Gestão da segurança do data center

Gestão de segurança em data center e seus procedimentos e protocolos de segurança, com gestão de riscos aplicada no ambiente.

Prof.ª Julio Cesar Ribeiro de Lima Gonçalves

1. Itens iniciais

Propósito

Realizar a gestão de segurança de um data center exige grande responsabilidade de todos os profissionais da área de operação e, por isso, conhecer e cumprir a política de segurança é fundamental.

Objetivos

- Identificar os conceitos básicos da gestão de segurança e das normas de implementação da política de segurança.
- Analisar protocolos e procedimentos operacionais de segurança.
- Descrever como é realizada a gestão de risco.

Introdução

Gerir a segurança da informação é muito importante em qualquer corporação, empresa ou órgão governamental que utiliza TI (Tecnologia da informação) como seu principal serviço ou como um dos pilares estratégicos do negócio. A prevenção é a forma mais eficaz contra desastres, como perda, sequestro de dados e ataques cibernéticos aos seus serviços e equipamentos. Essas são apenas algumas das grandes preocupações dos gestores de segurança da informação.

Os ataques feitos pela internet são os mais comuns. Entretanto, ataques físicos à infraestrutura de TI também podem ocorrer. Assim, a camada de segurança física nas instalações do data center precisa ser intransponível para as ameaças e será foco do estudo.

Quando falamos do data center, ambiente composto de equipamentos que disponibilizam sistemas críticos para a organização, concluímos que a camada de segurança deve ser primordial para garantir o funcionamento e a integridade, incluindo a segurança física e lógica em todos os seus ambientes, juntamente com o controle de acesso a todas as áreas críticas.

A camada de segurança é criada de acordo com definição da política de segurança da empresa, que dita como será a segurança em cada área, quais os protocolos e como esses protocolos de segurança serão obedecidos pelos funcionários da empresa e funcionários terceirizados.

Como exemplo, algumas empresas proíbem a realização de visitas às suas instalações e até mesmo a visita de funcionários não envolvidos com a operação do data center, garantindo que a segurança seja implantada em todas as camadas do ambiente da forma mais rígida possível.

Por essas razões, no local de instalação de um data center existirá grande quantidade de dispositivos de segurança como: câmeras, cercas de proteção, portões controlados por guardas de segurança, além de mais outras camadas, estabelecendo perímetros de segurança, até se chegar ao local em que os servidores estão instalados. Além disso, tudo é monitorado durante 24 horas, sete dias por semana por uma equipe especializada.

Introdução

Realizar a gestão de segurança de um data center é uma das grandes preocupações entre todas as organizações. A utilização desses ambientes cresce a cada ano, com o aumento da oferta de novos serviços.

Espalhados em locais estratégicos ao redor do mundo, os data centers centralizam milhares dados, informações, aplicações e serviços para diversas empresas e usuários e, por isso, são o alvo principal de criminosos digitais que, a cada dia, lançam inúmeras de tentativas de ataque aos serviços hospedados. Os criminosos digitais podem ter as seguintes motivações:

Causar a indisponibilidade dos serviços

Ataque que pode interromper a operação das empresas e de seus clientes, consequentemente causando prejuízo.

Obter informações estratégicas

Essas informações podem ser usadas por competidores.

Sequestrar dados

Ataque que consiste em criptografar as informações contidas em um servidor para extorquir dinheiro, pedindo resgate.

Esses são exemplos de ataques lógicos. Em alguns casos, os ataques podem ser físicos, isto é, o alvo são as instalações dos data centers e os sistemas auxiliares que mantêm o funcionamento, como sistemas elétricos, sistemas de telecomunicações, entre outros.

> Para evitar ataques, a gestão da segurança da informação, que inclui a área do data center, deve prever todos os tipos de situações, por meio de uma política de segurança.

Normas aplicadas

Fazer uma gestão da segurança da informação de forma eficiente garante benefícios, desde o total conhecimento das operações realizadas em sua infraestrutura, até a garantia da proteção de dados e informações estratégicas da empresa e dos seus clientes. Os benefícios vão além da conformidade com as normas, a empresa pode capitalizar com a gestão adequada ofertada. Também é preciso garantir que políticas, processos, hardwares e softwares atendam às necessidades, considerando todos os riscos das atividades do negócio.

Segurança da informação.

> Para que todas as regras sejam cumpridas de forma eficiente, as normas da segurança devem ser seguidas com a fiel observância de controles, regras e diretrizes.

Todo o time de Tecnologia da Informação usa como um guia de boas práticas as recomendações do conjunto de normas **ISO/IEC da série 27000**. Especificamente, para o ambiente de data center, aplica-se a norma ISO/IEC 27001:2013.

Essa norma segue os padrões estabelecidos pela ISO, sendo um modelo para que as empresas com data center garantam que suas infraestruturas e seus serviços, além da gestão da segurança da informação, estejam de acordo com os padrões estabelecidos. A norma tem como objetivo garantir os pontos essenciais para os sistemas corporativos seguros:

- Integridade dos dados
- Confidencialidade dos dados
- Disponibilidade dos dados

A norma também visa definir o modelo de gestão de riscos, com a aplicação de controles, monitoramento e revisões. Essa é uma das maneiras de implementar, monitorar e estabelecer objetivos tangíveis, criando uma lista com diversas opções e sugestões de segurança da informação, que será aplicada à política de segurança, conforme a necessidade.

Como obter a certificação ISO/IEC 27001:2013

ISO/IEC 27001:2013.

Qualquer empresa ou entidade governamental que deseja obter a certificação da norma deverá passar por processos de auditorias. As auditorias são realizadas por entidades certificadoras habilitadas pela ISO, em que são verificados todos os processos e as conformidades com a norma, observando as especificidades de cada organização.

O processo de auditoria inclui a verificação das diretrizes padrão contidas na norma, a análise da documentação dos processos de segurança e a realização de auditorias internas para busca de inconformidades nos processos. Após esse primeiro passo, a empresa terá um prazo para fazer as adequações necessárias e, em seguida, uma auditoria final, externa, para a obtenção do certificado.

Benefícios no uso da norma ISO/IEC 27001:2013

A norma ISO/IEC 27001:2013 apresenta os seguintes benefícios:

- Mais garantia de segurança para a rede corporativa da empresa;
- Diferencial para clientes que procuram empresas certificadas;
- Redução de custos na prevenção de incidentes de segurança da informação;
- Mais organização, controle e produtividade;
- Conformidade com requisitos legais;
- Maior valor de mercado, em divulgações e diferenciação em negociações.

Norma NIST SP 800-53

Outra norma bastante utilizada para a criação da política de segurança é a norma Internacional **NIST SP 800-53** que apresenta controles de segurança recomendados pelo National Institute of Standards Technology (NIST), o Instituto Nacional de Padrões Tecnológico. Essa norma é utilizada em conjunto com a ISO 27001, para projetar e implementar os controles de segurança da empresa.

