

SIGN IN

Working Toward a

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



CREDENTIALING



MEMBERSHIP



ENTERPRISE



PARTNERSHIPS



TRAINING & EVENTS



RESOURCES



st+, CompTIA

JOIN



ABOUT US



CAREERS



SUPPORT

STORE

entas certas
r durante uma

SIGN IN

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.

CREDENTIALING

▼ Usar e se eles
r se as

MEMBERSHIP

▼ eu e se

ENTERPRISE

▼ de dos

PARTNERSHIPS

▼

TRAINING & EVENTS

▼ as de gestão
ção

RESOURCES

▼ Commission
have para o

JOIN

▼ is, atividades,
proativa e

ABOUT US

▼

CAREERS

▼ programa de
equada para

SUPPORT

, essas são

STORE

SIGN IN

es

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.

CREDENTIALING

✓ truturada,
ão mais

MEMBERSHIP

✓ ser criadas

ENTERPRISE

✓

PARTNERSHIPS

ia
✓ ação de
ando uma

TRAINING & EVENTS

✓

RESOURCES

✓

JOIN

✓

ABOUT US

✓ dos
I), também

CAREERS

✓ ela qual este
e um plano,
e definição de
nedidas

SUPPORT

STORE

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.

VERIFICAR

CREDENTIALING



MEMBERSHIP



ando em uma
ntinuamente

ENTERPRISE



PARTNERSHIPS



dades
de

TRAINING & EVENTS



