão de Sistemas Abertos (OSI), um modelo de referência universal para protocolos de comunicação.

NIST: National Institute of Standards and Technology - NIST é uma unidade do Departamento de Comércio dos EUA. O NIST 800 Series é um conjunto de documentos que descreve as políticas, procedimentos e diretrizes de segurança de computadores do Governo Federal dos Estados Unidos. Os documentos estão disponíveis gratuitamente, e podem ser úteis para as empresas e instituições de ensino, bem como às agências governamentais. As publicações da Série NIST 800 evoluiu como resultado de uma pesquisa exaustiva sobre métodos viáveis e de baixo custo para otimizar a segurança da tecnologia da informação e das redes, de forma proativa. As publicações abrangem

ISO 27002

Todos os procedimentos e critérios que o NIST recomenda para avaliar e documentar as ameaças e vulnerabilidades e para a implementação de medidas de segurança para minimizar o risco de eventos adversos. As publicações podem ser úteis como diretrizes para a aplicação das regras de segurança e como referências legais em caso de problemas de segurança. Em fevereiro 2014 NIST publicou um novo quadro de segurança cibernético para infraestruturas críticas. Este quadro é muito interessante para qualquer indústria lidar com infraestruturas críticas. Ele fornece um ponto de vista útil sobre a aplicação de uma estrutura de segurança e utiliza não só os padrões NIST, mas também as normas ISO (27xxx) também.

ANSI: American National Standards Institute - ANSI é a principal organização que fomenta o desenvolvimento de padrões de tecnologia nos Estados Unidos. A ANSI trabalha com grupos da indústria e é o membro EUA da International Organization for Standardization (ISO) e da Comissão Eletrotécnica Internacional (IEC). A ANSI já estabeleceu normas de computador incluindo a American Standard Code para Information Interchange (ASCII) e do Small Computer System Interface (SCSI).

ITU-T: Sector da Normalização das Telecomunicações da União Internacional das Telecomunicações – ITU-T é o organismo internacional principal para desenvolver normas cooperativas para equipamentos e sistemas de telecomunicações. Antigamente, era conhecido como o CCITT e está localizada em Genebra, Suíça.

IEEE: Institute of Electrical and Electronics Engineers descreve-se como "a maior sociedade técnica profissional do mundo - promovendo o desenvolvimento e aplicação de tecnologia eletrônica e ciências afins para o benefício da humanidade, o avanço da profissão, e o bem-estar dos nossos membros." O IEEE promove o desenvolvimento de padrões que muitas vezes se tornam normas nacionais e internacionais. A organização publica um número de revistas, tem muitos capítulos locais, e grandes sociedades em áreas especiais, como o IEEE Computer Society. Os protocolos utilizados em uma base mundial para a conexão de rede sem fio são baseados na tecnologia IEEE, como os padrões de A, B, G e N e o WEP padrões de criptografia e WPA.

OWASP - Open Web Application Security Project (Projeto de Segurança de Aplicações Web Abertas): é um projeto de segurança de aplicativos de código aberto. A comunidade OWASP inclui corporações, organizações educacionais e indivíduos de todo o mundo. Esta comunidade trabalha para criar e disponibilizar livremente artigos, metodologias, documentação, ferramentas e tecnologias. A Fundação OWASP é uma organização de caridade que apoia e gerencia projetos e infraestrutura do OWASP. OWASP não faz afiliação com nenhuma empresa de tecnologia, embora ela suporte o uso da tecnologia de segurança. OWASP tem evitado filiação, pois considera que a liberdade das pressões organizacionais possa tornar o fornecimento de informações mais fácil, imparcial, prático e de baixo custo sobre a segurança de aplicativos. Os defensores do OWASP

consideram as dimensões: pessoas, processos e tecnologia. OWASP também é um corpo de padrões emergentes, com a publicação do seu primeiro padrão em Dezembro de 2008, o Padrão de Verificação de Segurança de Aplicações (ASVS - Open Web Application Security Project). O objetivo principal do projeto OWASP ASVS é normalizar a cobertura e o nível de rigor disponível no mercado quando se trata de realizar a verificação de segurança em nível de aplicativo. O objetivo é criar um conjunto de padrões abertos comercialmente viáveis que são adaptados às tecnologias específicas baseadas na web.

A edição Web Application foi publicada e um serviço Web Edition está em desenvolvimento.

PCI - Indústria de Cartões de Pagamento: É fato que o comércio que usa a Internet se baseia exclusivamente na confiança, os usuários não usam sistemas que acreditam ser inseguros. O PCI obriga o cumprimento de suas regras para os comerciantes, processadores de pagamento de terceiros e agências de serviço. PCI adotou OWASP como o padrão de fato para a proteção de cartões de pagamento.

II – Conteúdo do Curso:

O que é segurança da informação?

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada 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 da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as 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 e funções de

software e hardware.

Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e 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.

Por que a segurança da informação é necessária?

A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, hackers e ataques de denial of servisse (DoS) estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infraestruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se controlar o acesso. A tendência da computação distribuída reduz a eficácia da implementação de um controle de acesso centralizado.

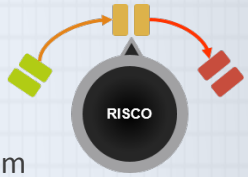
Muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controles a serem implantados requer um planejamento cuidadoso e uma atenção aos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de acionistas, fornecedores, terceiras partes, clientes ou outras partes externas. Uma consultoria externa especializada pode ser também necessária.

Código de prática

A ISO/27002 estabelece diretrizes e princípios gerais para iniciar, implementar, manter

e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêm diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação.

Os objetivos de controle e os controles desta Norma têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. Esta Norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades Interorganizacionais.



Análise, avaliação e tratamento de riscos

Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos.

O processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos. Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).

Convém que as análises/avaliações de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando uma mudança significativa ocorrer. Essas análises/ avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.

Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário. O escopo de uma análise/avaliação de riscos pode tanto ser em toda a organização, partes da organização, em um sistema de informação específico, em componentes de um sistema específico ou em serviços onde isto seja praticável, realístico e útil.

Tratando os riscos de segurança da informação

Convém que, antes de considerar o tratamento de um risco, a organização defina

Os critérios para determinar se os riscos podem ser ou não aceitos. Riscos podem ser aceitos se, por exemplo, for avaliado que o risco é baixo ou que o custo do tratamento não é economicamente viável para a organização. Convém que tais decisões sejam registradas.

Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada. Possíveis opções para o tratamento do risco incluem:

a) Aplicar controles apropriados para reduzir os riscos;
b) Conhecer e objetivamente aceitar os riscos, sabendo que eles atendem claramente à política da organização e aos critérios para a aceitação de risco;
c) Evitar riscos, não permitindo ações que poderiam causar a ocorrência de riscos;
d) Transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Convém que, para aqueles riscos onde a decisão de tratamento do risco seja a de aplicar os controles apropriados, esses controles sejam selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos. Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se em conta:

a) Os requisitos e restrições de legislações e regulamentações nacionais e internacionais;
b) Os objetivos organizacionais;
c) Os requisitos e restrições operacionais;
d) Custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais às restrições e requisitos da organização;

A necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Política de segurança da informação

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

A política de segurança da informação pode ser uma parte de um documento da política geral. Se a política de segurança da informação for distribuída fora da organização, convém que sejam tomados cuidados para não revelar informações sensíveis.

ISO 27002

Uma política de mesa limpa e tela limpa reduz o risco de acesso não autorizado, perda e dano da informação durante e fora do horário normal de trabalho. Cofres e outras formas de instalações de armazenamento seguro também podem proteger informações armazenadas contra desastres como incêndio, terremotos, enchentes ou explosão. Considerar o uso de impressoras com função de código PIN, permitindo desta forma que os requerentes sejam os únicos que possam pegar suas impressões, e apenas quando estiverem próximos às impressoras.

Conexões sem autorização e inseguras nos serviços de rede podem afetar toda organização. Este controle é particularmente importante para conexões de redes sensíveis ou aplicações de negócios críticos ou para usuários em locais de alto risco, por exemplo, áreas públicas ou externas que estão fora da administração e controle da segurança da organização.

O Que É?

- ISO: International Organization for Standardization (ou, em português, Organização Internacional para Padronização)
- IEC: International Electro-technical Commission (ou, em português, Comissão Eletrotécnica Internacional)
- ISO/IEC 27002:2013 Tecnologia da Informação— Técnicas de Segurança— Código de Prática para Controles de Segurança da Informação (anteriormente ISO/IEC 7002:2005)
- Capítulos dentro da Norma:

1. Introdução
2. Escopo
3. Referências Normativas
4. Termos e Definições
5. Estrutura desta Norma
6. Políticas de Segurança da Informação
7. Organização da Segurança da Informação
8. Segurança do Recursos Humanos
9. Gestão de Ativos
10. Controle de Acesso
11. Criptografia
12. Segurança Física e Ambiental
13. Operações de Segurança
14. Segurança das Comunicações
15. Sistema de Aquisição, Desenvolvimento e Manutenção
16. Relacionamento com Fornecedores
17. Gestão de Incidentes de Segurança da Informação
18. Aspectos de Segurança da Informação da Gestão de Continuidade de Negócios
19. Conformidade

ISO 27002

Dados e Informações

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

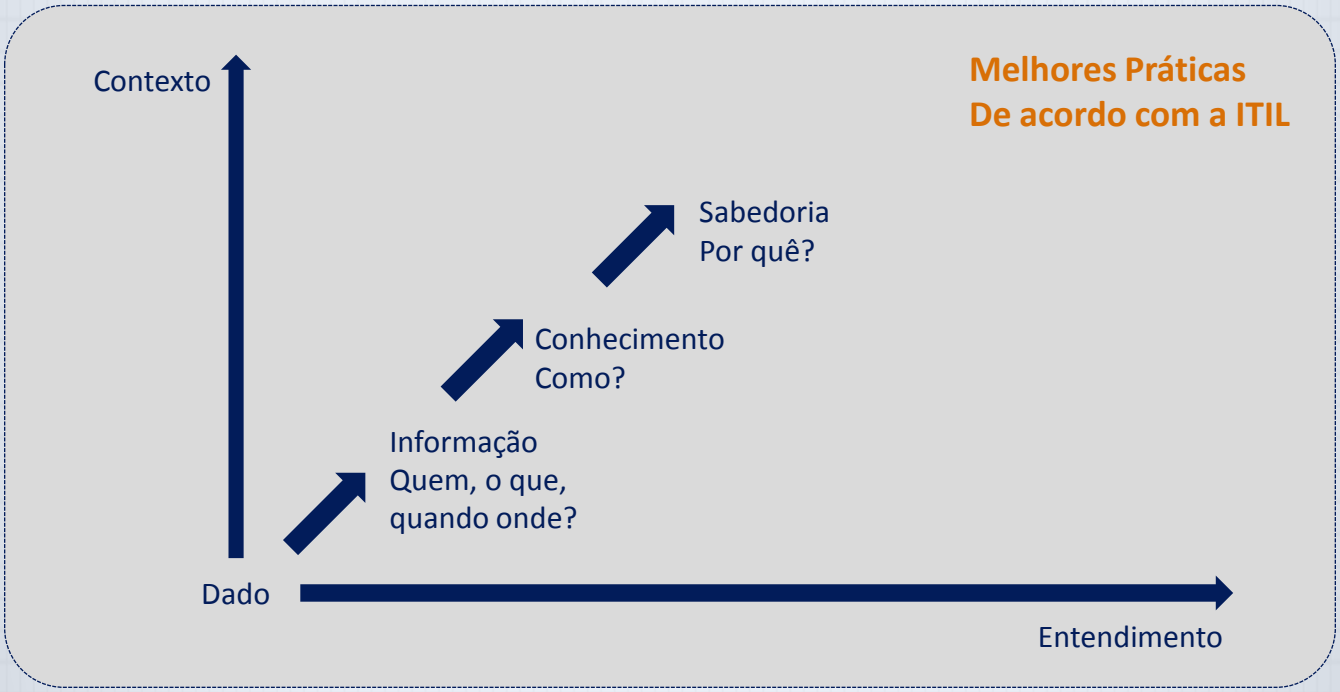
- Dados podem ser processados pela Tecnologia da Informação, mas apenas se tornam informação após terem adquirido um certo significado;
- Informação pode assumir a forma de texto, mas também da palavra falada e de imagens de vídeo.

Dados:	02/04/09
Informações:	02/04/09
	mm-dd-aa

Exemplos de mídias para armazenamento de dados:

- Papel
- Microficha
- Magnético (ex.: fitas)
- Óptico (ex.: CDs)

DIKW: Dados, Informação, Conhecimento, Sabedoria



ISO 27002

A informação é a compreensão das relações entre partes dos dados
Informação responde quatro questões:

- Quem?
- O que?
- Quando?
- Onde?

Preservação da confidencialidade, integridade e disponibilidade da informação, além disso, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também podem estar envolvidas.

O Que é Segurança da Informação

Segurança da Informação envolve a definição, implementação, manutenção e avaliação de um sistema coerente de medidas que garantam a disponibilidade, integridade e confidencialidade do fornecimento (manual e informatizado) de informações.

Sistema de Informação – Tecnologia da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.

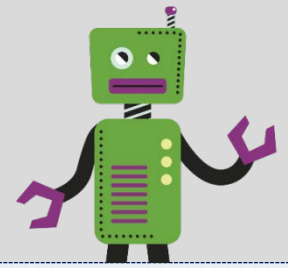
Sistemas de Informação

- A transferência e processamento de informação ocorrem através de um Sistema de Informação
- Cada sistema cujo objetivo é transferir informação é um Sistema de Informação
- Exemplos de Sistemas de Informação são arquivos em armários, telefones celulares e impressoras
- No contexto da Segurança da Informação, um Sistema de Informação é toda a combinação de meios, procedimentos, regras e pessoas que asseguram o fornecimento de informações para um processo operacional

ISO 27002

Tecnologia de Informação

- O uso da tecnologia para armazenamento, comunicação ou processamento de informações.
- A tecnologia inclui tipicamente computadores, telecomunicações, aplicativos e outros softwares.
- As informações podem incluir dados do negócio, voz, imagens, vídeos e etc.
- Tecnologia da Informação é frequentemente usada para apoiar Processos de Negócios através de Serviços de TI.



Valor da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

ISO/IEC 27002 Specification

- O valor da informação é determinado pelo valor que o destinatário atribui a ela.
- História e contexto: O valor da informação vai além das palavras escritas, números e imagens: conhecimentos, conceitos, ideias e marcas são exemplos de formas intangíveis de informações. Em um mundo interconectado, informações e processos relacionados, sistemas, redes e funcionários envolvidos na operação, no manuseio e na proteção, são ativos, como outros ativos importantes do negócio, valiosos para os negócios de uma organização e, consequentemente, merecem ou exigem proteção contra diversos perigos.
- Considerações sobre o ciclo de vida: O valor e os riscos dos ativos podem variar durante sua vida. A segurança da informação continua a ser importante até certo ponto em todas as fases.
- A identificação dos riscos relacionados ao acesso de partes externas deve levar em conta as seguintes questões: valor e sensibilidade das informações envolvidas, e sua importância para as operações do negócio.
- As informações devem ser classificadas de acordo com seu valor, requisitos legais, sensibilidade e importância à organização.
- Os requisitos e controles de segurança devem refletir o valor para o negócio dos ativos de informação envolvidos, assim como seu dano potencial de negócio, que pode resultar de uma falha ou ausência de segurança.
- Classificação de informações: As informações devem ser classificadas de acordo com seus requisitos legais, valor, importância e sensibilidade à divulgação ou modificação não autorizada.

ISO 27002

Responsabilidades do gerenciamento: Um gerenciamento ruim pode fazer com que os funcionários se sintam desvalorizados, resultando em um impacto negativo de segurança da informação sobre a organização. Por exemplo, o gerenciamento ruim pode fazer com que a segurança da informação seja negligenciada ou pode levar a um potencial uso indevido dos ativos da organização.

Informação como um Fator de Produção

Os fatores de produção típicos de uma organização são:

- Capital;
- Mão-de-obra (manual) e;
- Matéria prima.

Na Tecnologia de Informação, é comum considerar também a Informação como um fator de produção:

- As empresas não podem existir sem informações.
- Um armazenamento que perde seu cliente e as informações guardadas não seria capaz de operar sem elas.
- Algumas empresas, como escritórios de contabilidade, bancos, seguradoras, possuem informações como seus únicos produtos/serviços.

Valor ao Negócio

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.

Segurança da Informação fornece a garantia dos Processos de Negócio através da aplicação de Controles de Segurança apropriados em todas as áreas de TI e de gerenciamento de Riscos de TI alinhados com os processos e diretrizes do Gerenciamento de Riscos Corporativos e de Negócios

Integridade

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

A Confiabilidade da informação é determinada por três aspectos:

- Confidencialidade;
- Integridade;
- Disponibilidade.

A confidencialidade é o grau no qual o acesso à informação é restrito a um grupo específico autorizado a ter esse acesso. Isto também inclui medidas para proteger a privacidade:

- O acesso à informação é concedido diante da necessidade de ter conhecimento. Não é necessário, por exemplo, para um empregado do setor financeiro ser capaz de ver relatórios de conversas com clientes.
- Os empregados tomam medidas para garantir que a informação não chegue àquelas pessoas que não precisem dela. Eles garantem, por exemplo, que nenhum documento confidencial se encontre sobre suas mesas enquanto eles estão longe (política da mesa limpa).
- O gerenciamento de acesso lógico garante que pessoas ou processos não autorizados não possuam acesso aos sistemas, bancos de dados e programas automatizados. Um usuário, por exemplo, não tem o direito de alterar as configurações de seu computador.
- Uma segregação de funções é criada entre a organização de desenvolvimento do sistema, a organização de processamento e a organização do usuário. Um desenvolvedor de sistema não pode, por exemplo, efetuar alterações de salários.
- Segregações estritas são criadas entre o ambiente de desenvolvimento, o ambiente de teste e de aceitação e no ambiente de produção.
- No processamento e no uso de dados, são tomadas medidas para garantir a privacidade dos funcionários e de terceiros. O departamento de Recursos Humanos (RH) tem, por exemplo, a sua própria unidade de rede que não é acessível a outros departamentos.
- O uso de computadores por usuários finais está cercado por medidas para que a confidencialidade das informações seja garantida. Um exemplo é uma senha que dá acesso ao computador e à rede.

A integridade é o grau em que a informação está atualizada e sem erros.