Controles da segurança da informação.

A norma NIST SP 800-53 fornece um catálogo com diversos controles de segurança e privacidade para os sistemas de informação, visando proteger as operações, os ativos da empresa e funcionários de um conjunto de ameaças e riscos, incluindo ataques hostis, erros provocados por funcionários, catástrofes da natureza, falhas estruturais, ações de agências de inteligência, grupos terroristas e cibercriminosos.

Atenção

Os controles são flexíveis e personalizáveis e devem ser implementados como parte do processo de toda a organização para gerenciar riscos. Esses controles devem atender a diversos requisitos e necessidades de negócios, além de leis, ordens executivas, diretivas, regulamentos, políticas, padrões e diretrizes.

Papel das normas

A aplicação das normas tem um papel muito forte na tomada de decisão para implantação da política e a gestão de segurança. Oferece de forma simples, porém eficaz, a mitigação dos riscos sobre seus ativos de TI. Sua implantação estabelece um *framework* de privacidade e é feita em três partes:

Núcleo

Representa um conjunto de boas práticas de segurança cibernética, com resultados e controles de segurança de caráter técnicos, operacionais e gerenciais (conhecidos como referências informativas) suportando as cinco funções no gerenciamento de riscos: Identificar, Proteger, Detectar, Responder e Recuperar.

Níveis

Caracterizam a aptidão e a maturidade de uma empresa em gerenciar funções e controles.

Perfis

Têm o objetivo de apoiar a decisão e comunicar as medidas de segurança cibernética atuais e planejadas para a empresa.

Juntas, as três partes permitem que a empresa priorize e aborde os riscos de segurança cibernética, de acordo com as suas necessidades de negócios e missão.

As normas são usadas para definir quais são as melhores práticas que devem ser adotadas na gestão de segurança. Na maioria das políticas de segurança implantadas, são encontrados alguns padrões definidos como essenciais para a gestão da segurança.

Políticas de segurança padrão em data centers

As políticas de segurança padrão em data centers devem incluir a análise de diversos fatores. Veremos os principais a seguir.

Segurança física

Quando pensamos na segurança de um data center, os primeiros pontos são a criação e implantação dos perímetros de segurança. Cada uma dessas camadas possui uma série de dispositivos de segurança, como a utilização de guardas de segurança, cercas e circuito fechado de TV (CFTV), além do uso de tecnologias avançadas de detecção de intrusão, seguindo à risca as políticas de segurança implantadas e os protocolos de segurança.

Perímetros de Segurança.

Controle de acesso

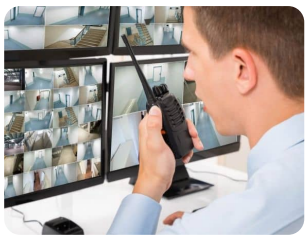
O controle de acesso ao data center é realizado visando que apenas pessoas autorizadas consigam o acesso ao ambiente. Em cada solicitação de acesso devem ser detalhadas quais atividades serão realizadas, estabelecendo-se os locais de acesso e a circulação, bem como uma estimativa de tempo de permanência do funcionário nas instalações do data center.

> O acesso ao data center sempre será temporário, sendo revogado após a finalização das atividades do funcionário.

Para acessar o datacenter, o funcionário precisa passar por algumas etapas:

Identificação e validação

Quando o funcionário chega ao data center, ele é recebido por guardas de segurança que fazem parte da equipe de segurança patrimonial do data center. Eles atuam nas rondas e, também, na identificação e validação de funcionários nos portões de entrada do primeiro perímetro de segurança. Tudo deve ser monitorado por supervisores de segurança, por meio de câmeras.



Autenticação multifator

O funcionário recebe um crachá e a próxima etapa é a autenticação multifator, com mais de uma maneira de provar que o funcionário é ele mesmo. Geralmente, são utilizados sistemas de biometria, leitor facial e senhas. O sistema de autenticação valida o funcionário, liberando o seu acesso.

Liberação das portas

Após vencer o primeiro perímetro, o funcionário ingressa nos locais onde tem a permissão de entrar, bastando apenas utilizar o sistema de controle de acesso para liberação das portas. Lembre-se de que o trânsito é por tempo limitado e exclusivo para os locais dentro do data center que foram aprovados na solicitação inicial.

Vejamos um caso concreto de como esse processo acontece.

Nos data centers da AWS (Amazon Web Services), esse processo é aplicado tanto para funcionários próprios quanto para funcionários de empresas terceirizadas. Os funcionários que necessitam entrar de forma rotineiramente em um dos data centers da AWS recebem permissões apenas para as áreas em que irão trabalhar, de acordo com suas funções.

As permissões são revisadas rotineiramente, a fim de garantir que sejam revogadas assim que o funcionário não necessite mais acesso àquele determinado local. Geralmente, esse modelo de permissão é feito quando novos sistemas estão sendo instalados na infraestrutura do data center, seja ela física ou lógica.

O monitoramento de todos os perímetros é realizado de forma intensa, por uma equipe de supervisão, utilizando sistemas de CFTV, sensores de detecção de intrusão e processamento analítico de imagem. As informações obtidas por esses sensores são cruzadas com o objetivo de realizar o registro de todos os acessos e eventos ocorridos.

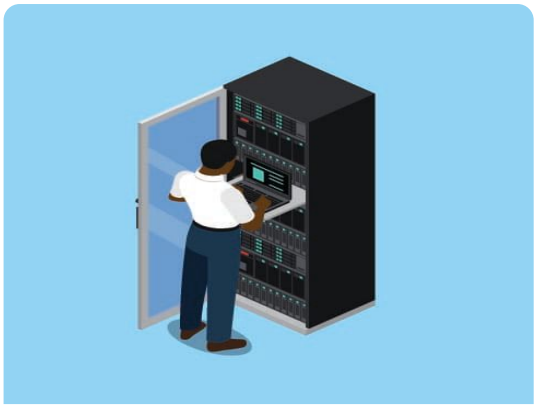
Todas as portas nas instalações dos data centers devem possuir sensores e alarmes ligados à central de monitoramento. Em caso de tentativa de violação ou de portas deixadas abertas após a passagem de uma pessoa autorizada, a central deve ser notificada e o protocolo prevenção de risco é acionado imediatamente.

Resumindo

A central presta o suporte em todos os perímetros da área de segurança, realizando monitoramento de forma contínua, durante 24 horas, sete dias por semana, monitorando, rastreando e prevenindo a segurança e controlando o acesso, a revogação de permissões e disponibilizando relatórios para análise e respostas a possíveis incidentes de segurança.