RESOURCES



JOIN



ABOUT US



ante entender
a

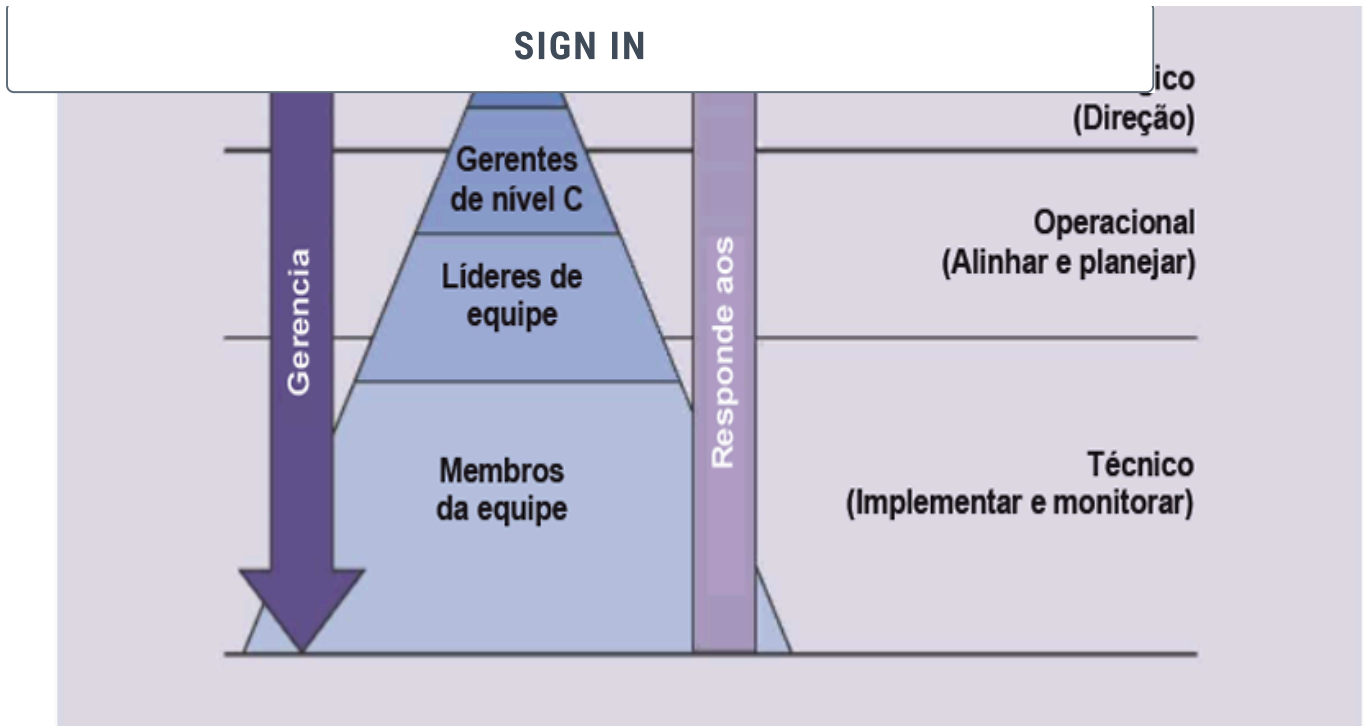
CAREERS



do alcançar
pecialidade

SUPPORT

STORE



É provável que a camada estratégica não contenha as pessoas mais

CREDENTIALING

✓ cluirá

MEMBERSHIP

✓ objectos da
as

ENTERPRISE

✓ eracional

PARTNERSHIPS

✓ a e suas

TRAINING & EVENTS

✓

RESOURCES

✓ pelo

JOIN

✓ ão da
/ar a

ABOUT US

✓ os dentro de

CAREERS

✓ e os

SUPPORT

ente dos

STORE

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.

CREDENTIALING



MEMBERSHIP



ENTERPRISE



PARTNERSHIPS



TRAINING & EVENTS



RESOURCES



JOIN



ABOUT US



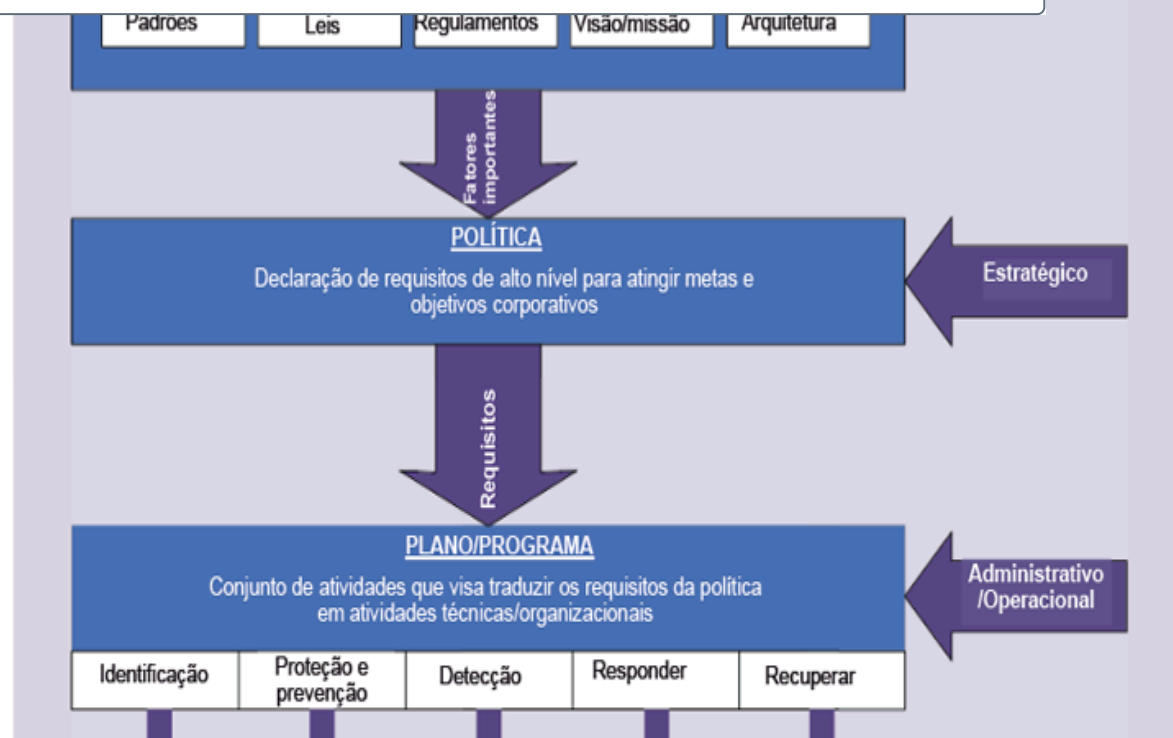
CAREERS



SUPPORT

STORE

SIGN IN



CREDENTIALING



MEMBERSHIP



ENTERPRISE



PARTNERSHIPS



TRAINING & EVENTS



RESOURCES



JOIN



ABOUT US



CAREERS



SUPPORT

organização
risco com

camada
os executivos
em seus
detectar,
almente se

SIGN IN

evitar muitas

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?”

CREDENTIALING

✓ tão seguindo

MEMBERSHIP

✓

ENTERPRISE

✓

uipe da

PARTNERSHIPS

✓

utilizados, os

continuidade

TRAINING & EVENTS

✓

ão da

equipe.

