SIGN IN

rking Toward a

Trabalhando em direção a um plano de continuidade de negócios maduro e gerenciado

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN

ABOUT US

CAREERS

SUPPORT

STORE

et+, CompTIA

entas certas
durante uma

ado, a
organização não pode mais fazer negócios até que a infraestrutura seja restaurada e novos equipamentos comprados e instalados.

Neste exemplo, ter uma cópia/backup externo, preciso e em dia do inventário pode permitir que a organização entre com um sinistro na seguradora, encomende novo hardware/software e determine a quantidade de recursos necessários para recompor a infraestrutura na nuvem. No entanto, a infraestrutura não é a única coisa que precisa ser recuperada. A organização pode precisar refazer seu data center e, portanto, precisaria determinar os profissionais necessários, as habilidades exigidas, quais processos estão em vigor e como funcionam, quais dados são necessários, se os dados podem ser restaurados, quanto espaço em rack e energia são necessários e em qual ordem os sistemas devem ser restaurados.

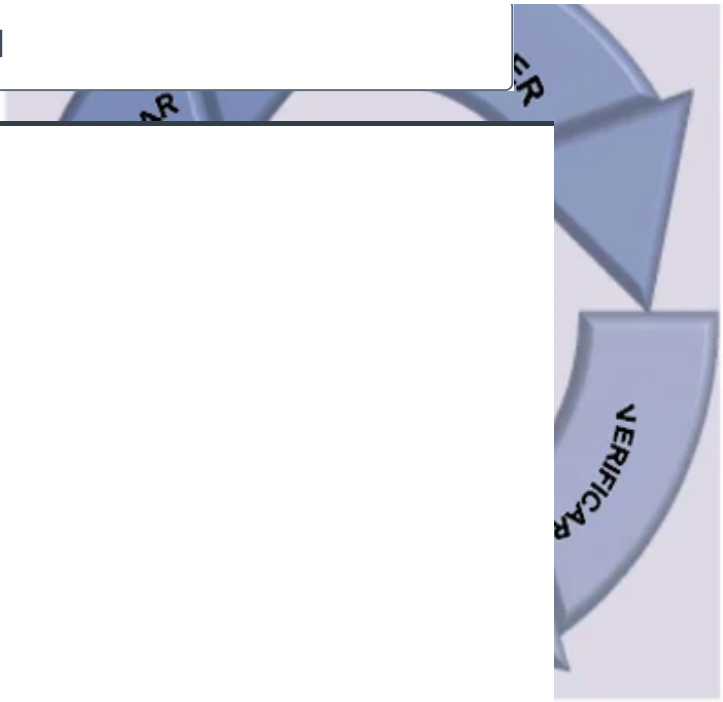
geopolíticas e avaliavam reduções de receita e outras áreas de risco. Muitos pensaram que as chances de uma pandemia eram muito baixas, aceitaram o risco e, posteriormente, descobriram que não estavam preparados.

Com frequência, frameworks podem ser usados para ajudar a atingir as metas organizacionais. Um framework pode ser definido como uma caixa de ferramentas, acompanhada por um manual que descreve as ferramentas, casos de uso e orientação sobre como e quando empregar essas ferramentas.

Devido às limitações de custos, restrições de recursos e falta de conhecimento, nem tudo pode ser implementado ao mesmo tempo. Requisitos futuros ou alterações podem ocorrer.

SIGN IN

UM FRAMEWORK PODE AJUDAR UMA ORGANIZAÇÃO A CONSTRUIR UMA CONTINUIDADE DE NEGÓCIOS DE SUCESSO E UM PLANO DE RECUPERAÇÃO DE DESASTRES (...) FORNECENDO UMA METODOLOGIA, ORIENTAÇÃO E FERRAMENTAS.



CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN

ABOUT US

CAREERS

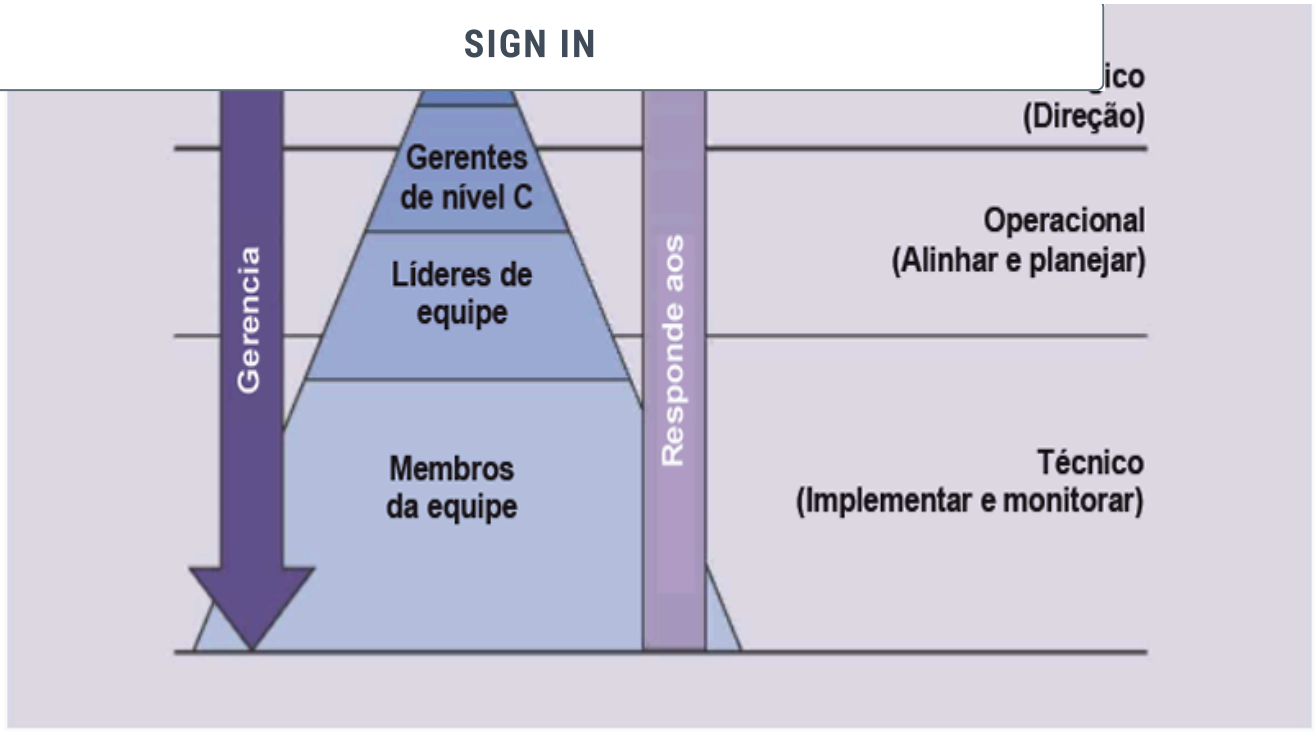
SUPPORT

STORE

ando em uma
ntinuamente

dades
de

ante entender
a
do alcançar
pecialidade



É provável que a camada estratégica não contenha as pessoas mais

cluirá
pectos da
as
eracional

a e suas

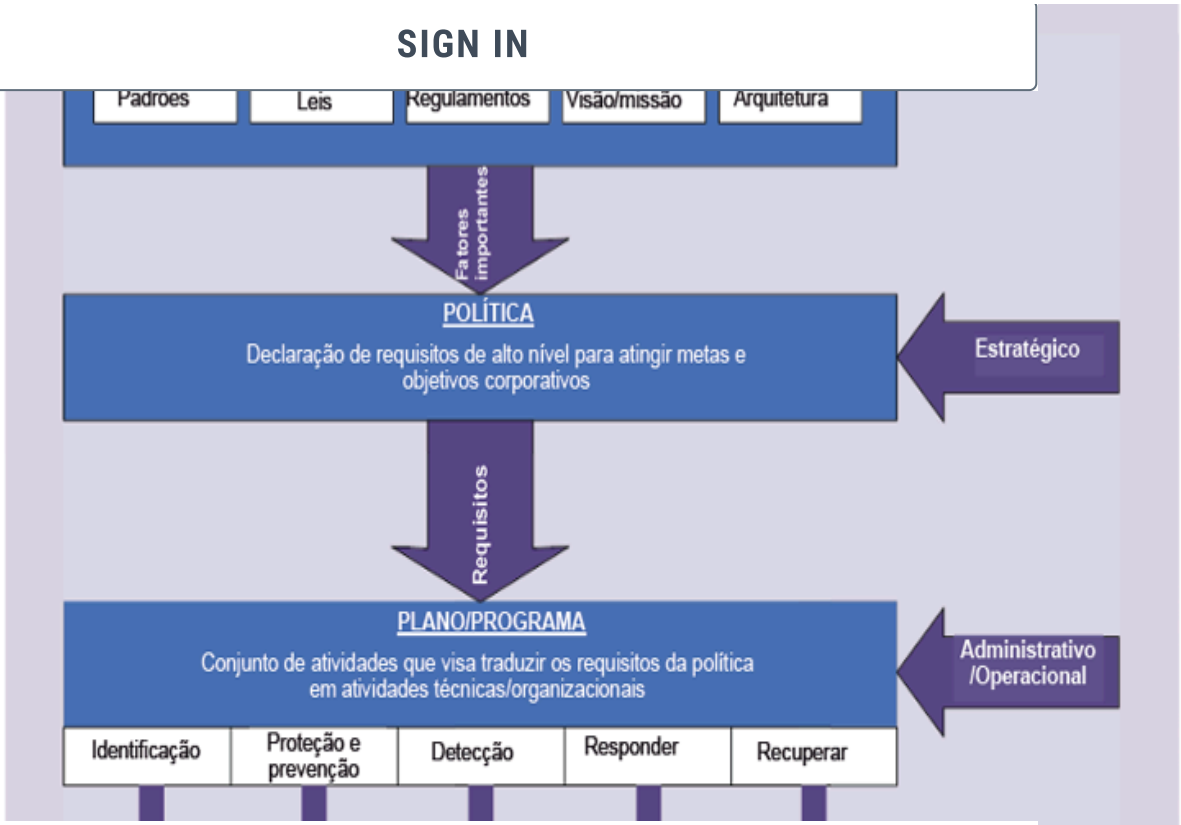
pelo
ão da
ar a
os dentro de

e os
ente dos
n orientação

SIGN IN

À primeira vista, pode parecer um exagero, mas o ponto principal aqui é que pode, e provavelmente haverá, eventos e cenários de risco que forçarão o fechamento de uma organização. Portanto, é necessário avaliar as funções críticas de negócios de uma organização em termos de risco e decidir a melhor forma de evitar, prevenir e mitigar o risco. Como pode haver restrições de orçamento e conhecimento, nem tudo pode ser implementado imediatamente. Quando for o caso, as prioridades devem ser definidas ou recursos adicionais devem ser obtidos.

SIGN IN



CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN

ABOUT US

CAREERS

SUPPORT

STORE

organização
risco com

camada
os executivos
em seus
etectar,
almente se