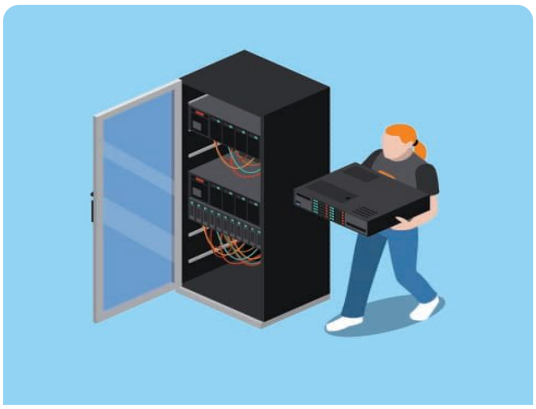
Segurança dos equipamentos

Protege contra perda, dano, furto e interrupção de ativos e das atividades do data center. Deve ser composta por medidas rígidas de segurança adotadas para que não sejam retirados equipamentos dos ambientes, nem sejam inseridos equipamentos sem autorização. A remoção ou a inclusão de equipamentos pode comprometer a infraestrutura e a operação de algum sistema do data center.



Gestão de capacidade

Realiza as métricas de utilização dos recursos nos equipamentos de processamento



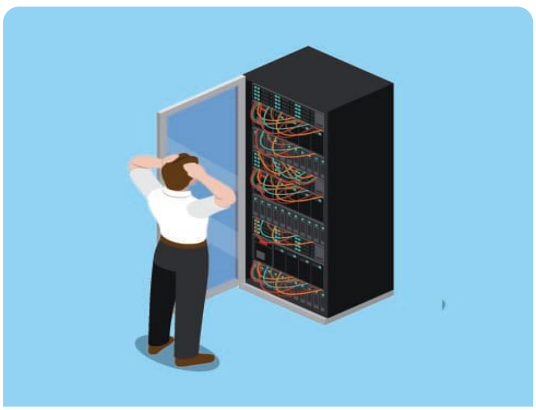
(servidores) e armazenamento (*storages*). Deve ser monitorada constantemente. As projeções de expansão devem ser feitas para estabelecer as necessidades de capacidade futura, garantindo o desempenho dos sistemas e ajudando na previsão de novos investimentos dos recursos computacionais do ambiente do data center.

Instalação

Os equipamentos devem ser instalados em racks (armários próprios para servidores) instalados em uma sala protegida, reduzindo os riscos de ameaças de outras áreas do data center, bem como as oportunidades de acesso não autorizado. Muitos racks podem ter controle de acesso, em que apenas funcionários previamente autorizados terão acesso.

Cabeamento

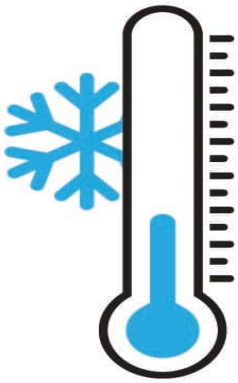
O cabeamento elétrico que energiza os equipamentos e os cabos de telecomunicações que transportam o tráfego de dados devem ser protegidos contra vandalismo, dano e roubo. Isso deve ocorrer principalmente fora do perímetro de segurança, caso a fibra seja de propriedade da empresa proprietária do data center.



Dica

No caso de operadora de telecomunicações, a empresa deve exigir a garantia dessas proteções em alguns quilômetros antes de chegarem ao data center. Essas exigências são consideradas medidas protetivas para evitar ataques físicos às infraestruturas críticas de funcionamento do data center.

Refrigeração



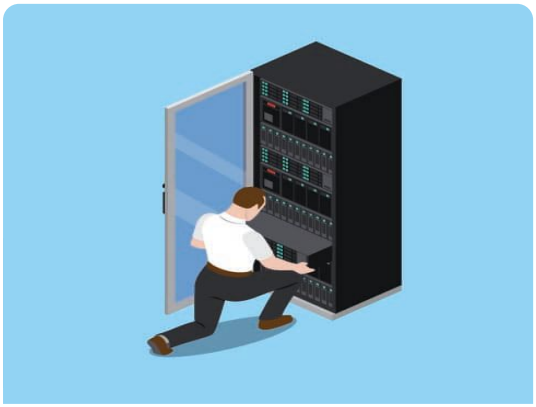
O sistema de refrigeração do ambiente do data center, onde estão instalados os equipamentos de processamento e armazenamento, é o segundo sistema mais crítico. Esse sistema tem que garantir uma temperatura constante entre 19°C e 25°C dentro do ambiente. Geralmente, são usados sistemas duplos independentes e redundantes, com controle digital permanente de temperatura e umidade dos ambientes.

Energia

O sistema elétrico é o sistema mais crítico de um data center. O fornecimento elétrico é feito por concessionárias de energia, distribuído em cabos de alta tensão para as subestações elétricas nos data centers, indo até a área dos *Uninterruptible Power Supply* (UPS) ou fonte de energia ininterrupta.

Os UPS são equipamentos responsáveis pela alimentação elétrica para os equipamentos dentro das salas de computadores nos data centers, tolerantes a falhas elétricas e outras interrupções causadas por falta de alimentação elétrica, utilizando módulos de baterias como redundância em tempo zero e funcionando até que as fontes de energia auxiliar, como geradores ou outra fonte independente de energia, entrem em atividade quando o fornecimento falha. Isso garante que distribuição da energia, dentro das áreas do data center, será contínua, estabilizada e ininterrupta. Os UPS são monitorados em tempo real por sistemas inteligentes.

Manutenções



As manutenções devem ser realizadas em todas as infraestruturas que compõem o data center. Manutenções em equipamentos de processamento e armazenamento, em período de garantia, somente poderão ser realizadas pela assistência técnica autorizada. Todo evento produzido nas manutenções deverá ser transcrito no sistema que controla os equipamentos instalados no data center.

Não são permitidas a entrada e a saída de peças, equipamentos e acessórios da sala de computadores sem o prévio conhecimento e autorização.

Tanto a entrada quanto a retirada de qualquer equipamento das instalações do data center serão feitas apenas com o preenchimento do pedido de solicitação de entrada ou retirada do dispositivo, pelo funcionário, para a gerência de controle de ativos e segurança do data center.

Segurança lógica

A segurança lógica é a responsável pela proteção dos sistemas de controle em um data center, além dos serviços prestados aos clientes. Essas proteções são feitas por softwares, dispositivos próprios de segurança com regras de restrições de acesso. Ela também realiza a proteção contra os ataques de criminosos digitais, bem como contra erros não intencionais, como, por exemplo, a remoção acidental de arquivos de um sistema.

⚠

Atenção

A utilização dos recursos tecnológicos nos processos, de soluções de firewalls, antivírus, antispam, entre outros, é praticamente indispensável.

Principais riscos à segurança lógica

As ameaças tratadas pela segurança lógica estão ligadas, em sua maioria, aos acessos indevidos, erros provocados e à perda dos dados por conta de erros, falhas na rede provocadas por softwares programados para esse propósito, fraudes e sabotagens.