As características da Integridade são:
- A Exatidão das informações
- A Probidade das informações

Medidas de Integridade

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Mudanças nos sistemas e nos dados são autorizados. Por exemplo, um membro da equipe entra com um novo preço para um item no site e outro membro verifica a validade desse preço antes de ser publicado;
- Sempre que possível, os mecanismos são construídos de forma que forcem as pessoas a usar o termo correto. Por exemplo, um cliente é sempre chamado de "cliente", o termo "comprador" não pode ser inserido no banco de dados para se referir ao cliente;
- As ações dos usuários são gravadas (registradas) de modo que é possível determinar quem realizou uma mudança na informação;

- As ações vitais do sistema, por exemplo, a instalação de um novo software, não podem ser realizadas por apenas uma pessoa. Ao segregar funções, posições e autoridades, pelo menos duas pessoas serão necessárias para realizar uma mudança que tem consequências importantes;
- A integridade dos dados pode ser assegurada em grande parte através de técnicas de encriptação, que protegem a informação de alterações ou acessos não autorizados. Os princípios de política e de gestão para a criptografia podem ser definidos em um documento separado de política

Disponibilidade

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Disponibilidade é o grau em que a informação está Disponível para o usuário e para o sistema de informação que está em operação no momento em que a organização a solicita.

As características de Disponibilidade são:

- Pontualidade: os sistemas de informação estão disponíveis quando necessário
- Continuidade: o pessoal pode continuar a trabalhar caso ocorra uma falha
- Robustez: Há capacidade suficiente para permitir que todos os empregados no sistema trabalhem

Medidas de Disponibilidade

- A gestão e o armazenamento de dados são realizados de forma que as chances de ocorrer uma perda de informação são mínimas. Os dados são, por exemplo, armazenados em um disco na rede, não no disco rígido do PC.
- Procedimentos de backup são criados. Os requisitos do regulamento para quanto tempo os dados devem permanecer armazenados são levados em consideração. O local do backup é separado do local físico do negócio para assegurar a disponibilidade dos dados em casos de emergência.
- Procedimentos de emergência são criados para garantir que as atividades possam ser retomadas o mais rápido possível após uma interrupção em grande escala.

Arquitetura da Informação

- A Segurança da Informação está intimamente relacionada à Arquitetura da Informação.
- A Arquitetura da Informação é o processo que está concentrado na definição do fornecimento de informações dentro de uma organização.
- A Segurança da Informação pode ajudar a garantir que o conjunto de requisitos do fornecimento de informações seja feito através da Arquitetura da Informação.

ISO 27002

- A Arquitetura da Informação se concentra principalmente em atender a necessidade de informação de uma organização e na maneira pela qual isso pode ser organizado. A Segurança da Informação pode apoiar este processo, garantindo confidencialidade, integridade e disponibilidade da informação.

Informações e Processos Operacionais

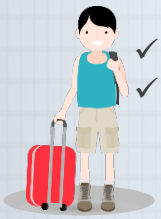
- Um Processo Operacional é o processo que está no núcleo do negócio;
- Em um processo operacional, as pessoas trabalham em um produto ou serviço para um cliente;
- Um processo operacional tem os seguintes componentes principais: Entrada, Atividades e Saída;
- Existem vários tipos de Processos Operacionais:
  - ✓ **Processo primário**
    Ex.: Fabricar uma bicicleta ou administrar o dinheiro.

  - ✓ **Processo Orientador**
    Ex.: Planejar a estratégia dos processos da empresa, apoiar as compras, as vendas ou o RH.

- Informação se tornou um importante fator de produção na realização dos Processos Operacionais.
- Um dos métodos para determinar o valor da informação é verificar o papel da informação nos vários Processos Operacionais.
- Cada Processo Operacional define requisitos específicos para o fornecimento de informações.
- Há processos que são muito dependentes da disponibilidade de informações.
  - ✓ **Ex.:** site da empresa.
- Outros processos são mais dependentes da precisão das informações.
  - ✓ **Ex.:** preços dos produtos.

Análise da Informação

- Análise da Informação fornece uma ideia clara de como uma organização lida com a informação - como a informação "flui" através da organização.
- Por exemplo:
  - ✓ Um hóspede faz uma reserva em um hotel através de seu Website;
  - ✓ Esta informação é passada para o departamento administrativo, que, em seguida, aloca um quarto;
  - ✓ A recepção sabe que o hóspede chegará hoje;
  - ✓ O departamento de limpeza sabe que o quarto deve estar limpo para a chegada do hóspede;



- Em todos esses passos, o mais importante é que a informação seja confiável.
- Os resultados de uma Análise da Informação podem ser usados para desenvolver um Sistema de Informação.

Gerenciamento de Informação

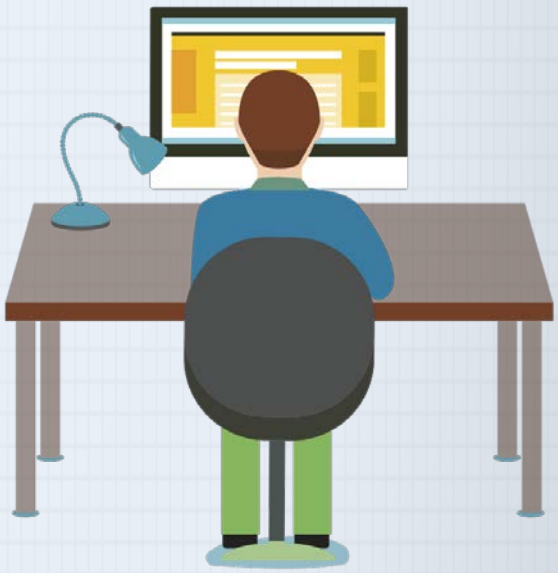
- O Gerenciamento de Informação define e dirige a Política relativa ao fornecimento de informação de uma organização.
- Dentro deste sistema, um Gerente de Informação pode fazer uso da Arquitetura da Informação e de uma Análise da Informação.
- O Gerenciamento de Informação envolve muito mais do que o processamento automatizado de informações realizado pela organização.
- Em muitos casos, a comunicação externa e a comunicação com a parte em forma de mídia da estratégia do Gerenciamento de Informação.

Informática

- O termo Informática está relacionado à ciência da lógica usada para trazer estrutura para informação e sistemas.
- É importante compreender que a informática pode ser usada para desenvolver programas.

O Que Aprendemos?

- As várias formas de Informação e Sistemas de Informação.
- O trio:
  - ✓ Confidencialidade;
  - ✓ Integridade;
  - ✓ Disponibilidade.
- Como a Segurança da Informação é importante para:
  - ✓ Os Processos Operacionais;
  - ✓ A Arquitetura da Informação;
  - ✓ Gerenciamento de Informação.



ISO 27002

Qual informação é valiosa na sua organização?

Exemplos de informação valiosa:

- Empregados (conhecimento e experiência);
- Produto ou serviço vendido;
- Dados pessoais de fornecedores, clientes e empregados;
- Processos internos;
- Manuais/receitas;
- Informações financeiras;
- Etc.

O Que uma Ameaça?

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

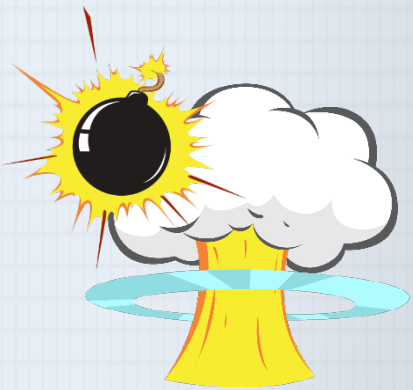
A causa potencial de um incidente indesejado que pode resultar em danos a um Sistema ou à Organização.

O termo "Ameaça" não está definido na ISO/IEC 27002:2013. Ao invés disso, o termo é definido no acompanhamento da norma ISO/IEC 27000:2012 Descrições e Vocabulário.

Ameaças e Medidas de Segurança da Informação

- No processo de Segurança da Informação, efeitos indesejados (Ameaças) são mapeados na medida do possível;
- A segurança da informação determina se algo deve ser feito para evitar tais efeitos;
- A Segurança da Informação determina quais medidas de segurança devem ser tomadas para evitá-los.

Riscos



Risco: combinação da probabilidade de um Evento ocorrer e sua Consequência.

ISO 27002

Risco - é o efeito da incerteza sobre os objetivos e é frequentemente caracterizado por referência a possíveis eventos e consequências, ou uma combinação dos dois.

O termo "Risco" não está definido na ISO/IEC 27002:2013. Ao invés disso, o termo é definido no acompanhamento da norma ISO/IEC 27000:2012 Descrições e Vocabulário.

Encontra-se abaixo a definição do acompanhamento da norma ISO/IEC 27000:2012:

2.61 risco: efeito da incerteza sobre os objetivos [Guia ISO 73:2009]

NOTA 1 - Um efeito é um desvio do esperado - positivo e/ou negativo.

NOTA 2 - Objetivos podem ter diferentes aspectos (tais como aspectos financeiros, de saúde e segurança, de segurança da informação e de metas ambientais) e podem ser aplicados em diferentes níveis (como estratégico, por toda a organização, por projeto, por produto e por processo).

NOTA 3 - Risco é muitas vezes caracterizado como uma referência a potenciais eventos (2.24) e consequências (2.15), ou uma combinação dos dois.

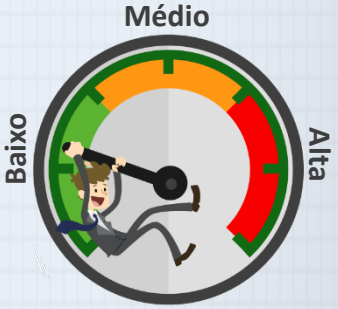
NOTA 4 - O risco da segurança da informação é muitas vezes expresso em termos de uma combinação das consequências de um evento de segurança da informação e da probabilidade associada (2.40) a uma ocorrência.

NOTA 5 - Incerteza é o estado, mesmo parcial, de deficiência de informações relacionadas à compreensão ou ao conhecimento de um evento, suas consequências ou probabilidades.

NOTA 6 - Riscos da segurança da informação estão associados ao potencial de exploração das vulnerabilidades de um ativo de informação ou grupo de ativos de informação pelas ameaças, e, assim, causar prejuízos à organização.

Análise de Risco

Análise de Risco: uma utilização sistemática de informações para identificar fontes e estimar o risco.



Análise de Risco

- Metodologia/processo para ajudar a adquirir uma visão/compreensão dos riscos que a

ISO 27002

Organização está enfrentando e que precisa se proteger.

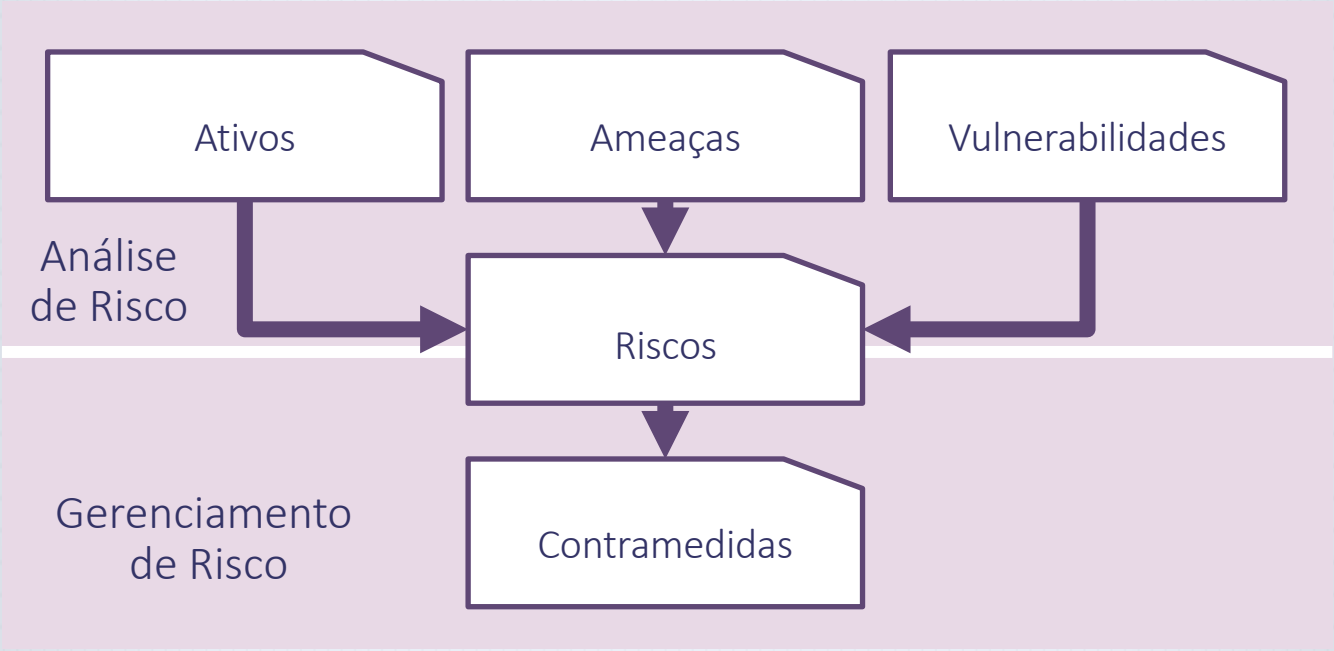
- Fornece a base para a avaliação de risco e para as decisões para lidar com o risco.
- Análise de risco inclui estimativas de risco.

Nota: os riscos possuem “donos” que também devem estar envolvidos na análise e avaliação de riscos.

O termo "Análise de Risco" não está definido na ISO/IEC 27002:2013. Ao invés disso, o termo é definido no acompanhamento da norma ISO/IEC 27000:2012 Descrições e Vocabulário.

Ameaças, Riscos e Análise de Risco

Melhores Práticas de acordo ITIL® e CRAMM.



Quando uma Ameaça se materializa, surge um Risco para a organização. Tanto a extensão do risco, quanto o gerenciamento de sua avaliação determinam se Medidas devem ser tomadas a fim de minimizar o Risco e o que ele pode se tornar.

ISO 27002

Avaliação de Risco

Melhores Práticas de acordo ITIL® e CRAMM.

- Avaliação de Risco deve incluir uma abordagem sistemática para estimar a magnitude dos Riscos (Análise de Risco) e o processo de comparar os Riscos estimados em relação aos critérios de Risco para determinar a significância dos Riscos (Estimativa de Risco).

- Avaliação de risco é a soma total de:
  - ✓ Avaliação e Apreciação de Ativo;
  - ✓ Avaliação e Apreciação de Ameaça;
  - ✓ Avaliação de Vulnerabilidade.

- Avaliação de Risco (ISO/IEC 27000:2012):
  - ✓ processo geral de identificação de risco, análise de risco e estimativa de risco.

Incidentes e Desastres de Segurança da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Incidente de Segurança da Informação:

- Quando uma ameaça se manifesta. Exemplo: Um hacker consegue invadir a rede da empresa.

Desastre de Segurança da Informação:

- Um ou mais incidentes ameaçam a continuidade de Segurança da Informação da empresa. Exemplo: Um ou mais hackers apagam ou destroem ativos críticos da segurança da informação, causando uma grande perda de acesso à informação.

Gerenciamento de Risco

Gerenciamento de Risco:

O processo de **Ameaças**

Para **Riscos**

Para **Medidas de Segurança**

ISO 27002

Análise de Risco

- Uma ferramenta para esclarecer quais Ameaças são relevantes para os Processos Operacionais e para identificar os Riscos associados. O nível de segurança adequado juntamente com as Medidas de Segurança associadas podem, desta forma, serem determinados.

Objetivos:

1. Para identificar Ativos e seus Valores;
2. Para determinar Vulnerabilidades e Ameaças;
3. Para determinar o Risco das Ameaças se tornarem realidade e interromperem o Processo Operacional
4. Para determinar o equilíbrio entre os custos de um incidente e os custos de uma Medida de Segurança.

Análise de Custo e Benefício

- Parte do processo de Análise de Risco da Segurança da Informação
- Questão:
  - ✓ Um servidor custa $100,000.-
  - ✓ As Medidas da Segurança da Informação para esse servidor custam $150,000.-
  - ✓ Conclusão: as Medidas da Segurança da Informação são muito caras...
  - ✓ Essa é uma conclusão Certa ou Errada?

Tipos de Análise de Risco

Análise Quantitativa de Risco:

- Tem o objetivo de calcular um Valor do Risco com base no nível do prejuízo financeiro e na probabilidade de que uma Ameaça possa se tornar um Incidente de Segurança da Informação;

- O Valor de cada elemento em todos os Processos Operacionais é determinado;

- Estes Valores podem ser compostos pelos custos das Medidas de Segurança da Informação, bem como o Valor da propriedade em si, incluindo itens como edifícios, hardware, software, informação e impacto nos negócios;
- O tempo se estende diante do surgimento de uma ameaça, a eficácia das Medidas de Segurança da Informação e o Risco de uma Vulnerabilidade ser explorada também são elementos a serem considerados;
- Uma Análise de Risco puramente quantitativa é praticamente impossível.

Análise Qualitativa de Risco:

- Baseia-se em cenários e situações;
- As chances de uma Ameaça se tornar realidade são analisadas com base em intuições;
- A análise, em seguida, examina o Processo Operacional cujo qual a Ameaça está relacionada e as Medidas de Segurança da Informação que já foram tomadas;
- Isso tudo leva a uma visão subjetiva das possíveis Ameaças;
- Medidas são posteriormente tomadas para minimizar o risco de Segurança da Informação;
- O melhor resultado é alcançado através da realização de análise em uma sessão em grupo, pois isso leva a um debate que evita que a visão de uma única pessoa ou de um único departamento domine a análise.

Tipos de Medidas de Segurança

Medidas Preventivas:
- ✓ Têm o objetivo de prever incidentes de Segurança.

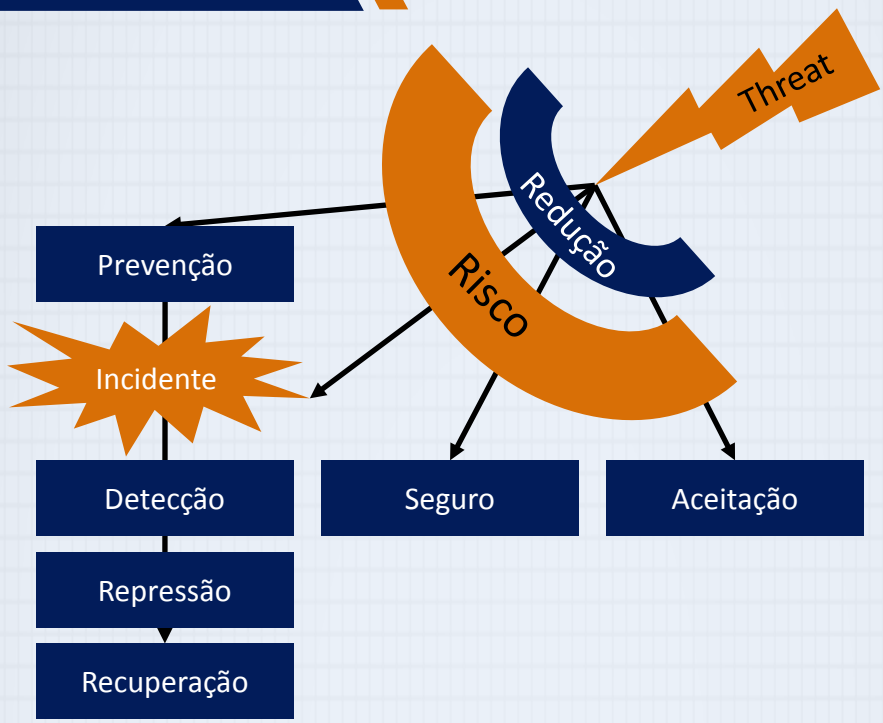
Medidas de Detecção:
- ✓ Têm o objetivo de detectar incidentes de Segurança.