SIGN IN

evitar multas que podem nos tirar do mercado", os executivos de nível C pegam essa declaração e tentam traçar um plano. Neste exemplo, o diretor de marketing (CMO) provavelmente examinaria como as comunicações com o cliente são afetadas, enquanto o diretor de informações (CIO) provavelmente pensaria em como os dados são armazenados, onde são armazenados e quais são as opções considerando um nível técnico. O diretor jurídico provavelmente examinará os requisitos definidos pela lei ou legislação e avaliará o risco de não conformidade. O diretor de segurança da informação (CISO) ou diretor de proteção de dados (DPO) também pode usar termos e frases como:

- **Treinamento**—"Devemos treinar nossos usuários sobre o uso aceitável dos dados."
- **Conscientização**—"Como vamos garantir que nossos usuários entendam por que eles não podem enviar esses dados?"

tão seguindo

uipe da

utilizados, os continuidade

ão da equipe.

os e

ente, seguida

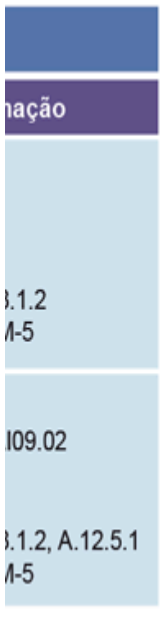
camada de o que emas,

SIGN IN

SUCESSO NÃO PODE SER CRIADO SEM A COMPREENSÃO DA HIERARQUIA ORGANIZACIONAL E DAS FUNÇÕES E RESPONSABILIDADES DA EQUIPE.