A seguir, temos os principais riscos à segurança lógica:

Perda de confidencialidade

É uma quebra de sigilo, permitindo que sejam expostas as informações restritas, acessíveis apenas por um grupo determinado de usuários.

Perda de integridade

É quando uma informação fica exposta e pode ser manuseada por mais de uma pessoa não autorizada.

Perda de disponibilidade

É quando uma informação deixa de estar acessível pelos usuários que necessitam dela.

Segurança física e os subsistemas do datacenter

No vídeo a seguir, explicaremos como a falta de uma política de segurança bem definida pode interferir nos subsistemas do datacenter, principalmente, nos subsistemas de energia elétrica, ar-condicionado, rede e na segurança dos dados.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vem que eu te explico!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Segurança física

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Segurança lógica

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Qual a principal providência para prover segurança física em um data center?

A

Instalar um circuito fechado de TV.

B

Estabelecer os perímetros de segurança.

C

Instalar um alarme de invasão.

D

Instalar um sistema de detecção e combate a incêndio.

E

Contratar uma empresa de vigilância.

A alternativa B está correta.

Os perímetros de segurança são os conjuntos de medidas que visam definir quem pode e quem não pode acessar as instalações. Com o estabelecimento dos perímetros de segurança, o acesso aos equipamentos é institucionalizado e impessoal.

Questão 2

Quais os principais riscos à segurança lógica de um data center?

A

Perda de confidencialidade, integridade e disponibilidade.

B

Danos nos equipamentos de TI.

C

Danos da rede elétrica.

D

Danos da rede de telecomunicações.

E

Ataques físicos, como, por exemplo, invasões.

A alternativa A está correta.

A segurança lógica diz respeito aos dados, então, a perda de confidencialidade, integridade e disponibilidade são os principais riscos para isso ocorrer.

Introdução

Neste módulo, abordaremos como são criados os procedimentos e protocolos de segurança para data centers e como são acionados e utilizados em eventuais ocorrências, incidentes, segurança e eventos de emergência. O objetivo é diminuir e evitar qualquer impacto nas organizações que criam esses protocolos.

Relembrando

Os data centers são ambientes de missão crítica, operando de modo contínuo.

Data center.

Independentemente do modelo e das operações realizadas nos data centers, é quase impossível eliminar todos os riscos de interrupção, sejam conhecidos ou inesperados, nas infraestruturas físicas e lógicas do data center.

Estar preparado para entrar em ação de forma eficaz e efetiva, em caso de início de um incidente, é essencial para a manutenção da disponibilidade. Essas ações visam minimizar ou evitar qualquer impacto nos negócios da empresa. A preparação demanda um conjunto de análises para antecipar, prevenir e diminuir os efeitos de incidentes e de eventos de emergência.

Protocolos de segurança

Toda organização deve providenciar a confecção dos protocolos a seguir. Esses protocolos visam mitigar ou evitar a ocorrência de eventos que impactem a continuidade da operação.

Procedimentos Operacionais de Emergência – Emergency Operating Procedures (EOP)

Visam garantir que as respostas sejam apropriadas, eficazes e sem falhas. A criação desses procedimentos começa com a análise dos subsistemas que podem faltar e representam alto risco de segurança para a operação do data center. Alguns exemplos são:

Falhas no funcionamento de um grupo gerador.

Falhas na distribuição elétrica.

Falhas em uma central de refrigeração na sala de computadores.

Os EOPs criam um plano de ação bem detalhado para isolar, com segurança, as falhas apresentadas nos sistemas e restaurar os serviços, ou acionar a redundância, quando possível e disponível. Esses procedimentos são desenvolvidos, aprovados e publicados. Também é importante que simulações sejam realizadas regularmente, com os objetivos de avaliar a eficácia da equipe na resposta à emergência e viabilizar o monitoramento da manutenção dos sistemas envolvidos.

Plano de Gestão de Crises – Crisis Management Plan (CMP)

No ambiente de data centers, uma variedade de situações de emergência são calculadas, assim como os procedimentos para resolvê-las. Os procedimentos são definidos, mas não é incomum que aconteçam eventos imprevistos. Quando um imprevisto ocorre, uma situação de crise é criada.

> Uma crise é uma situação de extrema dificuldade, que está fora do escopo das respostas preparadas e previstas no EOP.

As crises podem se estender por um longo período de tempo e se tornar ainda mais graves quando não são tratadas de forma coordenada, incluindo todos os colaboradores envolvidos. O objetivo principal do CMP é minimizar o seu impacto, por meio do plano de gestão de crises. Esse plano deverá ser desenvolvido pela equipe de operações em cooperação com a área de gestão de clientes.

Plano de Gestão de Crises.

As ações sobre quais procedimentos serão seguidos e o que fazer nesses casos devem ser bem detalhadas.

Continuidade do Negócio (Business Continuity) e Procedimentos de Recuperação de Desastres (Disaster Recovery Procedures)

Os procedimentos da continuidade de negócio e recuperação de desastres são partes importantes do plano de resposta de emergência e incidentes que será utilizado quando uma emergência for declarada. O plano deve ser de conhecimento obrigatório de coordenadores, equipes técnicas e gestores de todas as áreas do data center.

Os principais objetivos são:

Resguardar a vida, a saúde e a segurança de todas as pessoas.

Reprimir e conter danos às instalações e aos dispositivos.

Consolidar as operações e os serviços.

Gerenciar de forma eficaz os boletins com informações durante todo o incidente.

Os procedimentos de continuidade de negócios e recuperação de desastres, juntos, fornecem diversas orientações para realizar a recuperação de maneira rápida e eficaz após qualquer ocorrência que provoque uma avaria ou uso limitado de serviços e instalações do data center.

Todo plano de continuidade de negócio tem como principal objetivo diminuir o impacto financeiro e operacional de um incidente envolvendo a infraestrutura ou os sistemas. Esse plano prioriza todos os serviços considerados de missão crítica, que exigem imediata restauração, identificando os principais recursos e dependências. Esse documento deve guiar os planos de continuidade em cada um dos serviços categorizados e, também, informando o seu tempo de recuperação e o ponto de restauração disponibilizado.

Gerenciamento de incidentes

Para gerenciar de forma adequada as respostas às emergências, é necessária a criação de protocolos, garantindo que eventos abrangendo a segurança ou missão crítica sejam de conhecimento pela equipe apropriada — funcionários, contratados ou fornecedores.

Todos os incidentes precisam ser reportados imediatamente ao gestor de segurança, após a estabilização da situação. Uma descrição do incidente deve ser enviada para uma lista de distribuição, sua composição deverá ser definida pela gravidade de cada incidente ocorrido. O relatório deverá:

Ser completamente produzido e arquivado nas primeiras 24 horas após o incidente.

Conter uma descrição detalhada e em ordem cronológica dos fatos, além de todos os procedimentos realizados para estabilização e correção de cada fato.