Medidas Repressivas:
- ✓ Têm o objetivo de parar as consequências das Medidas Corretivas de Incidentes de Segurança.

Medidas Corretivas:
- ✓ Têm o objetivo de recuperar os danos causados por Incidentes de Segurança.

Seguro de Compra:
- ✓ Têm o objetivo de contratar seguro contra certos tipos de Incidentes de Segurança, porque a implementação de Medidas de Segurança pode ser cara .

ISO 27002



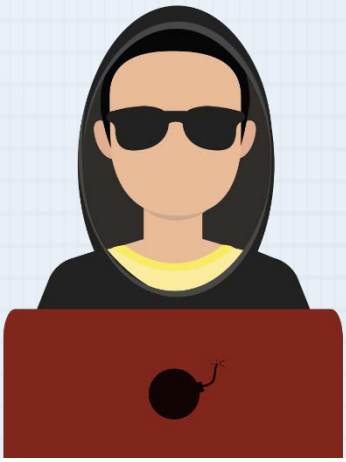
Tipos de Ameaças

Ameaças Humanas

- Intencional;
- Ações de hackers, Danos às propriedades, Destruição de e-mails após demissão;
- Não Intencional;
- Exclusão de dados não intencional
- Engenharia Social;
- Enganar as pessoas para fornecerem voluntariamente informações confidenciais: phishing.

Ameaças Não-humanas

- Raios;
- Incêndio;
- Enchente;
- Furacão;
- Tornado;
- Etc.



ISO 27002

Tipos de Dano

Dano Direto: Roubo.

Dano Indireto:

- Uma perda que pode ocorrer em consequência de outro evento.
  - ✓ Ex.: Devido a uma enchente que atingiu o datacenter, nenhum serviço de TI pode ser prestado, o que causa perda de receitas para o negócio.

Expectativa de Perda Anual (ALE):

- A quantidade de dano - expressa em termos monetários - que pode resultar de um incidente em um ano.
  - ✓ Ex.: Em média, 10 notebooks são roubados da empresa todos os anos.

Expectativa de Perda Única (SLE):

- Dano causado por um único incidente (pontual).

Tipos de Estratégias de Risco

Aceitabilidade de Risco:

- Certos riscos são aceitáveis;
- Medidas de segurança são muito caras;
- Medidas de segurança excedem possíveis danos;
- Medidas de segurança que foram tomadas são repressivas por natureza.

Risco Neutro:

- Os resultados das medidas de segurança tomadas são;
- A ameaça não existe mais;
- O dano resultante é minimizado
- As medidas de segurança tomadas são uma combinação de medidas preventivas, investigativas e repressivas.

Prevenção de Risco

- As medidas de segurança tomadas são de tal ordem que a ameaça é neutralizada a um grau que impede a ocorrência de um incidente. Ex .: A adição de um novo software que faz com que os erros no antigo software não sejam mais uma ameaça.
- As medidas de segurança que são tomadas são preventivas por natureza.

ISO 27002

Tratando Riscos de Segurança

Possíveis opções para o tratamento de Risco incluem:

a) Aplicação de controles apropriados para reduzir os Riscos;
b) Aceitar de forma consciente e objetiva os Riscos desde que eles claramente satisfaçam a Política e os critérios da Organização para Aceitação de Risco;
c) Evitar Riscos ao não permitir ações que fariam os Riscos ocorrerem;
d) Transferência dos Riscos associados a outras partes, por exemplo, Seguradoras ou Fornecedores.

Seleção de controles .... A seleção de controles é dependente de decisões organizacionais baseadas nos critérios de aceitação de risco, nas opções de tratamento de risco e na abordagem de gerenciamento de risco aplicadas à organização e também deve estar sujeita a todas as leis e regulamentos nacionais e internacionais pertinentes...

O trecho a seguir foi extraído da ISO/IEC 27002:2013:

Os controles podem ser selecionados a partir desta norma ou de outros conjuntos de controles, ou novos controles podem ser desenvolvidos para atender necessidades específicas, conforme necessário.

ISO/IEC 27002
Specification

A seleção de controles é dependente de decisões organizacionais baseadas nos critérios de aceitação de risco, nas opções de tratamento de risco e na abordagem de gerenciamento de risco aplicadas à organização, e também deve estar sujeita a todas as leis e regulamentos nacionais e internacionais pertinentes. A seleção de controles também depende da forma que os controles interagem para fornecer uma defesa profunda. Alguns dos controles nesta norma podem ser considerados como princípios que orientam a gestão da segurança da informação e são aplicáveis à maioria das organizações. Os controles são explicados em mais detalhe abaixo, juntamente com diretrizes de aplicação. Mais informações sobre a seleção de controles e outras opções de tratamento de risco podem ser encontradas em ISO/IEC 27005.

Os controles devem assegurar que os Riscos sejam reduzidos a um nível aceitável levando em conta:

a) Requisitos e restrições da legislação e regulamentação Nacional e Internacional;
b) Objetivos da organização;
c) Requisitos e restrições operacionais;
d) Custo de implantação e operação em relação aos Riscos que estão sendo reduzidos, e permanecendo proporcional às exigências e restrições da organização;
e) Necessidade de equilibrar o investimento da implementação e operação dos controles em relação aos danos que podem resultar de falhas de segurança.

ISO 27002

O que aprendemos?

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- **Termos:**
  - ✓ Ameaças;
  - ✓ Riscos;
  - ✓ Medidas de Segurança;
  - ✓ Análise de Risco;
  - ✓ Avaliação de Risco.
- **Tipos de Análises de Risco;**
- **Vários tipos de Ameaças e como lidar com elas;**
- **Vários tipos de danos;**
- **Estratégias de Risco que possuímos disponíveis;**
- **Medidas de Segurança que podem ser implementadas.**

Política de Segurança da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Orientação de gerenciamento para segurança da informação.

Objetivo:

- Fornecer orientação e suporte de gerenciamento para Segurança da Informação de acordo com os requisitos do Negócio, leis e regulamentos pertinentes.

ISO/IEC 27002 Specification

Conteúdo:

- As políticas de segurança da informação.

Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Gerência, publicado e comunicado aos empregados e partes externas relevantes.

Revisão das políticas de segurança da informação:

- As políticas de segurança da informação devem ser revisadas em intervalos planejados ou quando ocorrerem mudanças significativas para assegurar a sua contínua pertinência, adequação e eficácia.

- Através de uma Política de Segurança da Informação, a Gerência fornece direcionamento e suporte à organização.

- Esta Política deve ser escrita de acordo com os requisitos do Negócio, bem como de acordo com a legislação e regulamentos relevantes.

ISO 27002

- A Política de Segurança da Informação deve ser aprovada pelo Conselho Administrativo e publicada para todos os empregados e partes externas relevantes, tais como clientes e fornecedores;

- Publicando a Política.

✓ Crie uma versão resumida da Política com os pontos principais.
✓ Isso pode ser feito na forma de um panfleto para todos os funcionários e incluído como parte do kit introdutório aos novos empregados.
✓ A versão completa pode ser publicada na Intranet da empresa ou em algum outro local que seja de fácil acesso a todos os funcionários.

Conteúdos

Regulamentos:
- Um regulamento é mais detalhado do que um documento de política.

Procedimentos:
- Descreve em detalhes como certas medidas devem ser implementadas, e pode, às vezes, incluir instruções de trabalho.

Diretrizes:
- Fornecer orientação:
  - ✓ Descreve quais aspectos precisam ser examinados através de aspectos de segurança específicos;
  - ✓ Diretrizes não são obrigatórias, mas possuem natureza consultiva.

Normas:
- Por exemplo: conjunto de normas de plataformas específicas.

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.

- O objetivo geral da Segurança de TI é "Segurança equilibrada com profundidade", com controles justificáveis implementados para assegurar que a Política de Segurança da Informação está sendo aplicada e que os Serviços de TI que estão dentro dos parâmetros de segurança (isto é, Confidencialidade, Integridade e Disponibilidade) continuem a operar.

- Para muitas organizações, a abordagem em relação a Segurança de TI é feita através de uma Política de Segurança da Informação que é propriedade da Gestão da Segurança da Informação e mantida pela mesma.

ISO 27002

- Na execução da Política de Segurança, o Gerenciamento de Disponibilidade desempenha um papel importante na sua operação para os novos Serviços de TI.

- O objetivo geral da Segurança de TI é "Segurança equilibrada com profundidade", com controles justificáveis implementados para assegurar que a Política de Segurança da Informação está sendo aplicada e que os Serviços de TI que estão dentro dos parâmetros de segurança (isto é, Confidencialidade, Integridade e Disponibilidade) continuem a operar.

- Para muitas organizações, a abordagem em relação a Segurança de TI é feita através de uma Política de Segurança da Informação que é propriedade da Gestão da Segurança da Informação e mantida pela mesma.

- Na execução da Política de Segurança, o Gerenciamento de Disponibilidade desempenha um papel importante na sua operação para os novos Serviços de TI.

- O processo de Gestão da Segurança da Informação (GSI) deve ser o ponto focal para todas as questões de Segurança de TI, e deve garantir que uma Política de Segurança da Informação seja criada, mantida e reforçada, cobrindo usos e abusos de todos os sistemas e serviços de TI.

- **A GSI precisa entender todo o ambiente de Segurança de TI e de Negócio, incluindo:**
  - ✓ Política e planos de Segurança de Negócios;
  - ✓ Operação de negócios atual e seus requisitos de Segurança;
  - ✓ Planos de negócios futuros e requisitos;
  - ✓ Requisitos legislativos;
  - ✓ Obrigações e responsabilidades em relação à Segurança para os ANSs;;
  - ✓ Os Riscos do Negócio e do TI e sua gestão.

- **A Política de Segurança da Informação consiste em:**
  - ✓ Política geral de Segurança da Informação;
  - ✓ Política para usos e abusos dos ativos de TI;
  - ✓ Política de controle de acesso;
  - ✓ Política de controle de senha;
  - ✓ Política de e-mail;
  - ✓ Política de uso da internet;
  - ✓ Política antivírus;
  - ✓ Política de classificação da informação;
  - ✓ Política de classificação de documentos;
  - ✓ Política de acesso remoto;

ISO 27002

- ✓ Política sobre o acesso dos fornecedores aos Serviços de TI, informações e componentes;
- ✓ Política de alienação de bens.

Organização da Segurança da Informação

ISO/IEC 27002 Specification

Objetivos da Organização Interna:

- **Organização interna:**
  - ✓ Estabelecer uma estrutura de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

- **Dispositivos móveis e trabalho remoto:**
  - ✓ Garantir a segurança do trabalho remoto e no uso dos dispositivos móveis.

Conteúdo da organização interna:

- **Funções e responsabilidades da segurança da informação:**
  - ✓ Todas as responsabilidades da segurança da informação devem ser definidas e alocadas.

- **Segregação de funções:**
  - ✓ Funções e áreas de responsabilidade contraditórias devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido de ativos da organização.

- **Contato com autoridades:**
  - ✓ Devem ser mantidos contatos adequados com autoridades relevantes.

- **Contato com grupos de interesses específicos:**
  - ✓ Contato adequado com grupos de interesses específicos ou com fóruns e outros profissionais especialistas em segurança.
  - ✓ Associações devem ser mantidas.

Segurança da informação no gerenciamento de projetos:

- A segurança da informação deve ser abordada no gerenciamento de projetos, independentemente do tipo de projeto.

Política do dispositivo móvel:

- Uma política e medidas de segurança de suporte devem ser adotadas para gerenciar os riscos relacionados ao uso de dispositivos móveis.

ISO 27002

Trabalho remoto:
Uma política e medidas de segurança de suporte devem ser implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

Conteúdo:
- Sem uma Segurança da Informação eficaz, não é possível que uma organização sobreviva;
- Todos na organização devem aceitar isso. O conselho administrativo e a gerência devem agir de forma exemplar;
- Apenas quando a gerência apoia a própria Política é que os empregados levam a sério a Segurança da Informação e procuram cumprir as medidas;
- Segurança da Informação é um Processo que muitas pessoas estão envolvidas;
- O processo precisa ser controlado de forma eficaz;
- Se não há nenhuma responsabilidade ou gestão, então, a Segurança da Informação não será eficaz;
- A maneira pela qual a Segurança da Informação é gerida depende da natureza e do tamanho da organização;
- Em pequenas organizações, a Segurança da Informação pode ser apenas uma das responsabilidades de várias pessoas;
- Uma pessoa autônoma sem nenhum empregado é responsável por todos os aspectos de TI, incluindo a Segurança;
- Em grandes organizações, haverá pessoas cuja única responsabilidade é um aspecto particular da Segurança da Informação;
- No processo de Segurança da informação, consultas periódicas precisam ocorrer entre todos aqueles com responsabilidade primária;
- Além dos agentes de segurança da informação, estes também podem ser pessoas que são responsáveis pela execução de determinadas medidas;
- Normalmente, essas pessoas trabalham nos departamentos de Recursos Humanos, Informação, Finanças, Contabilidade ou Acomodação.

Funções

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

As funções de Segurança da Informação podem ter nomes diferentes, mas, em geral, se resumem às seguintes posições:
- O **Chief Information Security Officer (CISO)** é o mais alto nível da gestão da organização e desenvolve a estratégia geral para todo o negócio;
- O **Diretor de Segurança da Informação (DSI)** desenvolve a política da unidade de negócios com base na política da empresa e garante o seu cumprimento;
- O **Gerente de Segurança da Informação (GSI)** desenvolve a política de segurança da informação dentro da organização de TI e garante o seu cumprimento;

- Além dessas funções que são especificamente voltadas para a segurança da informação, a organização pode ter um **Diretor de Política de Segurança da Informação** ou um **Diretor de Proteção de Dados.**

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.

O Gerente de Segurança

O Gerente de Segurança é responsável por assegurar que os objetivos da Gestão da Segurança da Informação sejam atendidos, tais como:

- Desenvolver e manter a Política de Segurança da Informação;
- Comunicar e divulgar a Política de Segurança da Informação;
- Garantir que a Política de Segurança da Informação seja aplicada e cumprida;
- Identificar e classificar os ativos de TI e de informação, e o nível de controle e proteção exigido;
- Ajudar com Análises de Impacto nos Negócios;
- Realizar Análise de Risco de Segurança e gestão de risco;
- Criar controles de segurança e desenvolver planos de segurança;
- Desenvolver e documentar os procedimentos para operar e manter os controles de segurança;
- Monitorar e gerenciar todas as violações de segurança e lidar com incidentes de segurança;
- Relatórios, análises e redução do impacto e dos volumes de todos os incidentes de segurança;
- Promover educação e conscientização de segurança;
- Manter um conjunto de controles de segurança e documentação, e regularmente rever e auditar os controles e processos;
- Garantir que todas as alterações sejam avaliadas em relação a seus impactos em todos os aspectos de segurança, incluindo os controles de Política de Segurança e a segurança da informação, e participação em reuniões CAB quando for apropriado;
- Realizar testes de segurança;
- Participar em quaisquer revisões de segurança decorrentes de violações de segurança e ações corretivas;
- Assegurar que a confidencialidade, integridade e disponibilidade dos serviços sejam mantidas nos níveis acordados ANSs e que estejam em conformidade com todos os requisitos legais aplicáveis;
- Garantir que todo o acesso aos serviços por parceiros externos e fornecedores esteja sujeito às obrigações e responsabilidade contratuais;
- Atuando como um ponto focal para todas as questões de segurança.

Segurança do Recursos Humanos

ISO/IEC 27002 Specification

Objetivos:

- Antes do emprego - Para garantir que empregados e empregadores compreendessem suas

responsabilidades e fossem adequados às funções para as quais cada um era considerado.

- Durante o emprego - Para garantir que os empregados e os empregadores estejam cientes e cumpram com suas responsabilidades de segurança da informação.

- Rescisão e mudança de emprego - Para proteger os interesses da organização como parte do processo de alteração ou fim de emprego.

Conteúdo:

- **Verificação de antepassados –** verificam-se todos os candidatos à vaga de emprego e isso deve ser realizado em conformidade com as leis, regulamentos e ética relevantes e deve ser proporcional aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos.

- **Termos e condições de contratação** – os acordos contratuais entre empregados e empregadores devem indicar as responsabilidades em relação à segurança da informação para ambas as partes.

- **Responsabilidades da gerência** – a gerência deve exigir que todos os empregados apliquem segurança da informação em conformidade com as políticas e procedimentos estabelecidos pela organização.

- **Consciência, educação e treinamento de segurança da informação** - Todos os empregados da organização e, quando pertinente, empregadores devem receber educação de conscientização adequada, treinamento e atualizações regulares sobre políticas e procedimentos organizacionais relevantes para as funções.

- **Processo disciplinar** - Deve haver um processo disciplinar formal e que seja comunicado de forma adequada que irá ser usado para tomar medidas em relação aos empregados que tenham cometido alguma violação de segurança da informação.

- **Rescisão ou mudança de responsabilidades do emprego** – Responsabilidades e funções da segurança da informação que permanecem válidos após a rescisão ou mudança de emprego devem ser definidos, comunicados ao empregado ou empregador, e executados.

ISO 27002

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Todos os empregados são responsáveis pela segurança da informação. Esta responsabilidade deve ficar clara no contrato de trabalho.
- O manual dos empregados deve conter um código de conduta e sanções que são impostas para o caso de descumprimento do mesmo e se incidentes surgirem como consequência. O código de conduta pode indicar, por exemplo, que o uso privado dos e-mails privados não é permitido.
- O gerente é responsável pelas descrições de trabalho corretas e é, portanto, também responsável pelos vários aspectos relacionados à forma como se deve lidar com a informação em várias posições distintas
- Para uma posição que envolve confidencialidade, esta característica pode ter que ser observada mesmo após o término do trabalho. O gerente é responsável por documentar regras especiais para posições específicas. Em todos os casos, todos os funcionários com uma posição que envolva confidencialidade devem assinar um Acordo de Confidencialidade (NDA).
- Também é normal que os empregados precisem apresentar um atestado de bons antecedentes.

Código de Conduta

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- **O Manual do Funcionário deve conter um Código de Conduta e as sanções que serão impostas no caso de descumprimento do mesmo e se Incidentes de Segurança surgirem como consequência.**
- **O Código de Conduta pode indicar:**
  - ✓ Que e-mails pessoais não são permitidos;
  - ✓ Que os registros de empregados podem conter informações como o perfil de trabalho, contrato de trabalho e vários acordos assinados;
  - ✓ Que para o uso de e-mail, se declara ter ciência e intenção de se cumprir a legislação (por exemplo, na área de proteção de dados e cibercrimes), bem como adesão ao Acordo de Confidencialidade;
  - ✓ Uma campanha conscientizar os empregados sobre ameaças à segurança, tais como malware, phishing e spams;

- ✓ Que as 3 partes irão cumprir os requisitos de segurança da informação;
- ✓ Que seja autorizado usar telefone, e-mail e internet para fins pessoais, desde que o trabalho não sofra como resultado. Download de música, filmes, software e visitar sites de cunho sexual são expressamente proibidos.