RESOURCES

✓

JOIN

✓

ABOUT US

✓

os e

CAREERS

✓

ente, seguida

SUPPORT

camada de

STORE

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) norteamericano² 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.

CREDENTIALING



mo essas
IST. Por

MEMBERSHIP



ENTERPRISE



PARTNERSHIPS



TRAINING & EVENTS



RESOURCES



JOIN



ABOUT US



CAREERS



SUPPORT

STORE

ins entre
odo para

SIGN IN

es mais
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.

CREDENTIALING



ole ou

MEMBERSHIP



ENTERPRISE



} Tecnologia
mento de

PARTNERSHIPS



Tecnologia da
ontroles de

TRAINING & EVENTS



a ISO 27002

RESOURCES



bles de um

JOIN



ABOUT US



CAREERS



ção de

SUPPORT

lemas antes

STORE

itura, pois

SIGN IN

Desastres 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 menos.

CREDENTIALING



MEMBERSHIP



ENTERPRISE



PARTNERSHIPS



rá avaliado.
n ser

TRAINING & EVENTS



RESOURCES



ativo é
A razão para
a um ativo,

JOIN



uma

ABOUT US



organização
ma ficasse

CAREERS



SUPPORT

a etapa é a
eve elaborar
o para

STORE

SIGN IN

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.

CREDENTIALING



—

MEMBERSHIP



R

ENTERPRISE



O,
DE

PARTNERSHIPS



—

TRAINING & EVENTS



ALE. A

RESOURCES



lassificando-

JOIN



são

ABOUT US



aceitos. Essa

CAREERS



i ser aceitos e

SUPPORT

o

começar.

STORE

SIGN IN

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.

CRÉDENCIALING  param.

MEMBERSHIP 

ENTERPRISE 

PARTNERSHIPS 

TRAINING & EVENTS 

RESOURCES 

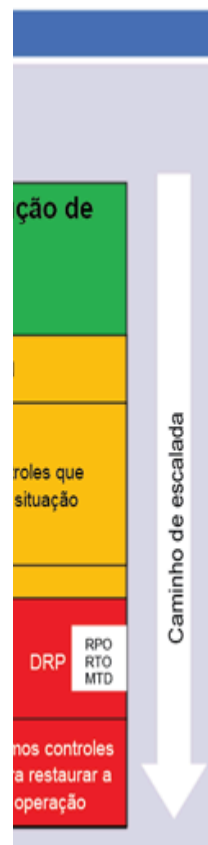
JOIN 

ABOUT US 

CAREERS 

SUPPORT

STORE

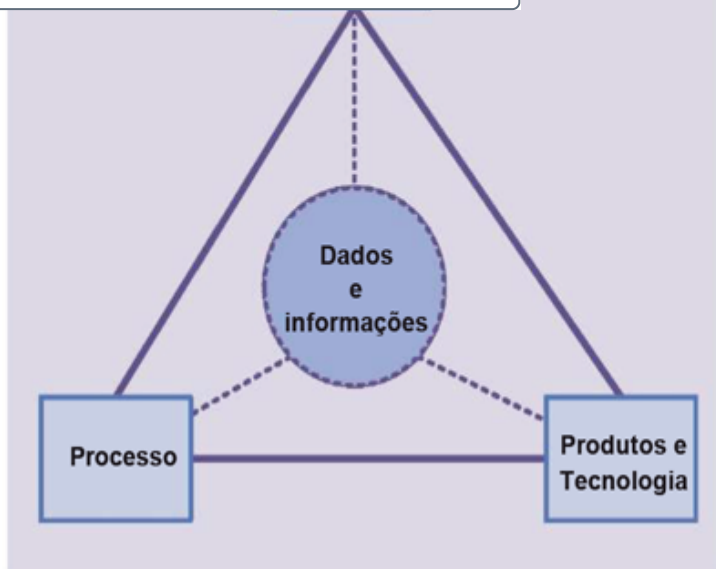


os são o
vo é qualquer

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



os. Nesse

MEMBERSHIP



os para

ENTERPRISE



s de

PARTNERSHIPS



proteção

TRAINING & EVENTS



grama pode

RESOURCES



JOIN



e ser

ABOUT US



CAREERS



SUPPORT

STORE

SIGN IN

Dados

NIST
Framework de
segurança
cibernética

Identificar

Proteger

Detectar

Responder

Recuperar

Diretriz

Detecta

Detém

CREDENTIALING

MEMBERSHIP

ENTERPRISE

PARTNERSHIPS

TRAINING & EVENTS

RESOURCES

JOIN

ABOUT US

CAREERS

SUPPORT

STORE



devem ser
dados. No
ne ilustrado

mais
-los com o
m controle
les

e proteger os
orrente (o que

SIGN IN

Organizado.