Esse relatório é extremamente importante para as seguintes fases:

Fase de análise de falhas

O relatório será apreciado por um comitê formado pelos setores internos da empresa, para definir que tipo de falha ocorreu e onde foi gerada.

Fase de consolidação das lições aprendidas

A documentação da determinação da causa do incidente e de como evitá-lo no futuro.

O relatório também deve ser usado como ferramenta educacional nos treinamentos e referência para todos os locais atingidos.

Para responder aos mais distintos tipos de riscos e crises que possam ocorrer nos data centers, as empresas devem rapidamente agir de forma coordenada, além de saber como proceder em situações inesperadas. O método operacional correto evitará erros comuns e a piora da situação.

Atenção

O plano de preparação de respostas à emergência é o elemento fundamental para a adoção desse processo e abrange a integração de pessoas, os procedimentos e sistemas que levam os operadores de missão crítica a executarem ações de forma previsível e totalmente eficaz.

Protocolos EOP, CMP e BC/DR

No vídeo a seguir, abordaremos os protocolos EOP – Emergency Operating Procedures (Procedimentos Operacionais de Emergência), CMP – Crisis Management Plan (Plano de Gestão de Crises) e BC/DR – Business Continuity (Continuidade do Negócio)/Disaster Recovery – Procedures (Recuperação de Desastres – Procedimentos).

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vem que eu te explico!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Protocolos de segurança

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Gerenciamento de incidentes

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Qual a principal função do procedimento operacional de emergência?

A

Garantir respostas oportunas, eficazes e sem erros.

B

Ter uma resposta pronta para todas as situações esperadas.

C

Recuperar-se de erros causados por falhas operacionais.

D

Informar a gestão da segurança sobre procedimentos em situação de emergência.

E

Implantar rapidamente um segundo local para operação.

A alternativa A está correta.

Os procedimentos operacionais de emergência visam garantir respostas corretas e imediatas a problemas previsíveis. Por exemplo, a ativação do gerador em caso de falta de energia.

Questão 2

Como é descrita uma situação de crise em uma gestão de segurança?

A

Situação de extrema dificuldade que não está prevista no plano de respostas a incidentes.

B

Quando uma situação tem pequenos pontos em divergência, impedindo o entendimento das operações.

C

Situação em que algum indivíduo causou uma falha proposital.

D

Quando uma situação passou mais tempo para ser resolvida conforme o esperado.

E

Situação em que ocorre uma falha em um subsistema do data center, como, por exemplo, energia elétrica.

A alternativa A está correta.

Uma crise é uma situação não prevista, de longa duração, fora do previsto nos procedimentos operacionais de emergência. Uma crise pode ter grande impacto na operação do negócio e até mesmo inviabilizar o negócio.

Introdução

Neste módulo, abordaremos a gestão de riscos, que é o conjunto de atividades com o objetivo implantar controles em uma empresa para mitigar o impacto de prováveis incidentes. Sua implantação racionaliza o uso dos recursos humanos e materiais para diminuir os riscos, realizando os devidos tratamentos preventivos.

Uma estratégia é antecipar as possíveis situações de risco e tratá-las como processo da empresa. Entretanto, imprevistos acontecem e, nesse caso, atua-se de maneira prescritiva, isto é, tratando-o quando o risco aparece sem ter sido previsto.

Gestão de riscos.

Conceito da gestão de riscos

A gestão de risco procura estimular um comportamento ativo entre os gestores da empresa, respondendo com agilidade a eventos, dúvidas e alterações de cenário. Para que isso tudo seja possível, é essencial o uso de um sistema de monitoramento de indicadores associados aos riscos e às suas ocorrências. O objetivo final é a melhoria contínua nos processos da empresa.

A gestão de riscos de segurança é o processo da gestão organizacional que motiva a aplicação de controles de segurança diante dos perfis de riscos. A norma ISO/IEC 27005 é adotada e prescreve a sua implantação. A norma tem a finalidade de apresentar:

Definição de processos

Para a gestão de risco e de segurança da informação.

Guia para gestão de risco

Pode ser usado em empresas, projetos, ciclos de melhoria contínua etc.

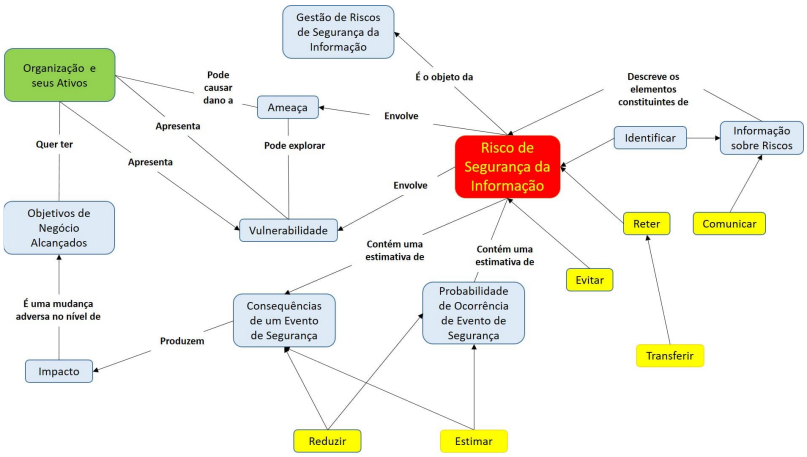
Guia para o desenvolvimento de práticas e metodologias

Para atender às obrigações e à gestão de riscos constantes da norma ABNT NBR ISO/IEC 27001:2006.

Norma de conformidade

Entre muitas normas e outros métodos de gestão de riscos no mundo.

A imagem a seguir apresenta um mapa conceitual geral sobre o qual se sustenta a norma 27005:



Mapa conceitual sobre gestão de riscos de segurança.

Os dados e conceitos básicos visualizados na imagem são determinados a seguir:

1

Organização

Uma empresa que possui um conjunto de ativos.

2

Impacto

Mudança avessa no nível de objetivos de negócios adquiridos.

3

Ameaça

Motivo aceitável de um imprevisto indesejado, que pode resultar em dano para um sistema ou uma empresa.

4

Ativo

Qualquer coisa de valor para uma organização. Um ativo é um elemento da empresa, pode ser qualquer elemento tangível, como seus subsistemas, ou intangível, como marca comercial, dados e informações da empresa.

5

Evento de seg. da informação

Ocorrência identificada de uma alteração de estado em um sistema, serviço ou rede, sugerindo uma possível violação da PSI da empresa, falha de controles ou uma situação desconhecida, que pode ser bastante relevante para a segurança da informação.

6

Consequência de um evento de segurança

Variação contrária no nível de um objetivo de segurança devido a um acontecimento. São os principais objetivos de segurança: confidencialidade, integridade, disponibilidade e autenticidade.