Propriedade

ISO/IEC 27002 Specification

Política do dispositivo móvel...

Guia de implementação

Sempre que a política de dispositivo móvel permite o uso de dispositivos móveis particulares, a política e medidas de segurança associadas também devem considerar:

a) separação de uso privado e uso corporativo dos dispositivos, incluindo o uso de software para suportar essa separação e para proteger os dados do negócio em um dispositivo particular;

b) fornecer acesso às informações do negócio apenas após os usuários assinarem um acordo reconhecendo suas funções (proteção física, atualização de software e etc.), renunciando a propriedade sobre os dados do negócio, permitindo a limpeza remota de dados pela organização em caso de roubo, perda do dispositivo ou quando o usuário não for mais autorizado a utilizar o serviço. Esta política tem de levar em conta a legislação de privacidade vigente.

Inventário de ativos

Guia de implementação

- .... Para cada um dos ativos identificados, deve ser atribuída a propriedade do ativo e a classificação deve ser identificada ....

Propriedade de ativos

Controle

- Ativos mantidos no inventário devem ter propriedade.

Guia de implementação

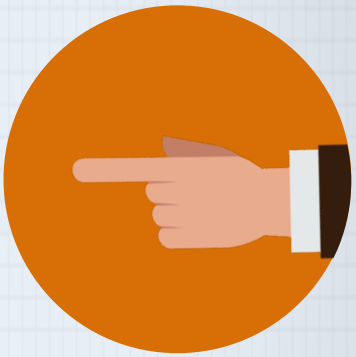
- Um processo para garantir a atribuição em tempo de propriedade de ativos é normalmente implementado. Propriedade deve ser atribuída quando os ativos são criados ou quando os ativos são transferidos para a organização. O proprietário do ativo deve ser responsável por sua gestão adequada durante todo o ciclo de vida do ativo.

ISO 27002

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Os Ativos do Negócio devem ser classificados de forma que seja possível definir níveis de segurança a eles. Isto é de responsabilidade do proprietário;

- Cada Ativo deve ter um Proprietário e isso deve estar registado;



- A informação que é registrada sobre o Ativo do Negócio é:
  - ✓ Tipo de ativo
  - ✓ Proprietário
  - ✓ Localização
  - ✓ Formato
  - ✓ Classificação
  - ✓ Valor para o negócio

- O Proprietário é a pessoa responsável por um Processo do Negócio, Sub-processo ou Atividade do Negócio e deve cuidar de todos os aspectos do Ativo do Negócio, incluindo Segurança, gestão, produção e desenvolvimento.

- O Proprietário é a pessoa que está responsável pelo Ativo do Negócio. Uma pasta na rede, por exemplo, pode ter um dono. Se alguém deseja ter acesso a essa pasta, o dono precisa fornecer a permissão.

- Com notebooks, o Usuário é normalmente registrado como o Proprietário.

- O Proprietário de um Ativo do Negócio atribui um nível adequado de acordo com uma lista de classificações. A classificação:
  - ✓ Indica o nível de segurança necessário. Isso é determinado em parte pela sensibilidade, valor, requisitos legais e importância para a organização;
  - ✓ Está de acordo com a maneira pela qual o bem da empresa é utilizado no negócio. O proprietário deve garantir que o ativo do negócio seja reclassificado se necessário;
  - ✓ Só pode ser rebaixada pelo Proprietário.

- Se um ativo tem uma classificação, é dada uma marca ou etiqueta a ele. Isto pode ser colocado de forma física e visível.

- O Proprietário determina quem tem acesso aos Ativos do Negócio específicos.

- A classificação de um Ativo do Negócio também determina como ele pode ser armazenado fisicamente.

- O Proprietário de Dados, geralmente um gerente, é a pessoa que permite o acesso durante o processo de autorização. Esta autorização pode ser processada automaticamente pelo software, ou pode ser concedida pelo gestor de sistema/aplicativos;

Incidentes da Segurança da Informação

Um incidente da Segurança da Informação é indicado por um único ou uma série de eventos indesejados ou inesperados de Segurança da Informação que possuem uma probabilidade significativa de comprometer a operação do negócio e ameaçam a Segurança da Informação

Gestão de Incidentes da Segurança da Informação

Objetivo:

- Gerenciamento de incidentes da segurança da informação e melhorias:
  - ✓ Garantir uma abordagem coerente e eficaz para a gestão de incidentes da informação da segurança, incluindo comunicação em eventos de segurança e fraquezas.

Incidentes de Segurança: Exemplos

- controle de segurança ineficaz;
- violação das expectativas de integridade, confidencialidade ou disponibilidade da informação;
- erros humanos;
- não conformidades com as políticas e diretrizes;
- violação de medidas de segurança física;
- alterações descontroladas do sistema;
- mau funcionamento de software ou hardware;
- violações de acesso.

Relatórios de Incidentes de Segurança

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Um relatório de Incidente deve, no mínimo, permitir que as seguintes informações possam ser introduzidas:

- Data e horário;
- Nome da pessoa que elaborou o relatório;
- Localização (onde é o incidente?);
- Qual é o problema? (descrição do incidente: incidente com vírus, roubo, invasão, perda de

dados, etc.)

- Qual é o efeito do incidente? Como foi descoberto?

Consequências de NÃO relatar incidentes

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Empregados, funcionários temporários e usuários externos devem todos estar cientes dos procedimentos de comunicação de vários tipos de incidentes e das fraquezas que podem ter uma influência na Confiabilidade das Informações e da Segurança dos Ativos do Negócio.

- Eles devem ser obrigados a comunicar todos os incidentes e fraquezas o mais rápido possível para o Service Desk ou para uma pessoa específica.

- Duas questões são de grande importância e precisam ser esclarecidas pela gerência:
  - ✓ Relatar Incidentes de Segurança é essencialmente uma forma de aprender com eles para evitar que incidentes similares ocorram novamente;
  - ✓ Relatar um Incidente não deve ter o intuito de punir o autor do Incidente.

- No entanto, se um empregado sabotou intencionalmente um Sistema de Informação, vazou informações ou causou danos aos ativos da empresa, o incidente deve ser comunicado à polícia.

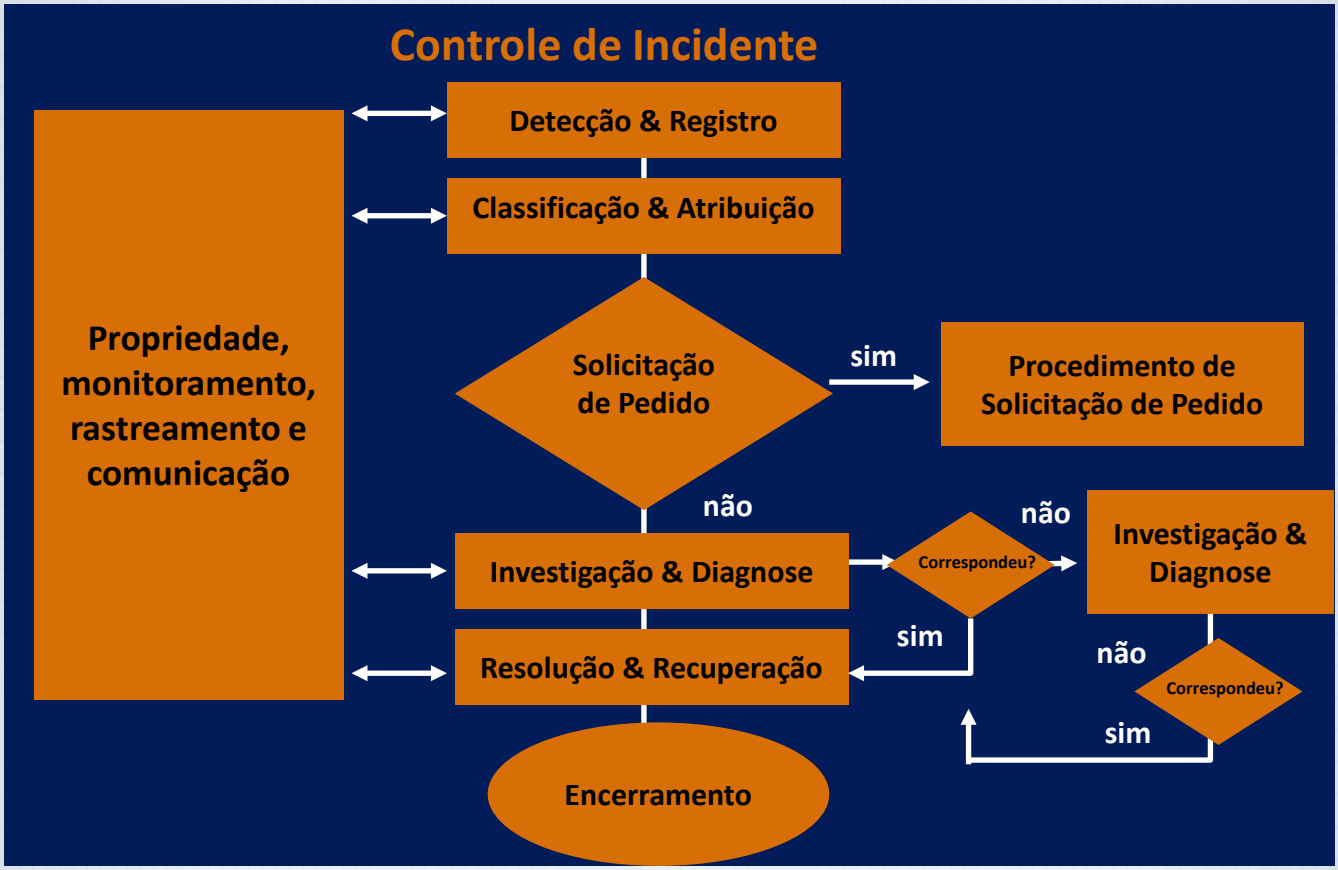
- É importante que as pessoas não tenham medo de relatar um incidente temendo pela resposta da Gerência ou por não quererem ser vistas como “dedo-duro”.

- O processo deve também assegurar que a pessoa que relatou um Incidente de Segurança da Informação seja informada das medidas e seus resultados posteriores.

ISO 27002

Processo de Gestão de Incidente Genérico

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.



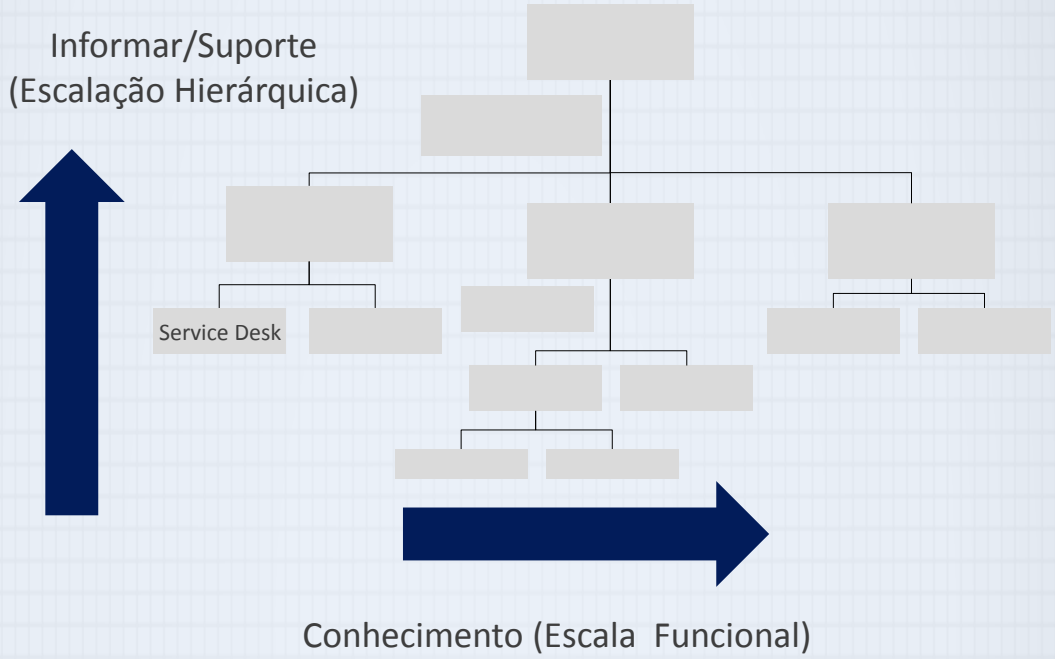
- Observe que propriedade, monitoramento, rastreamento e comunicação são todos realizados pelo Service Desk. O Service Desk é o proprietário do incidente, mas isso não implica que o Service Desk seja responsável por ele. Há uma grande diferença entre propriedade e responsabilidade. Por exemplo, quando o Suporte de Segunda Linha assume a questão do Suporte de Primeira Linha (o Service Desk) para trabalhar em uma resolução, a propriedade do incidente ainda reside com o Service Desk, mas a responsabilidade passou do Suporte de Primeira Linha para o Suporte de Segunda Linha.

- Observe que existem várias atividades neste fluxo de processo que podem ocorrer mais de uma vez. Por exemplo, as atividades de Investigação & Diagnose podem ser realizadas no Suporte de Primeira, Segunda e Terceira Linha para apenas o mesmo incidente. Este passo do processo é, por conseguinte, iterativo.

ISO 27002

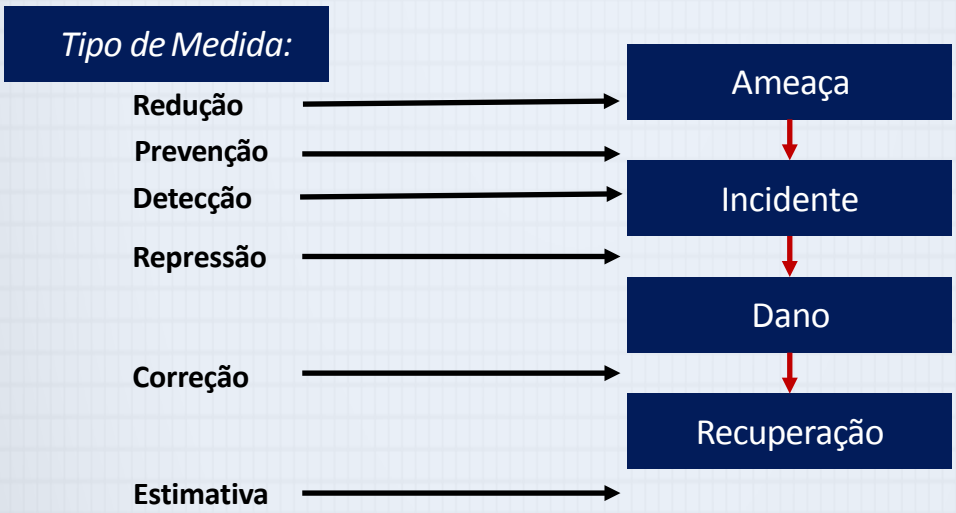
Tipos de Escalação de Incidentes

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação e ITIL®.



Ciclo do Incidente

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.



ISO 27002

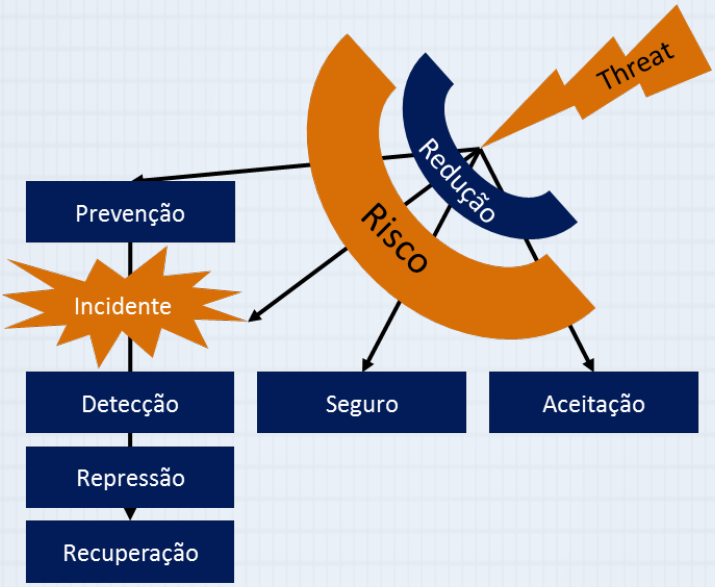
O que aprendemos?

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Os objetivos e o conteúdo da Política de Segurança da Informação;
- Os objetivos e o conteúdo da Organização de Segurança da Informação;
- O Código de Conduta, Propriedade, Funções e Responsabilidades com relação à Segurança da informação;
- A gestão de Incidentes de Segurança da Informação.

Tipos de Medidas de Segurança

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.



- **Medidas Preventivas**

✓ Têm o objetivo de prevenir Incidentes de Segurança.

- **Medidas de Detecção**

✓ Têm o objetivo de detectar Incidentes de Segurança

- **Medidas Repressivas**

✓ Têm o objetivo de deter as consequências dos Incidentes de Segurança.

- **Medidas Corretivas**

✓ Têm o objetivo de recuperar os danos causados por Incidentes de Segurança.

- **Compra de Seguro**

✓ Têm o objetivo de comprar um seguro contra certos Incidentes de Segurança, pois a aplicação de Medidas de Segurança pode ser cara.

ISO 27002

Medidas Preventivas

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Medidas Preventivas
Têm o objetivo de prever Incidentes de Segurança.

Exemplos:
- Cortar a conexão com a internet;
- Uma porta a prova de balas na sala de controle;
- Colocar informações confidenciais em um cofre.

Medidas de Detecção
Têm o objetivo de detectar Incidentes de Segurança.

Exemplos:
- Monitoramento por vídeo com adesivos para informar às pessoas que estão sendo filmadas;
- Informas às pessoas que o uso da internet é monitorizado irá dissuadir muitos empregados a terem atividades de navegação impróprias.

Medidas Repressivas
Têm o objetivo de deter as consequências dos Incidentes de Segurança.

Exemplos:
- Apagar um pequeno incêndio;
- Fazer backup.

Medidas Corretivas
Têm o objetivo de recuperar os danos causados por Incidentes de Segurança.

Exemplos:
- Um banco de dados foi excluído de forma não intencional. A idade do backup deste banco de dados irá determinar o quanto de esforço será feito na recuperação destes dados.

Compra de Seguro
Têm o objetivo de comprar um seguro contra certos Incidentes de Segurança, pois a aplicação de Medidas de Segurança pode ser cara.

Exemplos:
- Seguro contra incêndios;
- Colocar cópias de informações importantes em locais diferentes.