O framework de Segurança Cibernética (CSF) do National Institute of Standards and Technology (NIST) norteamericano[2] usa diferentes funções e categorias de atividades que devem ocorrer durante a construção de um programa. As funções podem ser definidas como identificar, proteger, detectar, responder e recuperar. Ao analisar as funções, fica claro que a proteção/prevenção tenta evitar que o risco se manifeste. Detectar, responder e recuperar tratam de problemas que surgem quando o risco se materializa.

mo essas
IST. Por



ıns entre
ɔdo para

frequentemente referenciadas durante o processo de desenvolvimento do framework.[3]

A revisão e a compreensão das referências informativas listadas podem fornecer uma visão mais profunda do que se espera e de como esses objetivos podem ser alcançados.

A Publicação Especial do NIST (SP) 800-53, Rev.5, cobre os controles de segurança e privacidade para sistemas de informação e organizações.[4] Ela documenta todos os controles em termos de objetivos de controle, orientações suplementares e aprimoramentos de controle e pode ser usado em conjunto com qualquer framework. Os objetivos de controle são metas que precisam ser atingidas. A orientação suplementar contém informações adicionais sobre o controle e, às vezes, também se refere a outros controles.

SIGN IN

esastres é
reconstruir/recuperar o local, a infraestrutura e os dados de uma organização quando algo de ruim acontecer.

Quando ocorre um desastre que resulta na destruição de infraestrutura ou dados de missão crítica, há duas métricas importantes:

1. O objetivo do ponto de retorno (RPO) define a quanta perda de dados uma organização pode sobreviver. O RPO é medido em função do tempo. Por exemplo, uma organização pode perder um dia de dados. No entanto, se a organização perder mais dados, pode correr o risco de ela não sobreviver.
2. O objetivo de tempo de retorno (RTO) define a quantidade de tempo que a organização tem para executar a operação de restauração. Por exemplo, o serviço afetado deve ser restaurado em quatro horas ou

CREDENTIALING
MEMBERSHIP
ENTERPRISE
PARTNERSHIPS
TRAINING & EVENTS
RESOURCES
JOIN
ABOUT US
CAREERS
SUPPORT
STORE

todo a organização corre o risco de danos financeiros, reputação,

á avaliado.
n ser

ativo é
A razão para
a um ativo,
uma
rganização
rma ficasse

a etapa é a
eve elaborar
o para

A próxima etapa é adicionar a probabilidade e impacto a cada risco. Isso pode ser feito usando abordagens quantitativa ou qualitativa. A versão qualitativa define o impacto e a probabilidade de risco em termos de alto, médio e baixo, tornando-se uma abordagem subjetiva.

A abordagem quantitativa usa porcentagens, moedas e resulta em uma projeção de perda potencial, tornando-se uma abordagem objetiva.

Isso permite que uma pontuação de risco seja adicionada à matriz de riscos que está sendo criada. A expectativa de perda anual (ALE) deve ser calculada ou estimada, caso possível. A ALE é um valor importante que define a quantidade de dinheiro que a organização pode gastar nos controles que gostaria de implementar. Não adianta gastar US$ 200 para proteger US$ 5.

ALE. A

lassificando-

são

aceitos. Essa

ser aceitos e

começar.

de alto nível
e a direção definida pela camada estratégica de negócios.

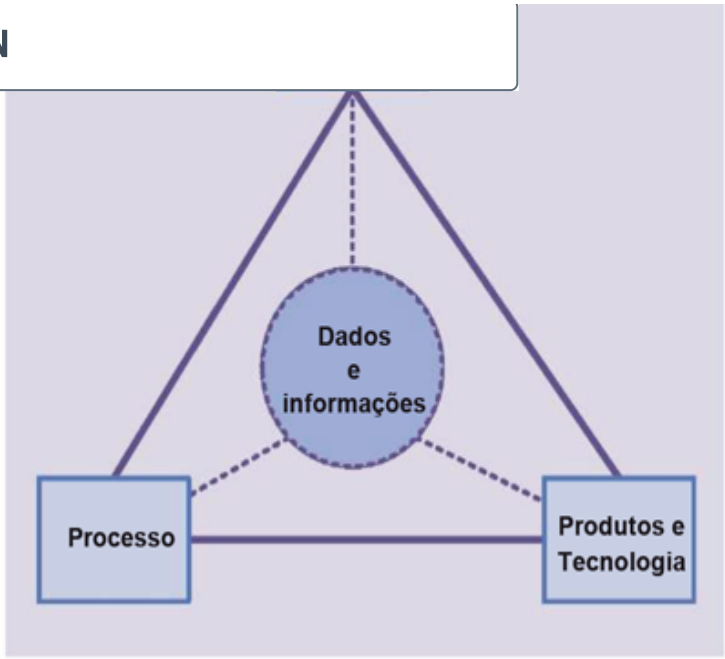
Estratégias de recuperação e desenvolvimento de continuidade (Fazer)
Um plano deve ser construído com ações específicas a serem tomadas para cumprir a política. Em outras palavras: "O que precisamos para garantir a redução da probabilidade ou do impacto do resultado negativo?"