7 Vulnerabilidade

É uma característica de construção do hardware (conjunto de peças) ou software (aplicações ou programas de computador) de um ativo ou grupo de ativos, que podem ser explorados por uma ou mais ameaças.

8

Risco de segurança da informação

O potencial que uma exploração de vulnerabilidades ameace um ativo ou conjunto de ativos e, dessa maneira, prejudique uma empresa. Um risco é mensurado em termos de probabilidade de consolidação do risco e de seus impactos.

9

Evitar o risco

A disposição de não se envolver em uma situação de risco ou de sair dela.

10

Comunicar o risco

A troca ou o compartilhamento de comunicação sobre risco entre um tomador de decisão e outras pessoas de interesse.

11

Estimar o risco

Processo de atribuir valores às possibilidades e consequências de um risco.

12

Identificar o risco

Processo de descobrir, listar e diferenciar elementos do risco.

13

Reduzir o risco

Conjunto de ações adotadas para reduzir a possibilidade de episódio ou resultados negativos, ou ambos, associadas a um risco.

14

Reter o risco

A aceitação do encargo da perda ou o melhoramento dos rendimentos ocorridos de um risco em particular.

15 Transferir o risco

É compartilhar com outro parceiro o encargo da perda ou o melhoramento do resultado, associado a um risco.

Saiba mais

PSI significa política de segurança da informação.

A partir das definições dadas, podemos deduzir, entre outras coisas, que o conceito de ativo é fundamental para a gestão de riscos. Os ativos são os elementos expostos aos riscos, assim, a identificação dos riscos envolve a coleta de dados sobre fatores como ativos, ameaças, vulnerabilidades, probabilidades, consequências e impactos.

Ativos de informação

Devido às especificidades de cada organização, a norma é bastante genérica quando mencionamos quais seriam os ativos expostos aos riscos. A norma traz uma disposição primária dos ativos entre ativos principais e de suporte. Os ativos primários apoiam-se nos ativos de apoio.

Classificação de ativos

São ativos principais de uma organização:

Processos e atividades do negócio

São executados visando à performance das funções da empresa. Processos são os meios que mais agregam valor à organização.

Informações

São usadas no apoio ao cumprimento desses processos, além das de modo pessoal, estratégicas ou com alto custo de alcance.

Além dos ativos elementares, o anexo B da 27005 (ISO/IEC, 2007) recomenda uma classificação de ativos de suporte, combinada por seis classes:

Hardware

Elementos mecânicos, eletrônicos e físicos, que suportam a execução automática de processos.

Software

Programas de computador de sistema operacional, de suporte, software empacotado e aplicativos de negócio padronizados ou específicos da organização.

Rede de computadores

Constituída por todos os dispositivos de redes e telecomunicações que interconectam os dispositivos e elementos dos sistemas de informação, como redes telefônicas, redes de computadores de longa distância, metropolitanas, locais e ad hoc, roteadores, bridges, hubs e outras interfaces de comunicação.

Pessoal

Constituído por grupos enquadrados entre tomadores de decisão, usuários, pessoal de manutenção e operação e desenvolvedores de software.

Site (sítio)

Constituído por todos os lugares que agregam os demais ativos sob escopo, bem como os meios para operar esse sítio, como:

- Espaços exteriores;
- Perímetros defensivos;
- Zonas dentro do perímetro (escritórios, zonas seguras);
- Serviços essenciais para operação de equipamentos;
- Serviços de comunicação;
- Utilidades para suprimento de energia elétrica, água, esgoto, condicionamento do ar etc.

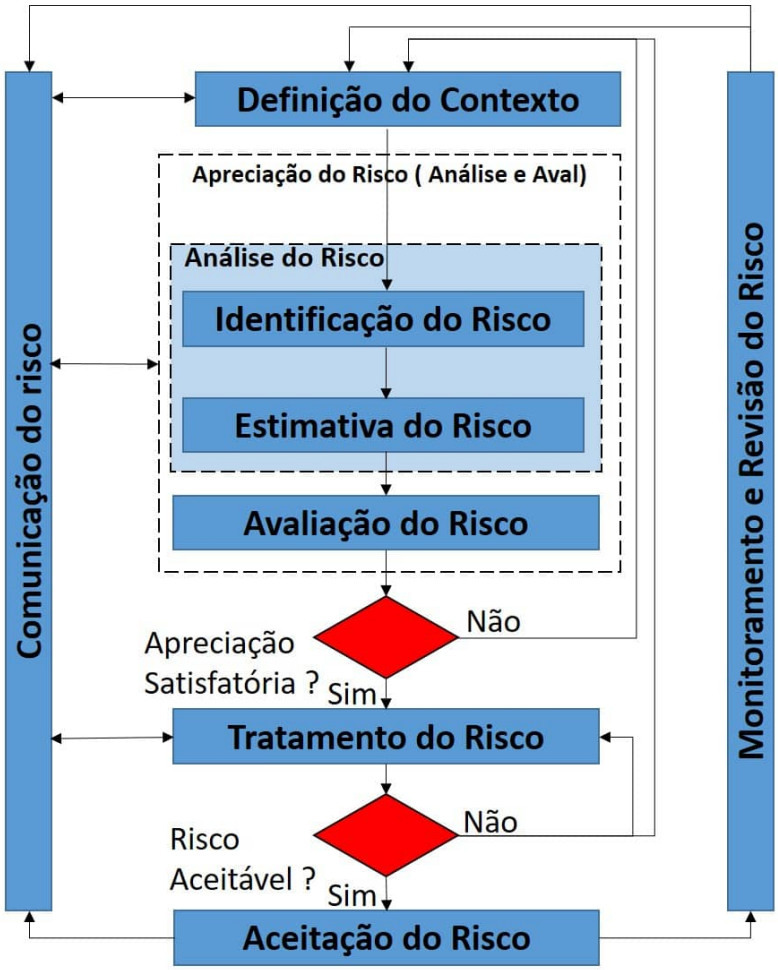
Estrutura organizacional

Constituída por:

- Autoridades (conselhos e comitês);
- Subunidades da organização (departamentos, divisões, seções);
- Projetos;
- Subcontratados e fornecedores.

Processo da gestão de riscos

O processo de gestão dos riscos é continuado e iterativo e suas atividades e fases são apresentadas nas cláusulas 7 a 12 da norma, compreendendo as seguintes fases ilustradas a seguir.



O processo de gestão do risco da ISO 27005.

A seguir, conheceremos mais detalhes sobre cada uma das etapas do processo de gestão do risco.

Definição do contexto

Fase de preparo para implementação da gestão de riscos, que abrange especialmente a definição de três aspectos:

- Critérios básicos para GRSI (Gestão de Riscos de Segurança da Informação);
- Escopo e alcances do GRSI (Gestão de Riscos de Segurança da Informação);
- Organização que vai atuar a GRSI (Gestão de Riscos de Segurança da Informação).