ISO 27002

Riscos e Medidas de Segurança

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Gerenciamento de Risco:

O processo de **Ameaças**

Para **Riscos**

Para **Medidas de Segurança**

Análise de Risco

Uma ferramenta para esclarecer quais Ameaças são relevantes para os Processos Operacionais e para identificar os Riscos associados. O nível de segurança adequado, juntamente com as Medidas de Segurança associadas, podem ser determinados.

Classificação de Informação

ISO/IEC 27002 Specification

Objetivo de assegurar que a informação receba um nível adequado de proteção de acordo com a sua importância para a organização.

Conteúdo

Classificação das informações deve ser classificada em termos de requisitos legais, valor, criticidade e sensibilidade à divulgação ou modificação não autorizada.

Rotulando a informação - Um conjunto apropriado de procedimentos para a rotulagem de informações deve ser desenvolvido e implementado de acordo com o esquema de classificação de informação adotado pela organização.

Manipulação de ativos - Os procedimentos para lidar com os ativos devem ser desenvolvidos e implementados de acordo com o esquema de classificação de informação adotado pela organização.

Classificação de Informações na Prática

- A classificação dada à informação é uma maneira rápida de determinar como esta informação será tratada e protegida;

- Para cada nível de classificação, os procedimentos de manipulação com segurança, incluindo o processamento, armazenamento, transmissão, desclassificação, e destruição, devem ser definidos. Isto também deve incluir os procedimentos para a cadeia de custódia e registro de qualquer evento relevante de segurança;

- A rotulagem e o manuseio seguro de informações classificadas é um requisito fundamental para arranjos de compartilhamento de informação;

- Etiquetas físicas é uma forma comum de rotulagem;

- No entanto, documentos eletrônicos requerem um meio eletrônico de rotulagem, como, por exemplo, uma mensagem de notificação na tela.

Segurança Física

Áreas Seguras

Objetivo:
Evitar acesso físico não autorizado, danos e interferências na informação da organização e nas suas instalações de processamento de informação.

Controles completos:

- O perímetro de segurança física Perímetros de segurança devem ser definidos e utilizados para proteger áreas que contêm informações críticas ou sensíveis, ou instalações de processamento de informações.

- Controle de entrada física As áreas seguras devem ser protegidas por controle de entrada adequado para garantir que somente pessoas autorizadas as acessem.
- Proteção para escritórios, quartos e instalações Segurança física para escritórios, quartos e instalações devem ser desenvolvidas e aplicadas.

- Proteção contra ameaças externas e ambientais Proteção física contra desastres naturais, ataques maliciosos ou acidentes deve ser desenvolvida e aplicada.

- Trabalho nas áreas seguras Procedimentos para o trabalho em áreas seguras devem ser desenvolvidos e aplicados.

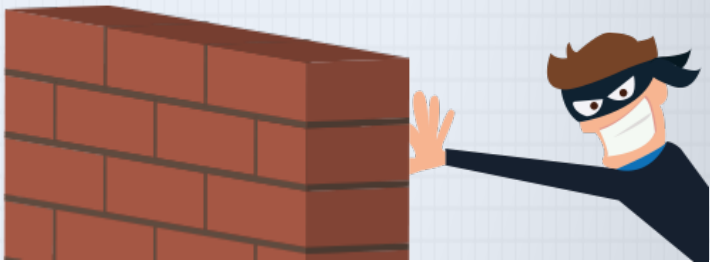
- Áreas de entrega e carregamento Áreas de acesso, tais como áreas de entrega e de carregamento, devem ser controlados e, se possível, isolados das instalações de processamento de informações para evitar o acesso de pessoas não autorizadas.
    - ✓ Trabalho nas áreas seguras. Áreas de acesso público, de entrega e de carregamento.

ISO 27002

Equipamento
Objetivo: Evitar perda, dano, roubo ou comprometimento de ativos e interrupção das operações da organização.

Descrições de controle total:

- Proteção e armazenamento dos equipamentos: Os equipamentos devem ser armazenados e protegidos de forma correta.
- Utilitários de suporte: Equipamentos devem ser protegidos contra falhas de energia e outras interrupções causadas por falhas nos utilitários de suporte.
- Segurança de cabeamento: Cabos de energia e telecomunicações transportam dados ou serviços de informação e devem ser protegidos contra interceptação, interferência ou danos.
- Manutenção dos equipamentos: Deve ser realizada a manutenção dos equipamentos de forma correta para garantir disponibilidade e integridade dos mesmos.
- Remoção de ativos: Equipamentos, informações ou softwares não devem ser retirados do local sem autorização prévia.
- Segurança dos equipamentos e ativos fora das premissas: Deve-se aplicar segurança aos ativos fora das premissas, levando em conta os diferentes riscos de trabalhar fora das dependências da organização.
- Alienação ou reuso seguro: Todos os itens que contenham armazenamento de mídia devem ser verificados para garantir que quaisquer dados sensíveis e softwares licenciados tenham sido devidamente removidos ou substituídos antes de serem alienados ou reutilizados.
- Usuários: Os usuários devem se certificar de que seus equipamentos tenham a proteção adequada.
- Política de mesa e tela limpas: Uma política de mesa limpa para papéis, dispositivos portáteis de armazenamento de mídia (ex.: pendrive) e uma política de tela limpa devem ser adotadas para as instalações de processamento de informações.



ISO 27002

Medidas de Segurança Física

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Segurança Física emprega uma combinação de medidas organizacionais, estruturais e eletrônicas;
- Medidas de Segurança Física precisam ser planejadas e coordenadas de forma coerente.

Exemplos:

- Proteção dos equipamentos através do controle de temperatura (ar condicionado, umidade);
- Cabos devem ser instalados de tal forma que evitem interferências. A interferência ocorre quando os cabos captam ruídos e estática dos cabos de energia que estão próximos;
- A exclusão de Informação Confidencial na mídia de armazenamento quando uma pessoa deixa a organização.

Medidas de Segurança Física

Categorias:

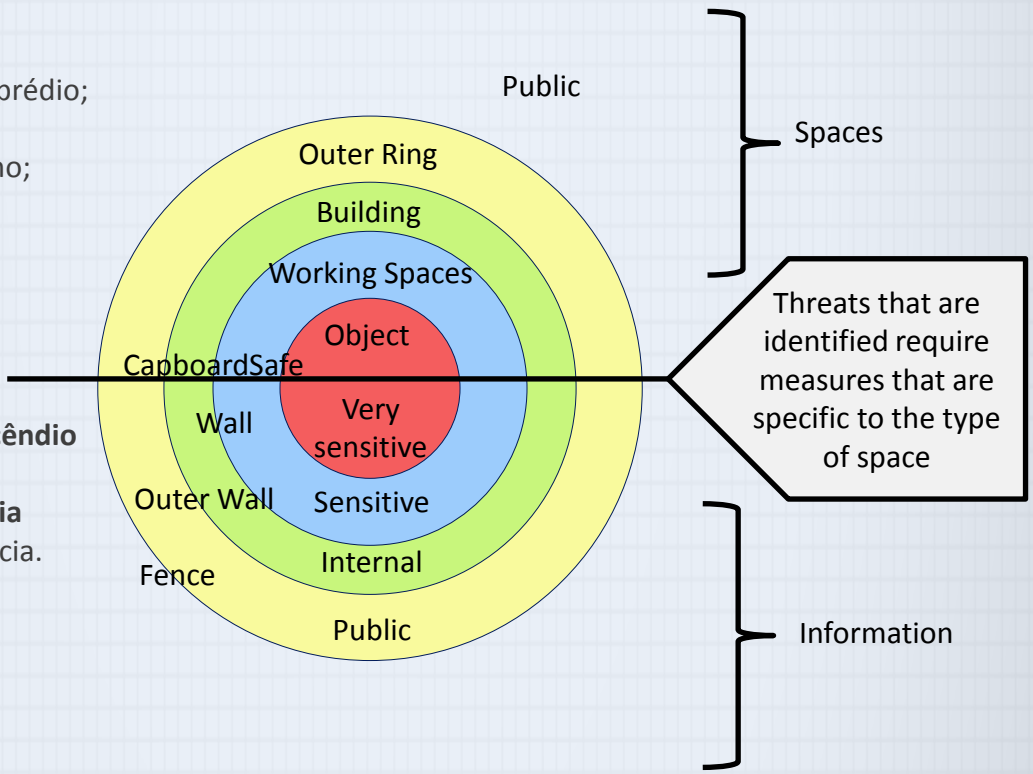
- Anéis de Proteção;
- A área ao redor do prédio;
- O edifício;
- O espaço de trabalho;
- Os objetos.

Alarmes

- Sensores;
- Monitoramento.

- **Proteção contra incêndio**

- **Plano de Emergência**
- Plano de Contingência.



ISO 27002

Segurança Técnica

Controle de Acesso

- Requisitos da organização de controle de acesso Objetivo: limitar o acesso à informação e às instalações de processamento de informação.
- Gerenciamento de acesso do usuário Objetivo: assegurar o acesso do usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.
- Responsabilidades dos usuários Objetivo: tornar os usuários responsáveis pela proteção de suas informações de autenticação.
- Controle de acesso a aplicativos e sistemas Objetivo: impedir o acesso não autorizado a sistemas e aplicativos.

Criptografia

- Controles de criptografia Objetivo: garantir o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e/ou integridade das informações.

Conteúdo:

- Política de controle de acesso Uma política de controle de acesso deve ser estabelecida, documentada e revisada de acordo com os requisitos de segurança da empresa e da informação.
- Acesso a redes e serviços de rede Usuários só devem ter acesso às redes e aos serviços de rede cujos quais tenham sido especificamente autorizados a utilizar.
- Registro e cancelamento de registro do usuário Um processo formal de registro do usuário e de cancelamento deve ser implementado para possibilitar a atribuição de direitos de acesso.
- Provisionamento de acesso ao usuário Um processo formal de provisionamento de acesso ao usuário deve ser implementado para atribuir ou revogar direitos de acesso para todos os tipos de usuário para todos os sistemas e serviços.
- Gerenciamento de direitos de acesso privilegiado A atribuição e utilização de direitos de acesso privilegiado devem ser restritas e controladas.
- Gerenciamento de informações de autenticação secreta de usuários A atribuição de informações de autenticação secreta deve ser controlada através de um processo formal de gestão.

ISO 27002

- Revisão dos direitos de acesso dos usuários Proprietários de ativos devem rever os direitos de acesso dos usuários regularmente.

- Uso de informações de autenticação secreta Usuários devem ser obrigados a seguir as práticas da organização em relação ao uso de informações de autenticação secreta.

- Restrição de acesso às informações O acesso às informações e funções do sistema de aplicativos deve ser limitado de acordo com a política de controle de acesso.

- Procedimentos de log-on seguro Quando indicado pela política de controle de acesso, o acesso à sistemas e aplicativos deve ser controlado por um procedimento de log-on seguro.

- Sistema de gerenciamento de senhas O sistema de gerenciamento de senhas deve ser interativo e garantir senhas de qualidade.

- Uso de programa utilitário privilegiado O uso de programas utilitários que podem ser capazes de substituir controles de sistemas e de aplicativos deve ser restrito e estritamente controlado.

- Controle de acesso ao código-fonte do programa O acesso ao código-fonte do programa deve ser restrito.

Medidas de Segurança Técnica

Conteúdo:

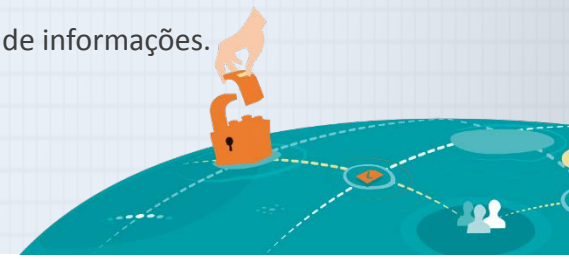
- Política sobre o uso de controles criptográficos Uma política sobre o uso de controles criptográficos para a proteção de informações deve ser desenvolvida e implementada.

- Gerenciamento de chaves A política sobre utilização, proteção e tempo de vida de chaves criptográficas deve ser desenvolvida e implementada através de todo seu ciclo de vida.

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- A gestão dos Ativos da Empresa, a Segurança da Infraestrutura de TI e a proteção dos dados contra acessos indesejados através do controle de acesso e aplicativos criptográficos.

- O uso correto de um aplicativo e o processamento correto de informações.



ISO 27002

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Gerenciamento de Acesso Lógico:
  - ✓ Concessão de acesso à Informação digital e Serviços de Informação para aquelas pessoas que estão autorizadas, bem como evitar que pessoas não autorizadas tenham acesso a essa Informação digital ou Serviço.
- Requisitos de Segurança para Sistemas de Informação:
  - ✓ Exigências relativas à aquisição e desenvolvimento de sistemas de informação.
- Criptografia:
  - ✓ Um meio para manter informações em segredo: criptografia de dados.
- Segurança de arquivos do sistema.
- Prevenção de vazamento de informações.

Criptografia

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Política de Criptografia - conteúdo:

- No que a organização deve usar a criptografia;
- Quais tipos de criptografia a organização usa e em quais aplicativos;
- Controle e gerenciamento de chaves;
- Cópia de segurança
- Controle.

Criptografia: Gerenciamento de Chaves

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

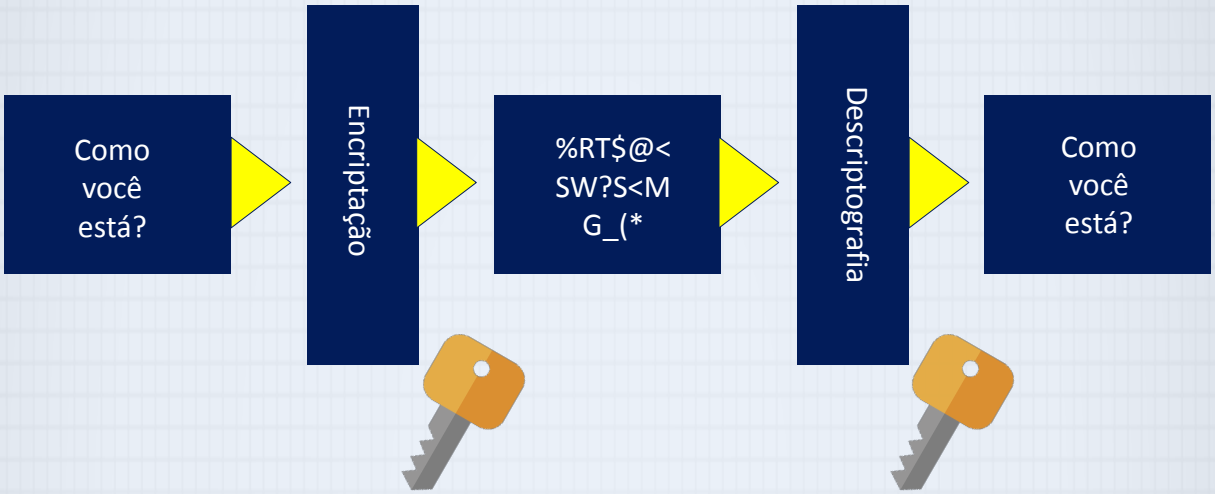
- As chaves criptográficas devem ser protegidas contra alteração, perda e destruição;
- Chaves secretas e pessoais precisam ser protegidas contra a divulgação não autorizada;
- O equipamento utilizado para gerar, armazenar e arquivar as chaves deve ser protegido fisicamente;
- Registro dos pares de chaves: quais pares foram emitidos a quem e quando;
- Quando uma chave irá expirar?
- O que deve ser feito quando uma chave for comprometida?
- Evite usar a mesma chave em sistemas diferentes (por exemplo, notebooks).

ISO 27002

Tipos de Sistemas Criptográficos

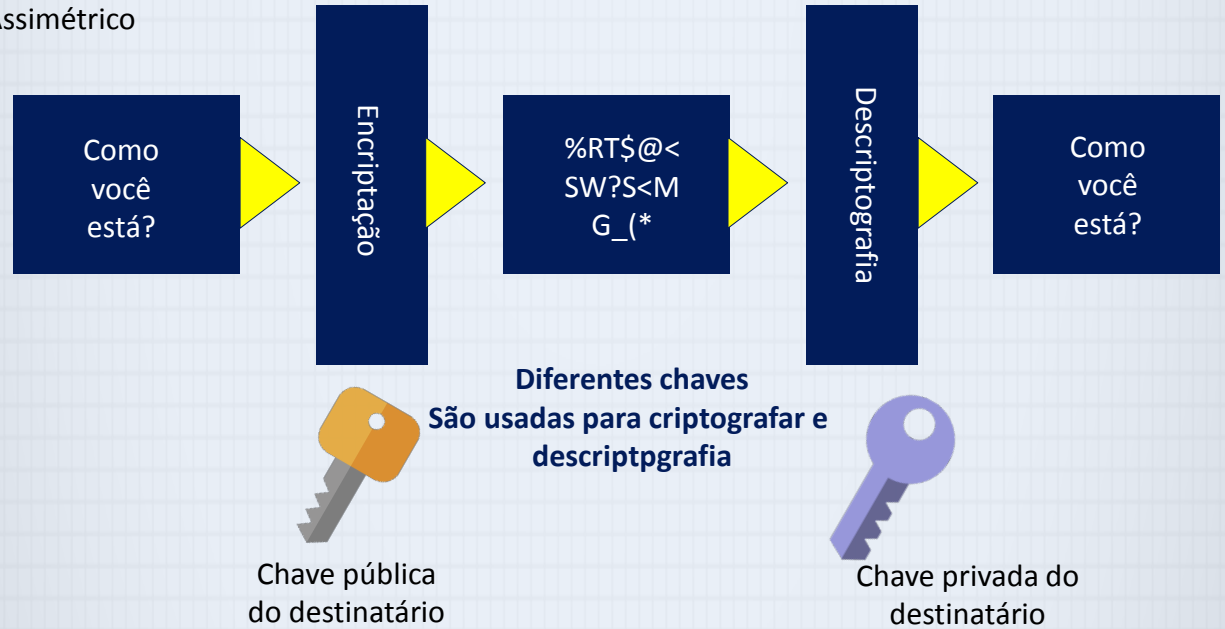
Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Simétrico



A mesma chave secreta foi compartilhada

Assimétrico



ISO 27002

Assinaturas Digitais

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Assinaturas digitais são criadas utilizando criptografia assimétrica.
- Uma assinatura digital é o método utilizado para confirmar se a informação digital foi produzida ou enviada por quem ela afirma ser – semelhante à assinatura de caneta em documentos de papel.
- A assinatura digital é geralmente constituída por dois algoritmos:
  - um para confirmar que a informação não foi alterada por terceiros;
  - outro para confirmar a identidade da pessoa que "assinou" a informação;
- Em alguns países (por exemplo, os da União Europeia), uma assinatura digital possui a mesma validade que a assinatura no "papel". Na maioria dos casos, é necessário usar um certificado atestado para verificar a veracidade desta assinatura digital (por exemplo, um smartcard).