Os incidentes geralmente ocorrem de três maneiras, conforme ilustrado na **figura 5**:

1. Alguma coisa para de funcionar, mas as funções de negócios não são afetadas.
2. Alguma coisa para de funcionar e as funções de negócios são afetadas.
3. Algumas funções de negócios param.

os são o
vo é qualquer

SIGN IN

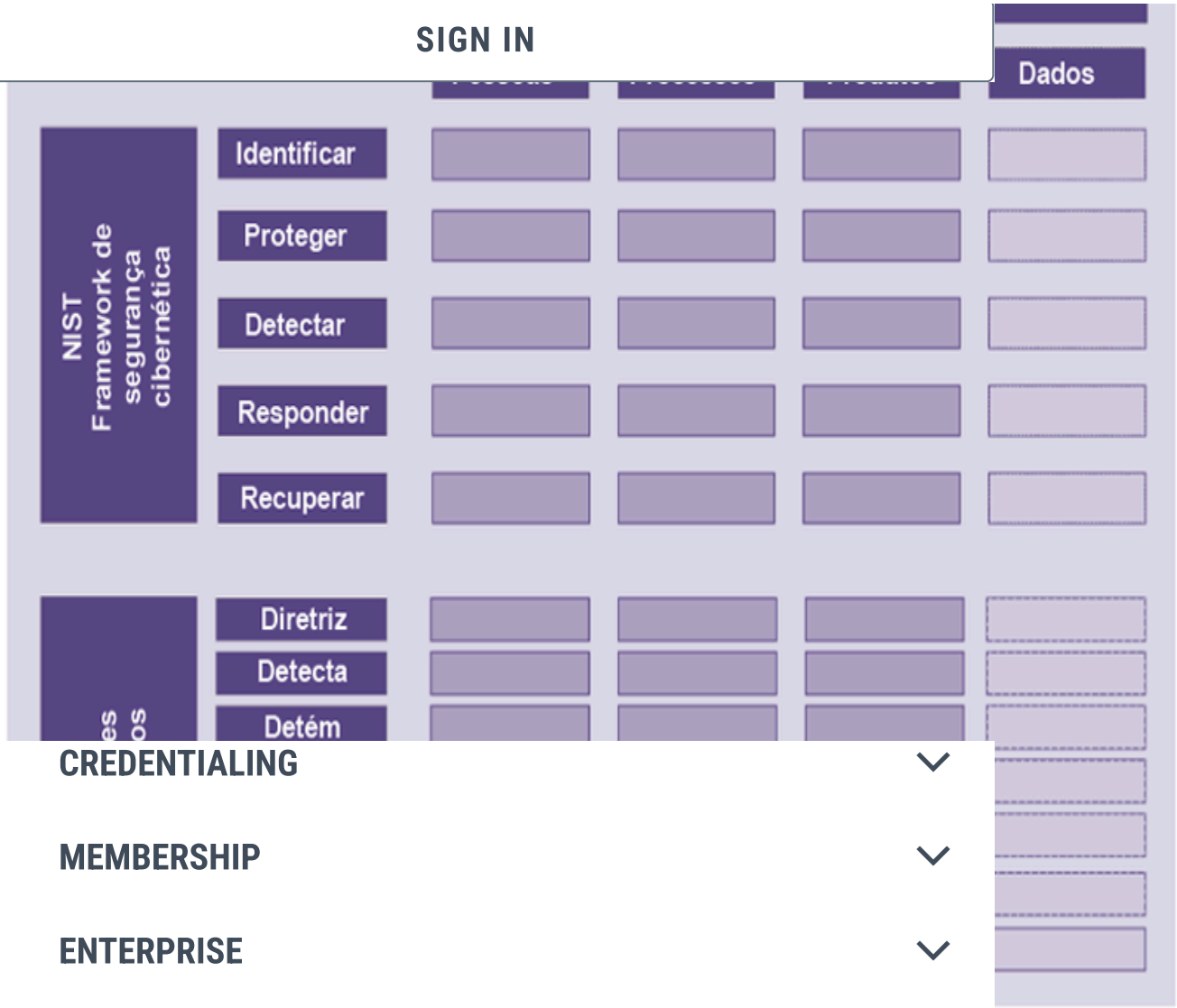


Os dados estão provavelmente entre os ativos mais importantes que precisam ser protegidos. Duas direções diferentes para proteger os dados são ilustradas na pirâmide na **figura 6**.

A primeira direção a seguir é trabalhar para proteger processos, produtos e pessoas. Os dados são protegidos, assim como os ativos que funcionam com os dados.

CREDENTIALING
MEMBERSHIP
ENTERPRISE
PARTNERSHIPS
TRAINING & EVENTS
RESOURCES
JOIN
ABOUT US
CAREERS
SUPPORT
STORE

os. Nesse
os para
s de
proteção
grama pode
e ser



evem ser
dados. No
ne ilustrado

mais
-los com o
m controle
les

e proteger os
