PARA QUE SERVE
UMA ESTRUTURA DE

SEGURANÇA CIBERNÉTICA

ATHENA
SOLUÇÕES INTELIGENTES

SUMÁRIO

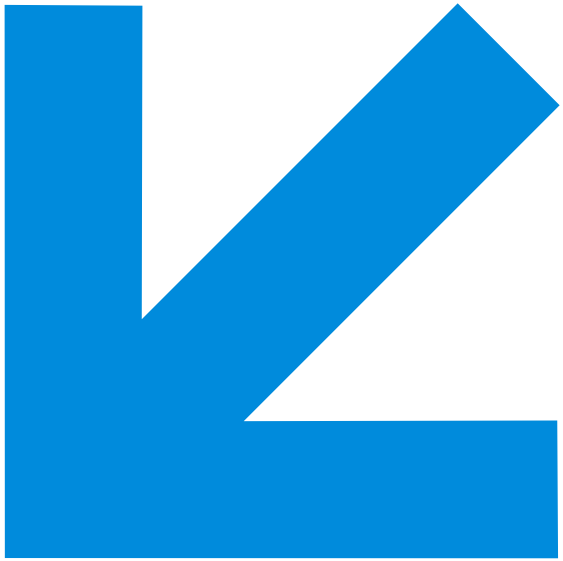
INTRODUÇÃO

As ameaças de segurança cibernética exploram a maior complexidade e conectividade de sistemas de infraestrutura crítica, o que coloca em risco a segurança das informações dos indivíduos, das empresas, economia e governos.

Para combater esses riscos cibernéticos, o NIST (Instituto Nacional de Padrões e Tecnologia) desenvolveu uma estrutura de segurança cibernética baseada em riscos para fornecer às agências governamentais e ao setor privado padrões e melhores práticas para ajudar a gerenciar os riscos de segurança cibernética.

+de **421 milhões**

de pessoas tiveram suas informações pessoais roubadas por cibercriminosos em 2022



Estima-se que os custos com **Ransomware** cheguem a

US$ 265 bilhões até 2031

O custo médio de uma violação de dados atingiu um recorde histórico de **US$ 4,35 milhões**

(R$ 22 milhões) no ano passado

Em 2022 foram mais de **25,2 mil** vulnerabilidades de segurança relatadas, um aumento de **26,5%** em relação ao ano anterior

O QUE É O **NIST**?

A estrutura de segurança cibernética do NIST é uma **ferramenta poderosa para organizar e melhorar seu programa de segurança cibernética**. É um conjunto de diretrizes e práticas recomendadas para ajudar as organizações a construir e melhorar sua postura de segurança.

A estrutura apresenta um conjunto de recomendações e padrões que permitem que as organizações estejam mais bem preparadas para **identificar e detectar ataques cibernéticos, além de fornecer diretrizes sobre como responder, prevenir e se recuperar de incidentes cibernéticos.**

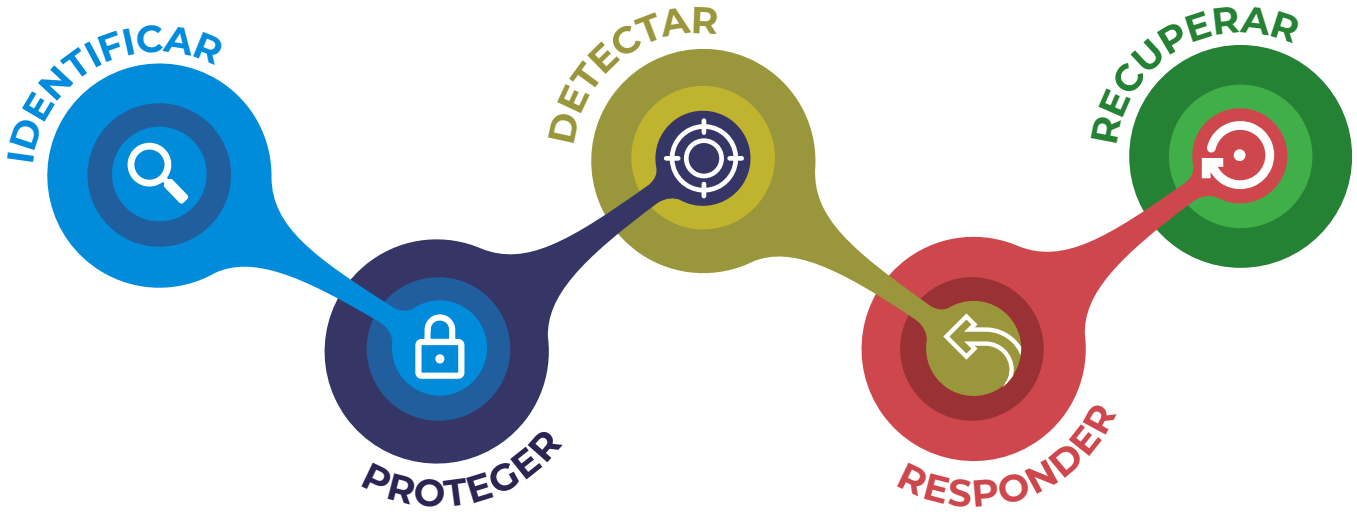
NIST CYBERSECURITY FRAMEWORK

Essa estrutura aborda a **falta de padrões quando se trata de segurança cibernética** e fornece um conjunto de regras e diretrizes para as organizações de todos os setores.