Três Passos para Online Banking

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- A Associação Holandesa de Bancos mostrou que 98% das pessoas que utilizam o online banking consideram o meio seguro.
- No entanto, cerca de 20% dessas pessoas não tomam o suficiente de medidas de segurança
- Os bancos trabalham diariamente na segurança, mas a responsabilidade pela segurança também se encontra com o cliente.
- Isso levou à campanha dos “3 OKs” nos Países Baixos: A segurança do seu PC está OK?.
- O site do seu banco está OK?.
- O seu pagamento está OK/correto?.
- Somente ao prestar mais atenção, é possível evitar uma grande quantidade de prejuízo.

ISO 27002

Phishing

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Phishing é uma forma de fraude na internet;
- Uma fraude é definida como a realização de uma transação não autorizada;
- Geralmente a vítima recebe um e-mail pedindo para verificar ou confirmar uma conta bancária com os números da conta, senhas e cartão de crédito, por exemplo:
  - ✓ Às vezes mensagens SMS são usadas.
  - ✓ Até mesmo contato telefônico já utilizado.

Spam

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Spam é nome para o coletivo de mensagens indesejadas;
- O termo é normalmente utilizado para e-mails indesejados, mas mensagens publicitárias indesejadas em sites também são consideradas spam;

- Um filtro de spam pode diminuir esse problema;
- Existem algumas coisas que os usuários de computador podem fazer para combater o spam. Algumas delas são:
  - ✓ Nunca responda uma mensagem de spam, até mesmo para cancelar a inscrição, pois, desta forma, você estará apenas confirmando para o remetente do spam que o seu endereço de e-mail é real, o que fará com que ele envie ainda mais e-mails indesejados.
  - ✓ Não encaminhe mensagens de spam e não distribua endereços de e-mail (usar a funcionalidade CCO).

Malware: Um Software Malicioso

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Malware é uma combinação das palavras Malicioso e Software;
- Trata-se de um software indesejado, como vírus, worms, Cavalos de Troia e spywares;
- A solução padrão contra malwares é fazer varreduras com um antivírus e usar um firewall;
- A varredura do antivírus por si só não é tão eficaz contra malwares que surgem devido a ações humanas, tais como a abertura de e-mails suspeitos ou e-mails de remetentes desconhecidos.

ISO 27002

Malware: Vírus

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Definição:

- Um vírus é um pequeno programa de computador que se multiplica propositalmente, às vezes em formas alteradas;

- As versões replicadas do vírus original são, em virtude desta definição, também vírus. Para que o vírus se espalhe é necessário um programa que contenha um código executável.

Explicação:

- Assim que o programa é executado, o vírus procura novos programas para tentar infectá-los. Um vírus só pode se espalhar para fora do sistema infectado se um usuário transferir arquivos do sistema infectado para um novo sistema.

- Tradicionalmente, os hóspedes dos vírus eram apenas programas, mas atualmente documentos também podem atuar como hóspedes de um vírus, pois cada vez mais possuem códigos executáveis, como macros, VBScript ou ActiveX. Na grande maioria dos casos, os vírus são equipados com uma carga que abriga outros códigos executáveis – normalmente esta carga é de natureza destrutiva.

Exemplos:

- Brain;
- Chernobyl.

Medidas:

- Certifique-se de que existe uma varredura de vírus no servidor de e-mail e nos computadores no local de trabalho;
- Certifique-se de que o assunto de vírus está incluído nas campanhas de conscientização de segurança;
- Certifique-se de que este tema está incluído na Política de Segurança da Informação da organização.

Malware: Worm

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Definição:

Um worm é um pequeno programa de computador que se multiplica propositalmente. O resultado da multiplicação são cópias do original e se espalham por outros sistemas, fazendo uso dos recursos de rede do seu hospedeiro.

Explicação:

- As diferenças entre vírus e worms estão se tornando cada vez mais tênue;
- Um vírus pode atacar seu hospedeiro através de diferentes programas e infectar novos programas ao transferir seu código ativo;
- Um worm, ao contrário, não depende de um usuário para se espalhar: assim que um worm é ativado, ele irá se espalhar automaticamente. É isto o que faz com que os worms consigam se espalhar por grandes áreas em um curto período de tempo;
- As duas semelhanças mais importantes são a dependência de um código executável no hóspede e a utilização de uma carga para realizar tarefas secundárias que são, geralmente, destrutivas.

Malware: Vírus

Exemplos:

- Melissa;
- I love you;
- Happy99;
- Blaster;
- Storm Worm.

Medidas:

- Certifique-se de que existe uma varredura (de vírus) no servidor de e-mails e nos computadores no local de trabalho;
- Como os worms podem ser descobertos na rede, utilize um monitor de rede;
- Certifique-se de que o assunto de vírus está incluído nas campanhas de conscientização de segurança;
- Certifique-se de que este tema está incluído na Política de Segurança da Informação da organização.
- Certifique-se de que existem formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

ISO 27002

Malware: Cavalo de Troia

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Definição:

- Um Cavalo de Troia é um programa que, além de executar a função normal, realiza atividades secundárias sem que o usuário do computador perceba, o que pode prejudicar a integridade do sistema infectado.

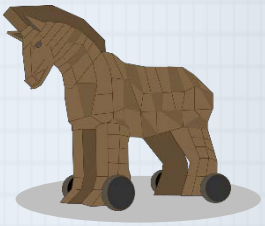
Explicação:

- Assim como o Cavalo de Troia da história grega, este programa se apresenta à primeira vista como algo útil, mas, quando é ativado pelo usuário, realiza todos os tipos de atividades indesejadas por trás;

- A carga do Cavalo de Troia muitas vezes instala uma "backdoor", através do qual pessoas desconhecidas podem ter acesso não autorizado ao sistema infectado;

- Outra atividade frequente deste malware é enviarem informações confidenciais do sistema infectado para outro local onde serão recolhidas e analisadas;

- A diferença mais perceptível com os vírus e worms é que o Cavalo de Troia não pode se replicar. E por este motivo, os Cavalos de Troia geralmente permanecem despercebidos por um longo período de tempo executando suas atividades maliciosas.



Exemplos:

- BackOrrifice;
- Netbus.

Medidas:

- Certifique-se de que há uma varredura de Cavalo de Troia e/ou vírus no servidor de e-mail e nos computadores no local de trabalho;

- Certifique-se de que o assunto Cavalo de Troia está incluído nas campanhas de conscientização de segurança;

- Certifique-se de que este tema está incluído na Política de Segurança da Informação da organização;

- As atividades dos Cavalos de Troia (comunicação) também podem ser descobertas na rede pelos gestores de rede. Ferramentas de monitoramento de rede podem ajudar com isso.

ISO 27002

Malware: Hoax

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Definição:

- Uma hoax (ou, em tradução literal, "embuste") é uma mensagem que tenta convencer o destinatário de sua veracidade e, em seguida, levar o leitor a realizar uma determinada ação.
- A disseminação de hoaxes depende de leitores que enviam deliberadamente a mensagem para outras vítimas em potencial que, então, podem também fazer o mesmo.

Explicação:

- A carga de uma hoax não é de natureza técnica, mas, sim, psicológica;
- Ao jogar com as emoções das pessoas, a hoax tenta convencer o leitor a compartilhá-la com outros (uma forma de engenharia social);
- Este é quase sempre o propósito de uma hoax , mas ela pode ocasionalmente tentar convencer as pessoas a depositarem dinheiro, fornecer informações pessoais (phishing) ou outras atividades maliciosas;
- Correntes de e-mail é a forma mais significativa e bem sucedida de hoax.

Malware: Bomba de Lógica

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Exemplos: Príncipe da Nigéria.

Medidas:

- Certifique-se de que há uma varredura de vírus no local de trabalho e uma solução antispam no servidor de e-mail. Uma hoax muitas vezes contém textos que podem ser reconhecidos por esses filtros;
- Certifique-se de que o assunto sobre as hoaxes está incluído nas campanhas de conscientização de segurança. Os funcionários devem estar atentos para perguntas estranhas em e-mails, especialmente aqueles que tentam convencer o leitor a realizar certas ações, como encaminhar a hoax para outros;
- Certifique-se de que este tema está incluído na Política de Segurança da Informação da organização;

- Certifique-se de que existem formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

Definição:

- Uma bomba de lógica é um pedaço de código que é construído em um sistema de software

Este código irá, em seguida, executar uma função quando estiverem reunidas condições específicas Nem sempre isso será usado para fins maliciosos. Um programador de computador, por exemplo, pode construir um código que destruirá arquivos confidenciais uma vez que deixarem a rede da empresa.

- Vírus e worms, muitas vezes, contêm bombas de lógica, que normalmente demoram algum tempo para serem "detonadas" para que o vírus ou worm se propaguem.

Medidas:

- Para softwares desenvolvidos por funcionários da empresa ou sob contrato com terceiros, realize uma audição do código por outra parte.

Malware: Spyware

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Definição:

- Spyware é um programa de computador que recolhe informações sobre o usuário do computador e as encaminha para terceiros. O seu objetivo é monetário.

- O Spyware não prejudica o computador e/ou o software instalado, mas, ao invés disso, ele viola a privacidade do usuário.

- Um Spyware pode ser reconhecido através de diversas maneiras, por exemplo:
  - ✓ O computador está mais lento do que de costume;
  - ✓ Programas estão sendo executados mesmo sem que você os tenha iniciado ou são programas que você nunca viu antes;
  - ✓ As configurações do computador foram modificadas e pode haver uma nova barra de ferramentas no seu navegador de internet que não estava lá antes e você não consegue removê-la;
  - ✓ Vários tipos de pop-ups aparecem sem mais nem menos ou quando você abre páginas da internet.

Medidas:

- Existem varreduras dos registros do Windows que procuram por chaves suspeitas de registros e buscam por spywares nos programas instalados;

- Muitos programas antivírus também detectam spywares;
- Use um firewall para detectar o tráfego da rede e procure por tráfico de rede saindo do seu computador sem nenhum motivo aparente;
- Certifique-se de que o assunto sobre spywares está incluído nas campanhas de conscientização de segurança;
- Certifique-se de que este tema está incluído na Política de Segurança da Informação da organização;
- Certifique-se de que existem formas eficazes de relatar incidentes e de que existam bons procedimentos de follow-up.

Malware: Botnet / Storm Worm

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Explicação:

- O Storm Worm é considerado por muitos como o futuro do malware;
- Ele é paciente, e, portanto, difícil de ser detectado;
- Este malware funciona como uma colônia de formigas, onde não há nenhum comando de controle central, mas sim uma conexão de rede entre milhares de PCs infectados;
- Como resultado, as máquinas infectadas não afetam o botnet;
- O Storm Worm não causa qualquer dano ao anfitrião, de modo que ele permanece despercebido;
- A razão pela qual Storm Worm é um sucesso tão grande é que os servidores que espalham o Storm Worm recodificam a mensagem de vírus a cada trinta minutos, mudando a assinatura do vírus e tornando-o ainda mais difícil de ser detectado por antivírus tradicionais.

Malware: Rootkit

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Explicação:

- Rootkit é um conjunto de ferramentas de software que é frequentemente utilizado por terceiros (normalmente um hacker) após invadir um sistema (computador);

- O rootkit se esconde nas profundezas do sistema operacional do sistema, o que pode causar instabilidade no sistema operacional;
- Um rootkit é quase impossível de ser removido sem danificar o sistema operativo;
- Rootkits podem trabalhar em dois níveis: nível do kernel e nível do usuário;
- Rootkits que trabalham no nível do kernel podem fazer quase qualquer coisa no sistema. O objetivo dessas ferramentas é ler, alterar ou influenciar os processos em execução, dados ou arquivos do sistema;
- Um rootkit ajuda o intruso a obter acesso ao sistema, sem a consciência do usuário;
- Existem rootkits para quase todos os sistemas operacionais.

Segurança Organizacional

Segurança das Operações

- Procedimentos e responsabilidades operacionais Objetivo: garantir o funcionamento correto e seguro de instalações de processamento de informações.
- Proteção contra malwares Objetivo: garantir que as informações e as instalações de processamento de informações estejam protegidas contra malwares.
- Backup Objetivo: se proteger contra perda de dados.
- Registro e monitoramento Objetivo: gravar eventos e gerar evidências.
- Controle de software operacional Objetivo: garantir a integridade dos sistemas operacionais.
- Considerações de auditoria de sistemas de informação Objetivo: minimizar o impacto das atividades de auditoria em sistemas operacionais.

Conteúdo:

- Procedimentos operacionais documentados Procedimentos operacionais devem ser documentados e disponibilizados a todos os usuários que os precisem.
- Gerenciamento da mudança Mudanças na organização, nos processos de negócio, nas instalações de processamento de informações e nos sistemas que afetam a segurança da

informação devem ser controladas.

- Gerenciamento de capacidade O uso de recursos deve ser monitorado, alinhado e projeções devem ser feitas sobre requisitos futuros de capacidade para garantir o desempenho exigido do sistema.

- Separação de desenvolvimento, teste e ambientes operacionais Desenvolvimento, teste e ambientes operacionais devem ser separados para reduzir os riscos de acesso não autorizado ou alterações no ambiente operacional.

- Controles contra malwares Controles de detecção, de prevenção e de recuperação para proteção contra malwares devem ser implementados juntamente com a conscientização dos usuários.

- Backup das informações As cópias de informações, softwares e imagens do sistema salvas como backup devem ser testadas regularmente, de acordo com a política de backup vigente.

- Registro de eventos Registro de eventos com gravação das atividades dos usuários, exceções, falhas e eventos de segurança da informação devem ser feitos, mantidos e revisados regularmente.

- Proteção dos registros de informações Instalações de registro e registros de informações devem ser protegidos contra a manipulação indevida e acesso não autorizado.

- Registros do administrador e do operador As atividades do administrado de sistema e do operador de sistema devem ser registradas e estes registros devem ser protegidos e revisados regularmente.

- Sincronização dos relógios Os relógios de todos os sistemas de processamento de informações relevantes dentro de uma organização ou domínio de segurança devem estar sincronizados através de uma única referência de tempo.

- Instalação de software em sistemas operacionais Procedimentos devem ser implementados para controlar a instalação de software em sistemas operacionais.

- Gerenciamento de vulnerabilidades técnicas Informações sobre vulnerabilidades técnicas de sistemas de informação sendo utilizados devem ser obtidas em tempo hábil, a exposição da organização a tais vulnerabilidades deve ser analisada e as medidas adequadas precisam ser tomadas para lidar com o risco em questão.

- Restrições sobre instalação de software Regras que controlam a instalação de softwares por

usuários devem ser definidas e implementadas.

- Controles de auditoria de sistemas de informação Os requisitos e atividades de auditoria que envolvem verificação de sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar interrupções nos processos do negócio.

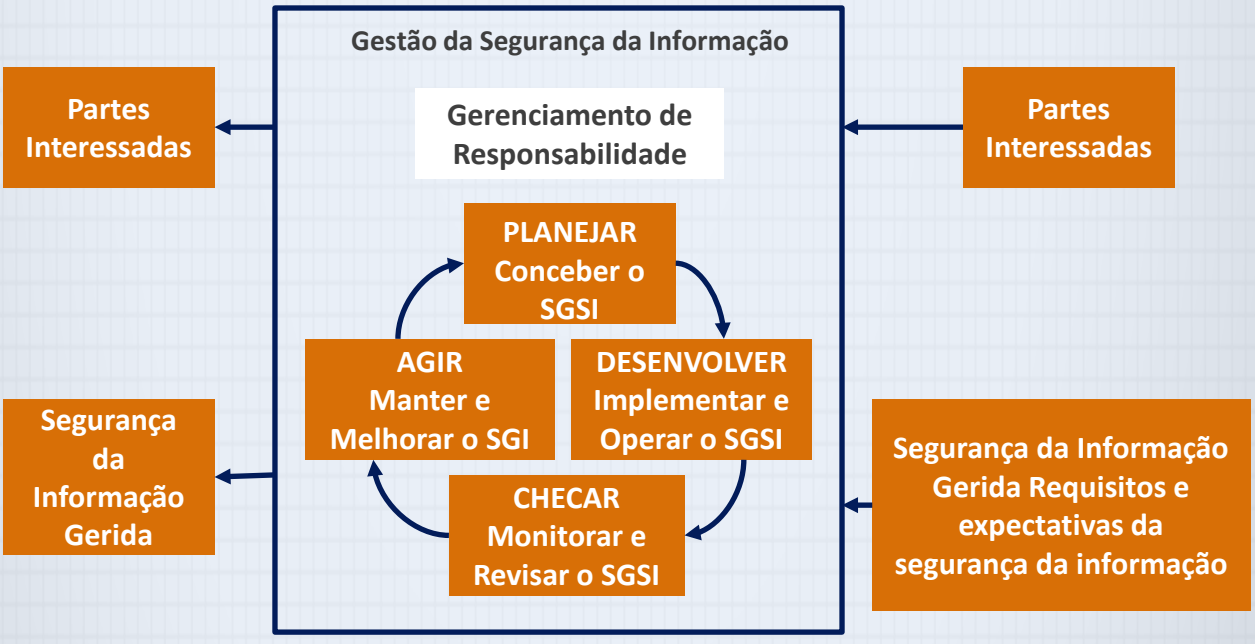
Medidas de Segurança Organizacional

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Características:

- Medidas Técnicas estão intimamente relacionadas com Medidas Organizacionais. Medidas Técnicas executam ou forçam Medidas Organizacionais;
- O ciclo PDCA é uma forma para implementar a Segurança da Informação na organização;
- Como promover a Segurança da Informação na organização;
- Como lidar e se preparar para desastres;
- O aspecto da comunicação da Segurança da Informação;
- Os aspectos operacionais, procedimentos de teste e gestão da Segurança da Informação.

O PDCA na Prática



ISO 27002

Os métodos de PDCA, que haviam sido partes obrigatórias da ISO/IEC 27001:2005, não são mais uma exigência estrita. Outros métodos podem ser adotados. No entanto, o PDCA ainda é uma parte importante deste curso.

Planejar (conceber o Sistema de Gestão de Segurança da Informação) Estabelecer a política do SGSI, objetivos, processos e procedimentos relevantes para o gerenciamento de risco e melhorar a segurança da informação para fornecer resultados de acordo com as políticas e objetivos gerais da organização.

Desenvolver (implementar e operar o SGSI) Implementar e operar a política do SGSI, controles, processos e procedimentos.

Checar (monitorar e revisar o SGSI) Avaliar e, quando aplicável, medir o desempenho do processo de acordo com a política do SGSI, objetivos e experiências práticas, e relatar os resultados à gerência para revisão.

Agir (manter e melhorar o SGSI) Tomar ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e revisão da gerência ou outras informações relevantes, para alcançar a melhoria contínua do SGSI.

Exemplos de Medidas Organizacionais

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Política de Segurança da Informação:
- Organização da Segurança da Informação;
- Criação de um Sistema de Gestão da Segurança da Informação (SGSI).

Pessoas:
- Triagem e confidencialidade;
- Registros de funcionários;
- Conscientização de Segurança;
- Gerenciamento de Acesso.