Análise do risco

A etapa de análise do risco é a composição dos processos de **identificação do risco, estimativa do risco** e de **avaliação de riscos**, que serão detalhadas a seguir.

Identificação do risco

A finalidade da identificação do risco é analisar o que pode acontecer para ocasionar uma perda potencial, ou ganhar percepção sobre como, onde e que perda pode ocorrer. A identificação do risco pode se dividir em cinco pontos:

Identificação de ativos

Recebe como entradas: a declaração do escopo e os limites da gestão de riscos e uma classificação preliminar de ativos da empresa, com recomendação do responsável por cada um, das localizações, funções e outras características dos ativos.

O objetivo é identificar quais dos ativos estão no escopo a ser gerenciado, produzindo como saída uma classificação de ativos, e com quais os riscos devem ser gerenciados, associado a uma lista de processos de negócio relacionados com os ativos e a relevância desses relacionamentos.

Identificação de ameaças

Entram informações sobre ameaças, adquiridas por meio da revisão dos registros de incidentes e eventos de segurança e dos responsáveis pelos ativos, dos usuários e de outras fontes, compreendendo catálogos externos de ameaças.

O objetivo é que advertências e suas fontes sejam identificadas. A atividade produz como saída uma lista dessas advertências, com a identificação de tipo e fonte da ameaça.

Identificação de controles

Recebe as entradas na documentação dos controles e planos de implementação de tratamento de risco, quando existentes.

O objetivo da identificação são que as formas de controles existentes e planejados sejam identificadas. A atividade gera a saída da classificação de todos os controles existentes e planejados, com seu andamento de implementação e uso.

Identificação de vulnerabilidades

Recebe como entradas a lista de ameaças conhecidas, a lista de ativos e a classificação de controles existentes e desenhados.

O objetivo é identificar as vulnerabilidades nos ativos, que podem ser exploradas pelas ameaças e, dessa forma, podem causar danos aos ativos e à empresa. A identificação de vulnerabilidades produz uma lista de vulnerabilidades em relação a ativos, ameaças e controles; e uma lista de vulnerabilidades não catalogadas a quaisquer ameaças, para revisão e monitoramento.

Identificação de consequências

Recebe como entradas a lista de ativos, a lista de processos de negócios da organização, e a lista de ameaças e vulnerabilidades correlacionadas com ativos e suas relevâncias.

O objetivo é identificar as consequências de eventuais prejuízos de confidencialidade, integridade e disponibilidade entre todos os ativos. A atividade produz como saída uma lista de cenários de imprevistos com suas consequências relacionadas aos ativos e processos de negócio. Esses cenários de imprevisto são apoios para a identificação dos riscos de segurança.

Estimativa do risco

Processo responsável por identificar, ajustar e avaliar os riscos. Abrange várias análises e descrições que visam mensurar e classificar um risco. A forma de avaliação do risco é um processo que deve ser executado em pelo menos duas repetições.

Tal abordagem é devida à interdependência entre os vários elementos verificados durante a identificação de ativos, ameaças, controles, vulnerabilidades, probabilidades, consequências, impactos e magnitude de riscos. A seguir temos as entradas e saída desta etapa:

Entradas	Saída
Critérios básicos, escopo e limites, bem como a organização responsável pelo processo de GRSI (gestão de risco e segurança da informação), definidos na fase de definição dos conceitos.	É uma classificação de riscos avaliados e considerados em níveis e priorizados de acordo com os critérios formados na fase anterior.

Avaliação do risco

O objetivo da avaliação do risco é priorizar os riscos, segundo os critérios de avaliação e objetivos relevantes para a organização. São inícios para a avaliação do risco os seguintes pontos: classificação de riscos com valorações de condições, critérios de estimativa de riscos afirmados na definição do assunto, e critérios de aceite dos riscos, declarados na definição do assunto.

Uma vez que as entradas forem feitas, são recebidos os estados dos riscos valorados e são confrontados com os critérios de estimativa estabelecidos os critérios da concordância de riscos. A saída da atividade é uma classificação de riscos priorizados, logo, os critérios de avaliação, em relação aos panoramas de incidente, levarão a esses riscos.

Avaliação do risco.

Tratamento do risco

O tratamento do risco é uma das etapas da gestão de riscos que cobre a decisão entre prender, evitar, transferir ou reduzir os riscos. A entrada dos dados para o tratamento de todos os riscos é uma classificação de riscos priorizados, conforme exigências e estimativa em relação aos cenários inesperados que induziram a esses riscos. Os escopos a serem adquiridos para o tratamento dos riscos são:

- Significado de quais controles serão agregados para reduzir alguns desses riscos;
- Posse ou concordância de outros riscos;
- Ação de evitar outros riscos;
- Mudança de quaisquer desses riscos a outros agentes;
- Significado de um plano de tratamento do risco.

As saídas desta fase são o plano de tratamento do risco e a classificação de riscos residuais, todos sujeitos à decisão de concordância pelos altos gestores da empresa.

Comunicação do risco

Comunicação.

A comunicação do risco é a união de diversas atividades sucessivamente executadas, envolve a troca de avisos sobre os riscos entre os tomadores de decisão e todos os funcionários da organização. O escopo da comunicação é fazer com que as informações estejam sendo trocadas ou compartilhadas entre os tomadores de decisão e outros interventores. As entradas para a comunicação do risco são todas as informações sobre riscos obtidas a partir das atividades de gestão de riscos e segurança da informação.

O saldo da atividade é a compreensão mútua e continuada do processo dos resultados, com o alcance de acordos sobre como gerenciar riscos. As principais informações compartilhadas ao redor dos riscos envolvem os seguintes pontos:

- Existência do risco;
- Natureza do risco;
- Formato do risco;
- Possibilidade do risco;
- Severidade do risco;
- Tratamento do risco;
- Discernimentos para aceitação do risco.

As percepções de risco variam muito de pessoa para pessoa, pois hipóteses, formação, considerações, necessidades e inquietações variam entre indivíduos, sendo necessário identificar, documentar e considerar visivelmente tais percepções e raciocínios.

Dessa maneira, a comunicação do risco tem duas direções (bidirecional), e mantê-la dessa forma é importante, pois pode impactar severamente a tomada de decisões e contribuir para que as corretas ações sejam tomadas. Comitês de debate durante a priorização e o tratamento apropriado dos riscos podem ser formados.

A comunicação de riscos facilita:

- Garantia dos resultados da gestão de risco;
- Coleta de informações sobre os riscos;
- Compartilhamento de decorrências da avaliação de riscos e o plano de tratamento de riscos;
- Compreensão mútua que elimina ou reduz a ocorrência e as consequências de brechas de segurança;
- Processo de tomada de decisões;
- Fluxo de conhecimentos sobre segurança da informação;
- Coordenação com outros parceiros e ampliação de respostas aos planos na ocorrência de incidentes;
- Formação de entendimento de responsabilidade acerca de riscos entre os tomadores de decisões e interventores;
- Melhor conscientização.