- 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*

CREDENTIALING



da

MEMBERSHIP



ENTERPRISE



interessadas
controle

PARTNERSHIPS



.O teste dos
ão existem.

TRAINING & EVENTS



RESOURCES



controles
conforme

JOIN



ABOUT US



ambiente de
de risco. Além
do mais

CAREERS



SUPPORT

STORE

de
m ser:

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.

CREDENTIALING



MEMBERSHIP



ENTERPRISE



lemonstrados
co para

PARTNERSHIPS



da NIST SP
que acontece

TRAINING & EVENTS



l. Se todos os
cial do

RESOURCES



nforme

JOIN



ABOUT US



CAREERS



SUPPORT

STORE

SIGN IN

O diagrama ilustra o processo de avaliação de risco, dividido em etapas e componentes inter-relacionados:

- Top Right (Legend):** Uma lista de ações: Evitar, Mitigar, Transferir.
- Top Center (Title):** "SIGN IN".
- Top Left (I. Categorizar):** Um bloco centralizado que recebe input de "Arquitetura" e "Entradas organizacionais" (ambos em caixas vermelhas). Ele também recebe input de "Vulnerabilidade" (caixa cinza) e "Risco Avaliação" (caixa cinza). O bloco "I. Categorizar" emite setas para "Pontuação de risco inerente", "Matriz de risco de definição de prioridades" e "Estratégia de risco".
- Top Right (Pontuação de risco inerente):** Um bloco cinza que recebe input de "Vulnerabilidade" e "Risco Avaliação". Ele emite setas para "Matriz de risco de definição de prioridades" e "Estratégia de risco".
- Top Right (Matriz de risco de definição de prioridades):** Um bloco cinza que recebe input de "Pontuação de risco inerente" e emite setas para "Estratégia de risco".
- Top Right (Estratégia de risco):** Um bloco cinza com uma borda tracejada que recebe input de "Matriz de risco de definição de prioridades" e emite setas para "BIA" e "Requisitos de PCN".
- Top Right (BIA):** Um bloco cinza que recebe input de "Estratégia de risco" e emite setas para "II. Seleccionar", "Requisitos de PCN" e "Determinar RPO/RTO".
- Top Right (Requisitos de PCN):** Um bloco cinza que recebe input de "BIA" e emite setas para "Determinar RPO/RTO" e "DR Os requisitos".
- Top Right (Determinar RPO/RTO):** Um bloco cinza que recebe input de "Requisitos de PCN" e emite setas para "DR Os requisitos".
- Top Right (DR Os requisitos):** Um bloco cinza que recebe input de "Determinar RPO/RTO" e emite setas para "Requisitos de PCN" e "DR Os requisitos".
- Top Right (II. Seleccionar):** Um bloco amarelo que recebe input de "BIA" e emite setas para "Limite de referência de controle" e "III. Implementar controles".
- Top Right (Limite de referência de controle):** Um bloco cinza que recebe input de "II. Seleccionar" e emite setas para "III. Implementar controles" e "Risco residual".
- Top Right (III. Implementar controles):** Um bloco verde que recebe input de "Limite de referência de controle" e emite setas para "Risco residual" e "4. Avaliar".
- Top Right (Risco residual):** Um bloco cinza que recebe input de "III. Implementar controles" e emite setas para "4. Avaliar".
- Top Right (4. Avaliar):** Um bloco verde que recebe input de "Risco residual" e emite setas para "VI. Monitor" e "V. Autorizar".
- Top Right (VI. Monitor):** Um bloco azul que recebe input de "4. Avaliar" e emite setas para "V. Autorizar" e "Certificação".
- Top Right (V. Autorizar):** Um bloco azul que recebe input de "VI. Monitor" e emite setas para "Certificação" e "Aceleração de risco".
- Top Right (Certificação):** Um bloco cinza que recebe input de "V. Autorizar" e emite setas para "Aceleração de risco".
- Top Right (Aceleração de risco):** Um bloco cinza que recebe input de "Certificação" e emite setas para "VI. Monitor".
- Top Right (Arquitetura):** Um bloco vermelho que recebe input de "I. Categorizar" e emite setas para "Mudanças", "Metas CIA" e "Requisitos de compliance".
- Top Right (Entradas organizacionais):** Um bloco vermelho que recebe input de "I. Categorizar" e emite setas para "Mudanças", "Metas CIA" e "Requisitos de compliance".