Gestão de Continuidade de Negócios:
- Plano de Continuidade de Negócios;
- Plano de Recuperação de Desastres.

Gerenciando Comunicação e Operando Processos>
- Procedimentos Operacionais;
- Gerenciamento da Mudança;
- Segregação de Funções.

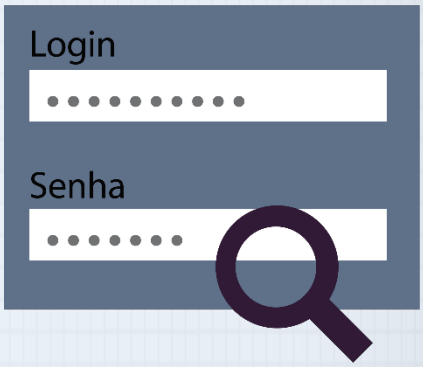
ISO 27002

Controle de Acesso (1)

Objetivo:
- Controlar o Acesso à Informação.

Seções:
- Requisitos do negócio para Controle de Acesso;
- Política de Controle de Acesso.

Gerenciamento de Acesso do Usuário:
- Registro do usuário;
- Gerenciamento de Privilégio;
- Gerenciamento de Senhas do Usuário;
- Revisão de Direitos de Acesso do Usuário;
- Responsabilidades do Usuário;
- Uso de senha;
- Política de Mesa Limpa e Tela Limpa;



Controle de Acesso (2)

Seções (continuação)
Política de Uso de Serviços de Rede:
- Autenticação do Usuário para Conexões Externas;
- Identificação de Equipamento em Redes;
- Diagnóstico Remoto e Proteção de Porta de Configuração;
- Segregação de Redes;
- Controle de Conexão de Rede;
- Controle de Roteamento de Rede.

Controle de Acesso ao Sistema de Operação:
- Procedimentos de Log-on Seguro;
- Identificação e Autenticação de Usuário;
- Sistema de Gerenciamento de Senha;
- Uso de Utilitários de Sistema;
- Sessão Expirada;
- Limitação de Tempo de Conexão.

ISO 27002

Controle de Acesso (2)

Seções (continuação)
Controle de Acesso à Informação e Aplicativos:
- Restrição de Acesso às Informações.
- Isolamento de Sistemas Sensíveis.

Computadores Portáteis e Trabalho Remoto:
- Computadores Portáteis e Comunicações.
- Trabalho Remoto.

Concedendo Acesso

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Na concessão de acesso, é feita uma distinção entre:
- Identificação;
- Autenticação e;
- Autorização.

1. Identificação é o primeiro passo no processo para a concessão de acesso. Na etapa de identificação, a pessoa ou o sistema apresenta um token, por exemplo, uma chave, nome de usuário ou senha;
2. O sistema, então, determina se o token é autêntico e quais recursos ele garante acesso
3. Assim que isso for determinado, as autorizações são liberadas.

Exemplos de Autenticação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Para salas especiais, tais como salas de computadores, pode-se usar medidas de autenticação mais robustas.

- Além dos passes de acesso, medidas adicionais de segurança são tomadas, tais como:
  - ✓ Algo que você saiba, por exemplo, um código;
  - ✓ Algo que você possua, por exemplo, um cartão;
  - ✓ Algo que faz parte de você, por exemplo, impressão digital ou varredura da íris.

Exemplos de Autenticação

- A concessão de direitos específicos, tais como o acesso seletivo para uma pessoa, como, por exemplo:

- ✓ A concessão de acesso de leitura/gravação para um arquivo de banco de dados para um Administrador de Banco de Dados
- ✓ A concessão de acesso a um edifício para uma pessoa de plantão durante o fim de semana;
- ✓ A concessão de acesso de leitura para outra pessoa a uma de suas pastas/diretórios pessoais;
- ✓ A concessão de acesso à área de embarque de um aeroporto após a verificação de segurança (autenticação) ter sido concluída com êxito.

Segregação de Funções

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- As tarefas e responsabilidades devem ser segregadas para evitar a possibilidade de alterações não autorizadas, não intencionais ou o uso indevido de ativos da organização;
- Na segregação de funções, uma revisão é realizada para saber se uma pessoa realiza tarefas de tomada de decisões, executivas ou de controle;
- Determina-se se a pessoa precisa de acesso à informação;
- Acesso desnecessário aumenta o risco das informações serem usadas intencionalmente ou não, alteradas ou destruídas. Isso é chamado de princípio da "necessidade de conhecer".;
- Uma vez que as necessidades de acesso e funções de funcionários são determinadas, as tarefas podem ser divididas para reduzir os riscos da organização.

Sistema de Gerenciamento de Senhas

Um sistema de gerenciamento de senhas deve:

a) Obrigar o uso de IDs e senhas individuais para manter a prestação de contas;
b) Permitir que os usuários selecionem e alterem suas próprias senhas e incluir um procedimento de confirmação para permitir erros de entrada;
c) Impor uma escolha de senhas de qualidade;
d) Impor alterações de senha;
e) Impor a alteração de senhas temporárias no primeiro log-on;
f) Manter um registro de senhas de usuários anteriores e evitar a reutilização;
g) Não exibir as senhas na tela enquanto estão sendo introduzidas;
h) Armazenar os arquivos de senha separadamente dos dados de sistema do aplicativo;
i) Armazenar e transmitir senhas de forma protegida (por exemplo, criptografadas ou hash).

ISO 27002

ISO/IEC 27002
Specification

Continuidade de Segurança da Informação

Aspectos da segurança da informação da gestão de continuidade de negócios:

- Continuidade de Segurança da Informação:
  - ✓ Objetivo: continuidade de segurança da informação deve ser incorporada nos sistemas de gestão de continuidade de negócios da organização.

- Redundâncias:
  - ✓ Objetivo: garantir a disponibilidade de instalações de processamento de informações.

Conteúdo:

- Planejamento da continuidade de segurança da informação A organização deve determinar suas exigências para segurança da informação e a continuidade da gestão de segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

- Implementando continuidade de segurança da informação A organização deve estabelecer, documentar, implementar e manter processos, procedimentos e controles para assegurar o nível necessário de continuidade de segurança da informação durante uma situação adversa.

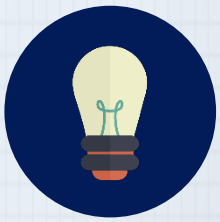
- Verificar, analisar e avaliar a continuidade de segurança da informação A organização deve verificar os controles de continuidade de segurança da informação estabelecidos e implementados regularmente para garantir que estejam válidos e eficazes em situações adversas.

- Disponibilidade de instalações de processamento de informações Instalações de processamento de informação devem ser implementadas com o suficiente de redundância para atender os requisitos de disponibilidade.

Por Que Gestão de Continuidade de Negócios?

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Proteção de processos de negócios;
- Continuidade de serviço;
- Sobrevivência da companhia;
- Lucro ou perda;
- Publicidade negativa.



Plano de Recuperação de Desastres (PRD):

- Para minimizar as consequências de um desastre e tomar as medidas necessárias para garantir que os funcionários, ativos de negócios e processos de negócios estejam disponíveis novamente

dentro de um tempo aceitável

- Tem objetivo de efetuar a recuperação imediatamente após um desastre.

Plano de Continuidade de Negócios (PCN):

- Para organizar métodos e procedimentos para falhas que duram um longo período de tempo;
- Organizar um local alternativo onde o trabalho possa ser realizado enquanto o local original é reconstruído;
- Tudo deve estar focado em manter a empresa funcionando, ainda que parcialmente, desde o momento do desastre até quando a empresa estiver totalmente recuperada.

Testando o Plano de RD e o Plano CN

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- Testes regulares são necessários para conscientizar os empregados sobre como agir em caso de desastres.
- Toda mudança que é feita nos processos de negócios deve ser incluída no plano. Um plano ultrapassado não irá ajudar a organização a se tornar operacional novamente.
- É essencial que em todos os testes os procedimentos sejam testados simulando uma situação da vida real para verificar se essas medidas são de fato corretas e eficazes.

O que aprendemos?

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

- **A importância de Medidas de Segurança:**
  - ✓ Os vários tipos de Medidas de Segurança;
  - ✓ As várias Classificações das Medidas de Segurança.
- **As várias Medidas de Segurança Física;**
- **As várias Medidas de Segurança Técnica:**
  - ✓ Criptografia;
  - ✓ Malware.
- **As várias medidas de segurança organizacional:**
  - ✓ Gerenciamento de Acesso;
  - ✓ Identificação, Autenticação, Autorização;
  - ✓ Gestão de Continuidade de Negócios.

ISO 27002

Conformidade

Conformidade com os requisitos legais e contratuais:

- Objetivo: evitar violações das obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e quaisquer requisitos de segurança.

Revisões de segurança de informação:

- Objetivo: garantir que a segurança da informação seja implementada e operada de acordo com as políticas e procedimentos organizacionais.

Conteúdo

- Identificação da legislação aplicável e requisitos contratuais Todos os regulamentos legais relevantes, requisitos contratuais e a abordagem da organização para atender a esses requisitos devem ser explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação e organização.

- Direitos de propriedade intelectual Procedimentos adequados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relativos aos direitos de propriedade intelectual.

- Proteção de registros Registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos legislativos, regulamentares, contratuais e de negócios.

- Privacidade e proteção de informação pessoal A privacidade e proteção de informação pessoal devem ser asseguradas, conforme exigido na legislação e regulamentação relevantes, quando aplicável.

- Regulamentação de controles de criptografia Controles de criptografia devem ser utilizados em conformidade com todos os acordos, legislação e regulamentos relevantes.

- Avaliação independente da segurança da informação A abordagem da organização para gerir a segurança da informação e a sua implementação (ou seja, controle de objetivos, controles, políticas, processos e procedimentos para a segurança da informação) devem ser revisados de forma independente em intervalos planejados ou quando ocorrem alterações significativas.

- Conformidade com as políticas de segurança e normas Gerentes devem avaliar periodicamente a conformidade do processamento de informações e procedimentos dentro da sua área de responsabilidade com as políticas de segurança, normas e quaisquer outros requisitos de segurança.

- Revisão de conformidade técnica Sistemas de informações devem ser regularmente revistos para cumprimento das políticas e normas de segurança da informação da organização.

Por Que Legislação e Regulamentos São Importantes?

- Observar os Regulamentos Legais;
- Observar a Conformidade;
- Cobrir Direitos de Propriedade Intelectual;
- Proteger Documentos do Negócio;
- Proteger Dados e Confidencialidade dos Dados Pessoais:
  - ✓ Ex.: Lei de Proteção de Dados Pessoais: a proteção dos dados pessoais e da privacidade;
- Evitar a Violação das Instalações de TI;
- Observar a Política de Segurança e Normas de Segurança;
- Controlar as Medidas;
- Realização de Auditorias em Sistemas de Informação;
- Proteger Meios Utilizados para Auditar Sistemas de Informação.

Legislação de Segurança da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Exemplos:

- Legislação envolvendo Privacidade, Tributos e Finanças, e Regulamentos para Bancos e Empresas (por exemplo, Sarbanes Oxley);
- Legislações Municipais, Estaduais e Federais;
- A própria Política da empresa e sua Legislação interna;
- A Legislação de uma nação estrangeira ao fazer negócios internacionais;
- Legislação envolvendo Privacidade;
- Os governos estão sujeitos à legislação de registros públicos. Esta legislação aborda a criação de arquivos, gerenciamento, destruição, transferência para o arquivo central, transferência entre governos e acesso a arquivos;
- Legislação destinada a crimes feitos com computadores.

ISO 27002

Atos Legislativos

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

A Lei de Registros Públicos:
- Regulamenta o armazenamento e destruição de documentos.

Lei de Proteção de Dados Pessoais:
- Regula o direito de inspeção de dados pessoais.

A Lei de Cibercrimes:
- Esta lei é uma alteração do Código Penal e Código de Processo Penal para facilitar o combate a crimes cometidos por meio da tecnologia de informação. Um exemplo de um novo delito são as invasões de computador.

A Lei de Acesso Público às Informações do Governo:
- Regula a inspeção de documentos escritos do governo. Dados pessoais não são documentos do governo.

Regulamentos de Segurança da Informação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Exemplos:
- Regulamentos envolvendo Privacidade, Tributos e Finanças, e Regulamentos para Bancos e Empresas (por exemplo, Sarbanes Oxley);
- Regulamentos Municipais, Estaduais e Federais;
- A própria Política da empresa e sua Legislação interna;
- Os Regulamentos de uma nação estrangeira ao fazer negócios internacionais;
- Regulamentos envolvendo Privacidade;
- Regulamentos para proteger os dados;
- Regulamentos sobre o uso correto de Licenças.

ISO 27002

Medidas de Legislação e Regulamentação

Melhores Práticas de acordo com os Fundamentos da Segurança da Informação.

Exemplos:

- **Medidas para proteger os Direitos de Propriedade Intelectual:**
  - ✓ Contratos de Licença;
  - ✓ Contratos de Direitos Autorais.
- **Medidas que envolvem proteção de registros organizacionais:**
  - ✓ Arquivos Criptografados;
  - ✓ Salas com Temperatura Controlada para Armazenamento de Registros em Papéis;
  - ✓ Uma Política de Eliminação de Registros;
- **Medidas que envolvem a proteção de informações pessoais:**
  - ✓ Direitos de Acesso adequados.
- **Prevenção do uso indevido de Instalações de Processamento de Informações:**
  - ✓ Monitoramento através de uma rede de Câmeras de Segurança.
- **Cumprimento das Políticas e Normas de Segurança:**
  - ✓ Revisões e Ações Corretivas realizadas pela Gerência.
- **Verificação de Conformidade Técnica:**
  - ✓ Avaliação da Vulnerabilidade.

Dicas para Fazer a Prova

- Leia toda a questão;
- Pense nas possíveis respostas;
- Olhe as opções de resposta;
- Leia atentamente o que é que está sendo pedido;
- Leia a questão inteira 2 ou 3 vezes;
- Sublinhe/destaque as palavras-chave;
- Você provavelmente terá 30-40 minutos para responder a todas as perguntas;
- Você tem 60 minutos no total, o que te permite tempo suficiente para ler cuidadosamente cada pergunta 2 ou 3 vezes;
- Procure pela MELHOR resposta;
- Pule a questão se estiver muito difícil e volte a ela mais tarde. Não se esqueça também de pular o número dessa questão na sua folha de respostas;
- Sempre responda as questões;
- Ignore as informações irrelevantes;
- Aplique o processo de eliminação.

III - Guia Preparatório

Visão Geral

EXIN Fundamentos de Segurança da Informação baseado na norma ISO/IEC 27002 (ISFS.PR).

Resumo

A segurança da informação é a proteção das informações de uma grande variedade de ameaças com o objetivo de assegurar a continuidade do negócio, minimizar o risco do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócios. (Definição da norma ISO/IEC 27002)

A segurança das informações vem ganhando importância no mundo da Tecnologia da Informação(TI). A globalização da economia está gerando uma troca cada vez maior de informações entre as organizações (seus funcionários, clientes e fornecedores) bem como uma explosão no uso de computadores em rede e dispositivos de informática.

A norma internacional, o Código de Prática para Segurança da Informação ISO/IEC 27002:2013, é uma norma amplamente respeitada e consultada e fornece uma estrutura para a organização e o gerenciamento de um programa de segurança das informações. A implementação de um programa com base nesta norma será muito útil para o objetivo de uma organização de atender a muitas das necessidades apresentadas no complexo ambiente operacional da atualidade. Uma compreensão categórica desta norma é importante para o desenvolvimento pessoal de todos os profissionais de segurança das informações.

Nos módulos de Segurança da Informação do EXIN, utiliza-se a seguinte definição: A Segurança da Informação lida com a definição, a implementação, a manutenção, a conformidade e a avaliação de um conjunto coerente de controles (medidas) que garantam a disponibilidade, a integridade e a confidencialidade da fonte de informações (manual e automática).

No módulo Fundamentos de Segurança da Informação do EXIN baseado na norma ISO/IEC 27002 são testados os conceitos básicos de segurança da informação e suas relações. Um dos objetivos desse módulo é aumentar a conscientização de que as informações são valiosas e vulneráveis e aprender quais medidas são necessárias para protegê-las.

Os tópicos para este módulo são:

- Informação e segurança: os conceitos, o valor da informação e da importância da confiabilidade.
- Ameaças e riscos: a relação entre as ameaças e confiabilidade.
- Abordagem e organização: a política de segurança e estabelecimento da Segurança da Informação.
- Medidas: física, técnica e organizacional, e;
- Legislação e regulamentação: a importância e funcionamento.

ISO 27002

Contexto - Programa de qualificação

O certificado em Fundamentos de Segurança da Informação do EXIN baseado na norma ISO/IEC 27002 faz parte do programa de qualificação em Segurança da Informação. O módulo é seguido pelos certificados de Gerenciamento de Segurança da Informação Avançado do EXIN baseado na norma ISO/IEC 27002 e Gerenciamento de Segurança da Informação Especializado do EXIN baseado na norma ISO/IEC 27002.

Público-alvo:
Qualquer pessoa na organização que manuseia informações. É também aplicável a proprietários de pequenas empresas a quem alguns conceitos básicos de Segurança da Informação são necessários. Este módulo pode ser um excelente ponto de partida para novos profissionais de segurança da informação.

Pré-requisitos: Nenhum
Formato do exame: Exame com questões de múltipla escolha
Estimativa de Tempo de Estudo: 60 horas
Exercício prático: Não aplicável
Tempo destinado ao exame: 60minutos

Detalhes do exame:
- Número de questões: 40
- Mínimo para aprovação: 65 % (26 de 40)
- Com consulta: não
- Equipamentos eletrônicos permitidos: não

ISO 27002

Requisitos do exame

Os requisitos do exame são os principais temas de um módulo. O candidato deve ter o domínio completo sobre estes temas. Os requisitos do exame são elaborados na especificação do exame.

Requisitos do exame	Especificação de exame	Peso (%)
1. Informação e segurança		**10%**
1.1. O conceito de informação 1.2 Valor da informação 1.3 Aspectos de confiabilidade		**2.5%** **2.5%** **5%**
2. Ameaças e riscos		**30%**
2.1 Ameaças e riscos 2.2 Relacionamento entre ameaças, riscos e confiabilidade da informação		**15%** **15%**
3. Abordagem e organização		**10%**
3.1 Política de segurança eorganização de segurança 3.2 Componentes da organização da segurança 3.3 Gerenciamento de incidentes		**2.5%** **2.5%** **5%**
4. Medidas		**40%**
4.1 Importância de medidas de segurança 4.2 Medidas físicas 4.3 Medidas técnicas 4.4 Medidas organizacionais		**10%** **10%** **10%** **10%**
5. Legislação e regulamentação		**10%**
5.1 Legislação e regulamentação		10%
Total		**100**

ISO 27002

Requisitos e especificações do exame

1. Informação e Segurança (10%)
1.1 O conceito de informação (2,5%)
O candidato entende o conceito de informação.
O candidato é capaz de:
1.1.1 Explicar a diferença entre os dados e informações.
1.1.2 Descrever o meio de armazenamento que faz parte da infraestrutura básica.