orrente (o que

SIGN IN

- Recuperar os dados de backups.
- Treinar os usuários sobre como trabalhar com os dados e os produtos nos quais os dados são usados.

Nesse ponto, a camada operacional ainda não informa à camada técnica como executar essas ações; ela simplesmente declara o que precisa ser feito. Basicamente, está criando os conjuntos de controle. Esses conjuntos de controle serão revisados pela equipe técnica para determinar quais são as opções de implementação. Uma vez implementados, os controles podem ser auditados e monitorados para comprovar a conformidade. Orientação sobre as famílias de controle e controles que podem ser usados podem ser encontrados no NIST CSF ou NIST SP 800-53. A orientação também pode ser encontrada na *ISO/IEC 27002:2013 Tecnologia da informação - Técnicas*

SIGN IN

mória?

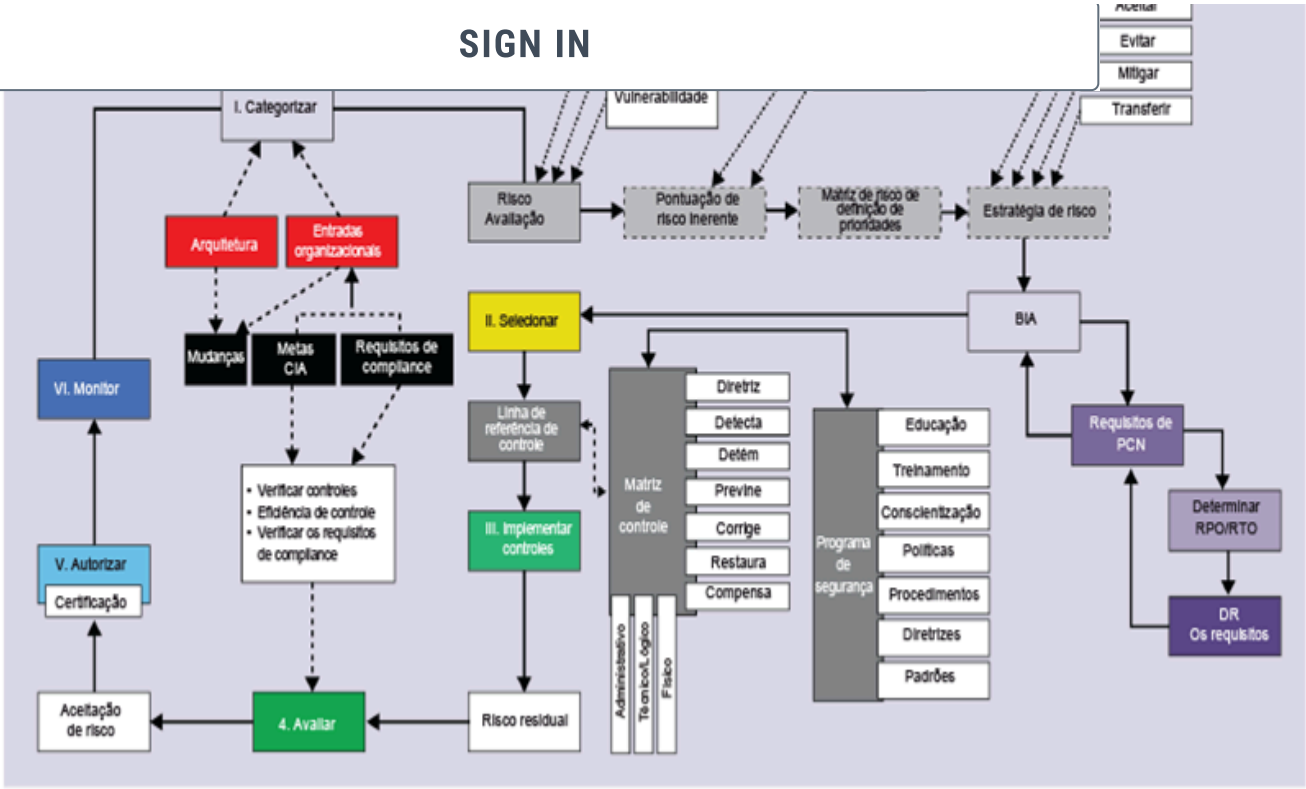
O DOMÍNIO DA CONTINUIDADE DE NEGÓCIOS VAI MUITO ALÉM DA PROTEÇÃO DA INFRAESTRUTURA.