Diferentes planos de comunicação do risco devem ser desenvolvidos para os casos de operação da organização sob condições normais e quando a empresa estiver operando em modo de emergência ou crise.

É importante, sobretudo, estabelecer um canal de informações sobre riscos com a área de relações públicas da organização, especialmente durante emergências ou crises. Não atender da forma correta à comunicação dos riscos diminui sensivelmente o efeito da gestão de riscos.

Comentário

A divulgação dos planos de gestão de riscos é fundamental para seu sucesso. Um plano de gestão de riscos guardado de forma bastante segura, cujo conteúdo é conhecido exclusivamente pela gestão da segurança, não conduz à melhoria da segurança.

Monitoramento e revisão do risco

Monitoramento e revisão do risco é o nome dado a um conjunto de atividades executadas, que envolvem o monitoramento dos diversos fatores de distinção do risco, a fim de identificar algumas mudanças no contexto da empresa, modernizar o panorama de riscos e aprimorar o processo de gestão de riscos. O processo de monitoramento e revisão do risco é dividido em dois subprocessos:

Monitoramento e revisão dos fatores de risco

Monitoramento e revisão dos fatores de risco recebem as entradas completas de informações originadas das atividades de GRSI (gestão de risco e segurança da informação). O objetivo é o monitoramento e a revisão dos riscos e de seus fatores (valoração dos ativos, impactos, ameaças, vulnerabilidades e probabilidades), a fim de identificar qualquer início de mudanças significativas no contexto organizacional. Durante o monitoramento e a revisão dos fatores de risco deve-se observar:

- Riscos não estáticos;
- Mudanças bruscas podem acontecer sem indicação visível e necessitam de monitoramento contínuo;
- A contratação de serviços externos pode auxiliar no monitoramento desses fatores.

A organização precisa rever todos os riscos de modo regular, principalmente quando grandes modificações ocorrem nos ambientes interno e (ou) externo. Destacam-se os principais aspectos para monitoramento:

- Novos ativos que foram incluídos no escopo;
- Modificações nos valores dos ativos devido a, por exemplo, mudanças em negócios;
- Novas ameaças que passaram a existir interna e (ou) externamente;
- Possibilidade de novas ameaças explorarem vulnerabilidades novas ou que aumentaram;
- Aumento do impacto ou de consequências em ameaças, vulnerabilidades e riscos, quando apreciados de forma agregada;
- Incidentes de segurança da informação.

O resultado do monitoramento e da revisão dos fatores de risco é a disposição contínua entre a gestão de riscos e os objetivos de negócios, dentro dos critérios de risco estabelecidos.

Monitoramento, revisão e melhoria da gestão de riscos

Esse subprocessos recebem as entradas de todas as informações trazidas das atividades de GRSI – gestão de risco e segurança da informação. O objetivo é fazer com que o processo de GRSI seja continuamente monitorado, revisto e aperfeiçoado, quando necessário e apropriado. O monitoramento, a revisão e a melhoria da gestão de riscos devem garantir os pontos a seguir:

- O processo de GRSI é adequado e adotado;
- Os riscos são realistas;
- A gestão de riscos tem capacidade de responder aos riscos.

O resultado do monitoramento é que o processo de GRSI mantém-se atualizado e continuamente relevante para o cumprimento dos escopos de negócio da empresa. De outra forma, sem o monitoramento, o processo de GRSI se tornará obsoleto e de pouca utilidade.

Gestão de riscos e seus principais processos

No vídeo a seguir, abordaremos os principais processos envolvidos na gestão de riscos.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vem que eu te explico!

Os vídeos a seguir abordam os assuntos mais relevantes do conteúdo que você acabou de estudar.

Conceito da gestão de risco

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Processo da gestão de riscos

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o aprendizado

Questão 1

Qual das alternativas a seguir define a gestão de riscos?

A

Processo sistemático que permite a identificação de riscos.

B

São as regras que mitigam eventos adversos nos procedimentos operacionais.

C

É o conjunto de medidas que deve ser treinado para que uma crise seja superada rapidamente.

D

Faz parte da gestão operacional da empresa, limita-se a identificar o risco e punir o responsável.

E

A gestão de riscos é o processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles de segurança diante do seu perfil de riscos.

A alternativa E está correta.

Segundo a definição, a gestão de risco é todo processo de identificação, classificação, avaliação e tratamento do risco. A gestão de riscos vai viabilizar a implantação de ações e controles que permitem a mitigação dos riscos.

Questão 2

Quais são as fases do processo de gestão de riscos?

A

Reunião preparatória, identificação dos riscos e tratamento dos riscos.

B

Definição de contexto, identificação do risco, estimativa do risco, avaliação do risco e tratamento do risco/ aceitação do risco.

C

Comunicação de risco, avaliação e aceitação do risco.

D

Apreciação e tratamento dos riscos.

E

Definição, comunicação e aceitação dos riscos.

A alternativa B está correta.

Segundo a norma ISO 27005 as fases são: definição de contexto, identificação do risco, estimativa do risco, avaliação do risco e tratamento de risco/aceitação do risco.

Considerações finais

Vimos que a gestão de segurança de data center é de extrema importância para toda a infraestrutura, desde a sua área externa até a área lógica, em que serviços, dados e informações estão sendo processados, armazenados e disponibilizados para os clientes. As operações realizadas devem estar em completo alinhamento e apoiadas pelas políticas, diretrizes e normas da empresa, bem como o uso de protocolos e normas de segurança, na garantia da sua continuidade de negócio e da recuperação de desastres.

O processo de gestão de riscos com o processo de segurança da informação é o núcleo de qualquer ação bem-sucedida da gestão da segurança da informação, e sua adoção, segundo o modelo da 27005, permite a construção de uma abordagem eficaz na organização, em que comunicação, monitoramento e melhoria contínua garantem que a GRSI (gestão de risco e segurança da informação) continuará a atender às necessidades da organização no curto, médio e longo prazo.

Chegamos à conclusão de que é importante dar destaque para o uso da gestão de riscos na gestão da segurança. O alcance da segurança da informação em uma organização compreende, de forma unânime, a implementação de controles de segurança. Uma determinação racional sobre quais controles de segurança serão implementados.

Podcast

Ouça o podcast. Nele falaremos sobre os principais fatores que impactam a segurança física de um data center.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Leia o artigo **Segurança física em datacenters: estudo de caso**, de Rogério Carvalho Rosa, Maria Cristina Aranda e Pedro Domingos Antoniolli, publicado na revista Fatec Zona Sul, v. 3, n. 4, jun. 2017, que apresenta um estudo de caso detalhado sobre o tema.

Referências

ANSI/TIA-942. **Telecommunications infrastructure standard for data centers.** Arlington, USA: TIA, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2019.** Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Rio de Janeiro: ABNT, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013.** Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.