1.2 Valor da informação (2,5%)
O candidato entende o valor da informação para as organizações. O candidato é capaz de:
1.2.1 Descrever o valor de dados / informação para as organizações.
1.2.2 Descrever como o valor de dados / informação pode influenciar as organizações.
1.2.3 Explicar como conceitos aplicados de segurança da informação protegem o valor de dados / informação.

1.3 Aspectos de confiabilidade (5%)
O candidato conhece os aspectos de confiabilidade (confidencialidade, integridade, disponibilidade) da informação.
O candidato é capaz de:
1.3.1 Nome dos aspectos de confiabilidade da informação.
1.3.2 Descrever os aspectos de confiabilidade da informação.

2. Ameaças e riscos (30%)
2.1 Ameaça e risco (15%)
O candidato compreende os conceitos de ameaça e risco.
O candidato é capaz de:
2.1.1 Explicar os conceitos ameaça, de risco e análise de risco.
2.1.2 Explicar a relação entre uma ameaça e um risco.
2.1.3 Descreva os vários tipos de ameaças.
2.1.4 Descreva os vários tipos de danos
2.1.5 Descrever diferentes estratégias de risco
2.2 Relacionamento entre ameaças, riscos e confiabilidade das informações. (15%).
O candidato compreende a relação entre as ameaças, riscos e confiabilidade das informações.
O candidato é capaz de:
2.2.1 Reconhecer exemplos dos diversos tipos de ameaças.
2.2.2 Descrever os efeitos que os vários tipos de ameaças têm sobre a informação e ao tratamento das informações.

3. Abordagem e Organização (10%)

3.1 Política de Segurança e organização de segurança (2,5%)

O candidato tem conhecimento da política de segurança e conceitos de organização de segurança. O candidato é capaz de:

3.1.1 descrever os objetivos e o conteúdo de uma política de segurança

3.1.2 descrever os objetivos e o conteúdo de uma organização de segurança.

3.2 Componentes da organização da segurança (2,5%)

O candidato conhece as várias componentes da organização da segurança. O candidato é capaz de:

3.2.1 Explicar a importância de um código de conduta

3.2.2 Explicar a importância da propriedade

3.2.3 Nomear os mais importantes papéis na organização da segurança da informação.

3.3 Gerenciamento de Incidentes (5%)

O candidato compreende a importância da gestão de incidentes e escaladas. O candidato é capaz de:

3.3.1 Resumir como incidentes de segurança são comunicados e as informações que são necessárias.

3.3.2 Dar exemplos de incidentes de segurança.

3.3.3 Explicar as consequências da não notificação de incidentes de segurança.

3.3.4 Explicar o que implica uma escalação (funcional e hierárquico).

3.3.5 Descrever os efeitos de uma escalação dentro da organização.

3.3.6 Explicar o ciclo do incidente.

4. Medidas (40%)

4.1 Importância das medidas de segurança (10%)

O candidato entende a importância de medidas de segurança. O candidato é capaz de:

4.1.1 Descrever as maneiras pelas quais as medidas de segurança podem ser estruturadas ou organizadas.

4.1.2 Dar exemplos de cada tipo de medida de segurança

4.1.3 Explicar a relação entre os riscos e medidas de segurança.

4.1.4 Explicar o objetivo da classificação das informações.

4.1.5 Descrever o efeito da classificação.

4.2 Medidas de segurança física (10%)

O candidato tem conhecimento tanto da criação e execução de medidas de segurança física. O candidato é capaz de:

4.2.1 Dar exemplos de medidas de segurança física.

4.2.2 Descrever os riscos relacionados a medidas inadequadas de segurança física.

4.3 Medidas de ordem técnica (10%)

O candidato tem conhecimento tanto da criação quanto da execução de medidas de segurança técnica.

O candidato é capaz de:
4.3.1 Dar exemplos de medidas de segurança técnica.
4.3.2 Descrever os riscos relacionados a medidas inadequadas de segurança técnica.
4.3.3 Compreender os conceitos de criptografia, assinatura digital e certificado.
4.3.4 Nome das três etapas para internet banking (PC, web site, pagamento).
4.3.5 Nomear vários tipos de software malicioso.
4.3.6 Descrever as medidas que podem ser usadas contra software malicioso.

4.4 Medidas organizacionais (10%)

O candidato tem conhecimento tanto da criação quanto da execução de medidas de segurança organizacional.
O candidato é capaz de:
4.4.1 Dar exemplos de medidas de segurança organizacional.
4.4.2 Descrever os perigos e riscos relacionados a medidas inadequadas de segurança organizacional.
4.4.3 Descrever as medidas de segurança de acesso, tais como a segregação de funções e do uso de senhas
4.4.4 Descrever os princípios de gestão de acesso
4.4.5 Descrever os conceitos de identificação, autenticação e autorização.
4.4.6 Explicar a importância para uma organização de um bem montado Gerenciamento da Continuidade de Negócios.
4.4.7 Tornar clara a importância da realização de exercícios.

5. Legislação e regulamentação (10%)

5.1 Legislação e regulamentos (10%)

O candidato entende a importância e os efeitos da legislação e regulamentações.
O candidato é capaz de:
5.1.1 Explicar porque a legislação e as regulamentações são importantes para a confiabilidade da informação.
5.1.2 Dar exemplos de legislação relacionada à segurança da informação.
5.1.3 Dar exemplos de regulamentações relacionadas à segurança da informação.
5.1.4 Indicar as medidas possíveis que podem ser tomadas para cumprir as exigências da legislação e regulamentação.

Justificativa de escolhas

Conceitos gerais de TI tais como Big Data, Cloud e Teleworking (trabalho remoto/à distância) também devem ser parte dos conhecimentos gerais dos candidatos. Requisitos para o exame: justificativa da distribuição de peso.

As medidas de segurança são, para a maioria do pessoal, os primeiros aspectos de Segurança da Informação que essas pessoas encontram. Consequentemente, as medidas são fundamentais para o módulo e têm o maior peso. A seguir, ameaças e riscos em termos de peso. Finalmente, a percepção da política, organização e legislação e regulamentação na área de Segurança da Informação são necessárias para compreender a importância das medidas de Segurança da Informação.

Lista de conceitos básicos

Este capítulo contém os termos com os quais os candidatos devem mostrar familiaridade. Os termos estão listados em ordem alfabética.

Acordo de confidencialidade	Non-disclosure agreement
Ameaça	Threat
Análise da Informação	Information analysis
Análise de Risco	Risk Analysis
Análise de risco qualitativa	Qualitative risk analysis
Análise quantitativa de risco	Quantitative risk analysis
Arquitetura da Informação	Information Architecture
Assinatura Digital	Digital Signature
Ativo	Asset
Ativos de Negócios	Business Assets
Auditoria	Audit

ISO 27002

Autenticação	Authentication
Autenticidade	Authenticity
Autorização	Authorization
Avaliação de Riscos (análise de dependência e vulnerabilidade)	Risk Assessment (Dependency & Vulnerability analysis)
Backup (Cópia de segurança)	Backup
Big Data (Grandes dados)	Big Data
Biometria	Biometrics
Botnet	Botnet
BYOD	BYOD (Bring your own device)
Categoria	Category
Certificado	Certificate
Chave	Key
Ciclo de Incidentes	Incident Cycle
Classificação	Classification
Código de boas práticas de segurança da informação (ISO/IEC 27002:2013)	Code of practice for information security (ISO/IEC 27002:2013)
Código de conduta	Code of conduct
Completeza	Completeness
Confiabilidade das informações	Reliability of information
Confidencialidade	Confidentiality

ISO 27002

Confiabilidade das informações	Reliability of information
Confidencialidade	Confidentiality
Conformidade	Compliance
Continuidade	Continuity
Medidas	Controls
Controle de Acesso	Access Control
Corretiva	Corrective
Criptografia	Encryption
Dados	Data
Danos • Danos diretos • Danos indiretos	Damage • Direct damage • Indirect damage
Desastre	Disaster
Detectivo	Detective
Disponibilidade	Availability
Engenharia Social	Social Engineering
Escalação • Escalação funcional • Escalação hierárquica	Escalation • Functional escalation • Hierarchical escalation

ISO 27002

Estratégia de Risco • Reter riscos • Evitar riscos • Redução de riscos	Risk Strategy • Risk bearing • Risk avoiding • Risk reduction
Evento de segurança	Security event
Exatidão	Correctness
Exclusividade	Exclusivity
Fator de produção	Production factor
Firewall pessoal	Personal Firewall
Fornecedor Ininterrupto de Energia (UPS-Uninterruptible Power Supply)	Uninterruptible power supply(UPS)
Gerenciamento da Continuidade de Negócios (GCN)	Business Continuity Management (BCM)
Gerenciamento da Informação	Information management
Gerenciamento da Mudança	Change Management
Gerenciamento de acesso lógico	Logical Access Management
Gerenciamento de ativos de negócios	Managing business assets
Gerenciamento de riscos	Risk Management
Hacking	Hacking
Hoax	Hoax
Identificação	Identification

ISO 27002

Impacto	Impact
Incidente de Segurança	Security incident
Informação	Information
Informações secretas de autenticação	Secret authentication information
Infraestrutura	Infrastructure
Infraestrutura de chave pública (ICP)	Public Key Infrastructure (PKI)
Integridade	Integrity
Interferência	Interference
· ISO/IEC 27001:2013	· ISO/IEC 27001:2013
· ISO/IEC 27002:2013	· ISO/IEC 27002:2013
Legislação de direitos autorais	Copyright legislation
Legislação sobre Crimes de Informática	Computer criminality legislation
Legislação sobre proteção de dados pessoais	Personal data protection legislation
Legislação sobre registros públicos	Public records legislation
Malware	Malware
Medida de segurança	Security measure
Meio de armazenamento	Storage Medium
Não-repúdio	Non-repudiation
Nuvem	Cloud

ISO 27002

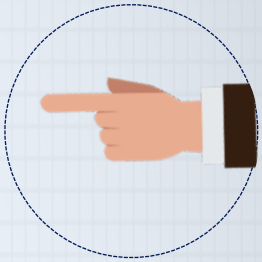
Oportunidade	Opportunity
Organização de Segurança	Security organization
Patch	Patch
Phishing	Phishing
Plano de Continuidade de Negócios (PCN)	Business Continuity Plan (BCP)
Plano de Recuperação de Desastre (PRD)	Disaster Recovery Plan (DRP)
Política de mesa limpa	Clear desk policy
Política de Privacidade	Privacy policy
Política de Segurança	Security policy
Porta de Manutenção	Maintenance door
Precisão	Precision
Preventiva	Preventive
Prioridade	Priority
Provisionamento de acesso do usuário	User access provisioning
Rede privada virtual (RPV)	Virtual Private Network (VPN)
Redutiva	Reductive
Redundância	Redundancy
Regulamentação de segurança para informações especiais p/ o governo	Security regulations for special information for the government
Repressiva	Repressive

ISO 27002

Revisão da segurança da informação	Information security review
Risco	Risk
Robustez	Robustness
Rootkit	Rootkit
Segregação de funções	Segregation of duties
Segurança em desenvolvimento	Security in development
Sistema de Informação	Information system
Sistema de Detecção de Intrusos (IDS)	Intrusion Detection System (IDS)
Spyware	Spyware
Stand-by	Stand-by arrangement
Teste de aceitação do sistema	System acceptance testing
Trabalho remoto/à distância	Teleworking
Trojan	Trojan
Urgência	Urgency
Validação	Validation
Verificação	Verification
Vírus	Virus
Vulnerabilidade	Vulnerability
Worm	Worm

ISO 27002

IV – Glossário



Termos e definições

Ativo: qualquer coisa que tenha valor para a organização.
Acordo de Não Divulgação: Veja Non-disclosure agreement (NDA).
Algoritmo: uma seqüência de instruções finita, muitas vezes usada para processamento de dados e cálculo.
Ameaça: qualquer coisa (o homem fez ou ato da natureza), que tem o potencial de causar danos. A probabilidade de uma ameaça vai usar uma vulnerabilidade para causar danos e cria um risco.
Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
Ativos de Negócio: tudo de valor que é de propriedade de uma empresa (exemplos: informação, softwares, equipamentos, mídia, serviços, pessoas e seus conhecimentos, mas também a reputação da organização).
Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco.
Análise/avaliação de riscos: processo completo de análise e avaliação de riscos.
Avaliação de riscos: processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco.
Bomba Lógica: Veja Logic Bomb.
Botnets: uma rede de computadores infectados. Veja Storm Worm botnet.
Carregar o Risco: uma estratégia de risco, nas quais certos riscos são aceitos, por exemplo, porque os custos das medidas de segurança são superiores aos possíveis danos.
Chave Pública: 5 seconds - Veja Public Key Infrastructure (PKI).
Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle é também usado como um sinônimo para proteção ou contramedida.
Compliance: Veja Conformidade.
Confiabilidade: a exigência de qualidade que abranje a confidencialidade, integridade e disponibilidade de informações (chamados de requisitos "CIA").
Confidencialidade: o grau em que o acesso à informação é restrito a um grupo definido de pessoas autorizadas. Isso também inclui medidas para proteção da privacidade.

ISO 27002

Conformidade: pode ser descrito como rastreabilidade, obrigatoriedade, flexibilidade, tolerância e dedicação. A empresa deve observar os regulamentos internos, bem como as leis do país e as exigências da legislação local.

Continuidade dos Sistemas: a disponibilidade de sistemas de informação no momento em que eles são necessários.

Crimeware: uma classe de softwares maliciosos projetados para se infiltrar ou danificar um sistema, projetado especificamente para automatizar os crimes financeiros.

Criptografia: o processo de transformar informação (referido como um texto simples) usando um algoritmo para torná-la ilegível para qualquer um, exceto os que possuem processos especiais, normalmente referida como uma chave.

Desastre: um grande incidente na qual a continuidade da empresa está ameaçada. Também o fato do sistema sobre o qual você depende muito no seu trabalho diário, está com problemas técnicos.

Diretriz: descrição que orienta o que deve ser feito e como, para se alcançarem os objetivos estabelecidos nas políticas.

Disponibilidade: o grau em que a informação está disponível para o usuário e para o sistema de informação que está em operação no momento que a organização requerer.

E-commerce: a compra e venda de produtos ou serviços através de sistemas eletrônicos, tais como a Internet e outras redes informáticas.

Energia Limpa: refere-se à prevenção de picos e quedas (energia suja) no fornecimento de energia.

Escalação Funcional: (Horizontal) o envolvimento de pessoal com conhecimentos mais especializados, tempo ou privilégios de acesso (serviço técnico) para resolver um incidente.

Escalação Hierárquica: que envolvem um maior nível de autoridade dentro da organização, quando parece que o atual nível de autoridade é insuficiente para garantir que o incidente seja resolvido a tempo e/ou de forma satisfatória.

Evitar o Risco: uma estratégia de risco em que sejam tomadas medidas para neutralizar a ameaça a tal medida em que a ameaça já não conduz a um incidente.

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Firewall: um conjunto integrado de segurança técnica e medidas destinadas a evitar acesso eletrônico não autorizado a um sistema informático em uma rede.

Gestão de riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. A gestão de riscos geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

ISO 27002

Gerenciamento de acesso lógico: ele garante que as pessoas não autorizadas ou os processos, não tenham acesso aos sistemas automatizados, bases de dados e programas. Um usuário, por exemplo, não tem o direito de alterar as configurações do PC.

Hacker: Uma pessoa comprometida com a evasão de segurança do computador, principalmente com acesso não autorizado à um computador remoto via redes de comunicação como a Internet.

Incidente: qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção ou redução na qualidade desse serviço.

Incidente de Segurança da Informação: um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Infra-estrutura de TI: todos os ativos de tecnologia da informação (hardware, software, dados), componentes sistemas, aplicações e recursos.

Infra-estutura de chave públca: Veja Chave Pública.

Integridade: o grau em que a informação está atualizada e sem erros. A características de integridade são a correção e a integridade das informações.

Logic Bomb: um pedaço de código intencionalmente inseridas em um sistema de software que irá desencadear uma função maliciosa quando as condições especificadas forem satisfeitas.

Malware: software desenhado para infiltrar ou danificar um sistema de computador sem que o proprietário seja informado.

Neutralizar o Risco: uma estratégia de risco em que sejam tomadas medidas de modo que as ameaças ou não já se manifestam, ou, se o fizerem, o dano resultante é minimizado.

Non-disclosure agreement (NDA): um contrato através do qual as partes concordam em não divulgar informação coberta pelo acordo. Um NDA cria um relacionamento confidencial entre as partes para proteger qualquer tipo de informações confidenciais e proprietárias ou um segredo comercial. Como tal, um NDA protege as informações de negócios não públicas.

Política: intenções e diretrizes globais formalmente expressas pela direção.

Patch: um pequeno pedaço de software projetado para corrigir problemas com a atualização ou um programa de computador.

Phishing: uma forma de fraude na internet, na tentativa de adquirir informações sensíveis, tais como nomes de usuários, senhas e detalhes de cartão.

Public Key Infrastructure (PKI): um conjunto de hardware, software, pessoas, políticas e procedimentos necessárias para criar, gerenciar, armazenar, distribuir e revogar certificados digitais.

ISO 27002

Risco: possíveis danos ou perda de informações; combinação da probabilidade de um evento e de suas consequências.

Rootkit: um conjunto de ferramentas de software que são frequentemente utilizados por terceiros (geralmente um hacker), após ter tido o acesso a um sistema (de computador). O rootkit se esconde no computador e possivelmente resultando na instabilidade do sistema operacional.

Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

Segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Segregação de Funções: define a pessoa para uma tomada de decisão, tarefas executivas ou de controles para evitar a possibilidade de alteração não autorizada, involuntária ou o uso indevido de ativos da organização. É determinado se a pessoa precisa ter acesso a da informação. Acesso desnecessário aumenta o risco das informações serem intencionalmente ou inadvertidamente utilizados, alterados ou destruídos.

Spam: um nome coletivo para mensagens indesejadas. O termo é normalmente utilizado para o e-mail indesejado, mas as mensagens de publicidade indesejada em sites também são consideradas como spam.

Spyware: um programa de computador que recolhe informações sobre o usuário do computador e envia estas informações para outro lugar. O objetivo disso é ganhar dinheiro. O Spyware não tenta danificar o PC e / ou o software instalado, mas sim de violar a privacidade.

Stand-by: uma medida repressiva, em que os recursos sejam colocados em serviço em caráter de urgência em caso de um desastre. Por exemplo, usando um local diferente, a fim de continuar o trabalho.

Storm Worm botnet: uma rede de computadores controlada remotamente "zumbis" (ou "botnet") que estão relacionados pelo Storm Worm, um cavalo de Tróia distribuído por meio de um spam.

Tratamento do risco: processo de seleção e implementação de medidas para modificar um risco.

Terceira parte: pessoa ou organismo reconhecido como independente das partes envolvidas, no que se refere a um dado assunto.

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.