Essas métricas podem ser indicadores de progresso e, às vezes, até precursoras de outros eventos, o que significa que podem ser usadas para muitos propósitos, até mesmo planejando upgrades de capacidade.

Feedback (agir)
O ciclo de feedback existe para consolidar todas as lições aprendidas e fornecê-las como informação durante o próximo ciclo de planejamento.

lemonstrados
co para
da NIST SP
que acontece
. Se todos os
cial do
nforme

SIGN IN



View Large Graphic

teção da
lo e liderado
ıtro da
ɔs e estão na
ue precisa
ade e
ra tomar
r, dando à
e construir

rganização a
ısará mais
ɔara

ser revisado,

É por isso que pode ser útil ampliar a abordagem baseada em riscos da NIST SP 800-37. É um framework abrangente que permite o monitoramento contínuo e o ajuste dos controles. É um processo interminável de definir o estado atual de uma organização e o estado desejado para detectar e preencher lacunas potenciais, já que nem tudo pode ser implementado de uma vez, resultando em múltiplos ciclos de planejamento e orçamento para preencher lacunas.

Notas de rodapé

[1] International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). ISO/IEC 27001:2013, *Security and*

ments, Suíça,

security

Framework

cation (SP)
and

P.800-

technology—
s—

technology—
controls—

5/final/documents/sp800-53r5-to-iso-27001-mapping.docx

[8] *Op cit* ISO/IEC 27002:2013

[9] National Institute of Standards and Technology, SP 800-37 Revision 2 *Risk Management Framework for Information Systems and Organizations*, EUA, dezembro de 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

SVEN DE PRETER, CDPSE, CISSP, COMPTIA CLOUD+, COMPTIA NET+, COMPTIA SEC+

É administrador de redes e sistemas sênior de uma organização que possui e administra salas de shows e teatros na Bélgica e uma organização de venda de ingressos com um centro de atendimento completo ao cliente. Durante seus mais de 20 anos na organização, ele acumulou experiência nas áreas de gestão de eventos e incidentes, gerenciamento de mudanças, líder de equipe operacional, virtualização de data center (usando VMware), conectividade e arquitetura. Ele também trabalhou em diferentes aspectos do programa de privacidade corporativa, prestando consultoria sobre diversas políticas, procedimentos e diretrizes. Ele também é um dos fundadores da *CertificationStation.org*, uma plataforma gratuita onde as pessoas que estudam para obter certificações de segurança podem discutir tópicos e materiais de treinamento.

< PREVIOUS ARTICLE

NEXT ARTICLE >