- Top Right (Mudanças):** Um bloco cinza que recebe input de "Arquitetura" e "Entradas organizacionais" e emite setas para "Metas CIA" e "Requisitos de compliance".
- Top Right (Metas CIA):** Um bloco cinza que recebe input de "Arquitetura", "Entradas organizacionais" e "Mudanças" e emite setas para "Requisitos de compliance".
- Top Right (Requisitos de compliance):** Um bloco cinza que recebe input de "Arquitetura", "Entradas organizacionais" e "Mudanças" e emite setas para "Requisitos de compliance".
- Top Right (Requisitos de compliance):** Um bloco cinza que recebe input de "Requisitos de compliance" e emite setas para "4. Avaliar".
- Top Right (Matriz de controle):** Um bloco cinza que recebe input de "II. Seleccionar" e emite setas para "Diretriz", "Detecta", "Detém", "Previne", "Corrige", "Restaura", "Compensa".
- Top Right (Programa de segurança):** Um bloco cinza que recebe input de "II. Seleccionar" e emite setas para "Educação", "Treinamento", "Conscientização", "Políticas", "Procedimentos", "Diretrizes", "Padrões".
- Top Right (Diretriz):** Um bloco cinza que recebe input de "Matriz de controle" e emite setas para "Detecta", "Detém", "Previne", "Corrige", "Restaura", "Compensa".
- Top Right (Detecta):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Detém", "Previne", "Corrige", "Restaura", "Compensa".
- Top Right (Detém):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Previne", "Corrige", "Restaura", "Compensa".
- Top Right (Previne):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Corrige", "Restaura", "Compensa".
- Top Right (Corrige):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Restaura", "Compensa".
- Top Right (Restaura):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Compensa".
- Top Right (Compensa):** Um bloco cinza que recebe input de "Diretriz" e emite setas para "Compensa".
- Top Right (Educação):** Um bloco cinza que recebe input de "Programa de segurança" e emite setas para "Treinamento", "Conscientização", "Políticas", "Procedimentos", "Diretrizes", "Padrões".
- Top Right (Treinamento):** Um bloco cinza que recebe input de "Educação" e emite setas para "Conscientização", "Políticas", "Procedimentos", "Diretrizes", "Padrões".
- Top Right (Conscientização):** Um bloco cinza que recebe input de "Educação" e emite setas para "Políticas", "Procedimentos", "Diretrizes", "Padrões".
- Top Right (Políticas):** Um bloco cinza que recebe input de "Educação" e emite setas para "Procedimentos", "Diretrizes", "Padrões".
- Top Right (Procedimentos):** Um bloco cinza que recebe input de "Educação" e emite setas para "Diretrizes", "Padrões".
- Top Right (Diretrizes):** Um bloco cinza que recebe input de "Educação" e emite setas para "Padrões".
- Top Right (Padrões):** Um bloco cinza que recebe input de "Educação" e emite setas para "Padrões".
- Top Right (Administrativo):** Um bloco cinza que recebe input de "Matriz de controle" e emite setas para "Técnico/Lógico", "Físico".
- Top Right (Técnico/Lógico):** Um bloco cinza que recebe input de "Administrativo" e emite setas para "Físico".
- Top Right (Físico):** Um bloco cinza que recebe input de "Administrativo" e emite setas para "Físico".

[View Large Graphic](#)

teção da
lo e liderado
ntro da
os e estão na
ue precisa
ade e
a tomar
r, dando à
e construir

rganização a
usará mais
para

ser revisado,

[SIGN IN](#)

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

CREDENTIALING	▼ <i>Security and</i> <i>ements, Suíça,</i>
MEMBERSHIP	▼ <i>security</i>
ENTERPRISE	▼ <i>Framework</i>
PARTNERSHIPS	▼
TRAINING & EVENTS	▼ <i>ation (SP)</i> <i>and</i>
RESOURCES	▼ <i>800-</i>
JOIN	▼
ABOUT US	▼ <i>technology—</i> <i>—</i>
CAREERS	▼
SUPPORT	
STORE	<i>technology—</i> <i>controls—</i>

SIGN IN

[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 >



[Privacy](#)

[Cookie Notice](#)

[Fraud Reporting](#)

[Bug Reporting](#)

1700 E. Golf Road, Suite 400, Schaumburg, Illinois 60173, USA | +1-847-253-1545 | ©2024 ISACA. All rights reserved.