O **NIST CSF é considerado o padrão-ouro** para a construção de um programa de segurança cibernética. Se você está começando a estabelecer um programa ou já está executando um processo, a estrutura é ideal, agindo como uma ferramenta de **gerenciamento de segurança de nível superior** que ajuda a avaliar o risco de segurança cibernética em toda a organização.

SEGURANÇA CIBERNÉTICA

A estrutura categoriza todos os recursos, projetos, processos e atividades diárias de segurança cibernética nessas 5 funções principais:



IDENTIFICAR

A função “Identificar” está focada em **estabelecer as bases para um programa eficaz de segurança cibernética**. Ela auxilia no desenvolvimento de um entendimento organizacional para **gerenciar o risco** de segurança cibernética para sistemas, pessoas, ativos, dados e recursos. Para permitir que uma organização foque e priorize seus esforços, consistente com sua estratégia de gerenciamento de riscos e necessidades de negócios, essa função enfatiza a importância de entender o contexto de negócios, os recursos que suportam funções críticas e os riscos de segurança relacionados.

As atividades essenciais incluem:

Identificar ativos físicos e de software para estabelecer a base de um programa de gerenciamento de ativos

Identificar o ambiente de negócios da organização, incluindo seu papel na cadeia de suprimentos

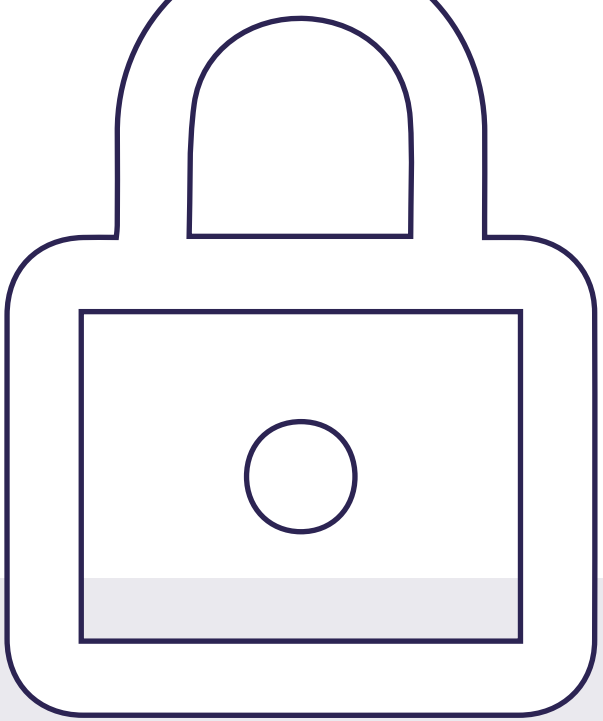
Identificar as políticas de segurança cibernética estabelecidas para definir o programa de governança, bem como identificar os requisitos legais e regulatórios relativos aos recursos de segurança cibernética da organização

Identificar vulnerabilidades de ativos, ameaças a recursos organizacionais internos e externos e atividades de resposta a riscos

Estabelecer uma estratégia de gerenciamento de risco, incluindo a identificação da tolerância ao risco

Identificar uma estratégia de gerenciamento de riscos da cadeia de suprimentos, incluindo prioridades, restrições, tolerâncias a riscos e premissas usadas para apoiar as decisões associadas ao gerenciamento

PROTEGER



Descreve as proteções apropriadas para garantir a entrega de serviços de infraestrutura crítica e oferece suporte à capacidade de limitar ou conter o impacto de um possível evento de segurança cibernética.

As atividades críticas incluem:

Implementar proteções para gerenciamento de identidade e controle de acesso dentro da organização, incluindo acessos físico e remoto

Capacitar a equipe por meio de treinamento de conscientização de segurança, incluindo treinamento de usuários privilegiados e baseados em funções

Estabelecer proteção de segurança de dados consistente com a estratégia de risco da organização para garantir confidencialidade, integridade e disponibilidade das informações

Implementar processos e procedimentos para manter e gerenciar as proteções de sistemas e ativos de informação

Proteger recursos organizacionais por meio de manutenção, incluindo atividades de manutenção remota

Gerenciar a tecnologia para garantir a segurança e a resiliência dos sistemas, de acordo com as políticas, procedimentos e acordos organizacionais

DETECTAR

A detecção de possíveis incidentes de segurança cibernética é fundamental e essa função define as atividades apropriadas para identificar a ocorrência de um evento de segurança cibernética em tempo hábil.

As atividades nesta função incluem:

Garantir que anomalias e eventos sejam detectados e seu impacto potencial seja entendido

Implementar recursos de monitoramento contínuo de eventos de segurança cibernética e verificar a eficácia das medidas de proteção, incluindo atividades físicas e de rede

RESPONDER

Essa função concentra as atividades apropriadas para agir em caso de um incidente de segurança cibernética detectado e suporta a capacidade de conter o impacto de um possível incidente.

As atividades essenciais incluem:

Garantir que o processo de planejamento de resposta **seja executado** durante e após um incidente

Analisar o incidente para garantir uma resposta eficaz e apoiar as atividades de recuperação, incluindo análise forense e determinar o impacto dos incidentes

Gerenciar as comunicações com as partes interessadas internas e externas durante e após um evento

Realizar atividades de mitigação para evitar a expansão de um evento e resolver o incidente

Implementar melhorias incorporando as lições aprendidas com as atividades de detecção/resposta atuais e anteriores

RECUPERAR

Identifica atividades apropriadas para renovar e manter planos de resiliência e restaurar quaisquer recursos ou serviços que foram prejudicados por conta de um incidente.

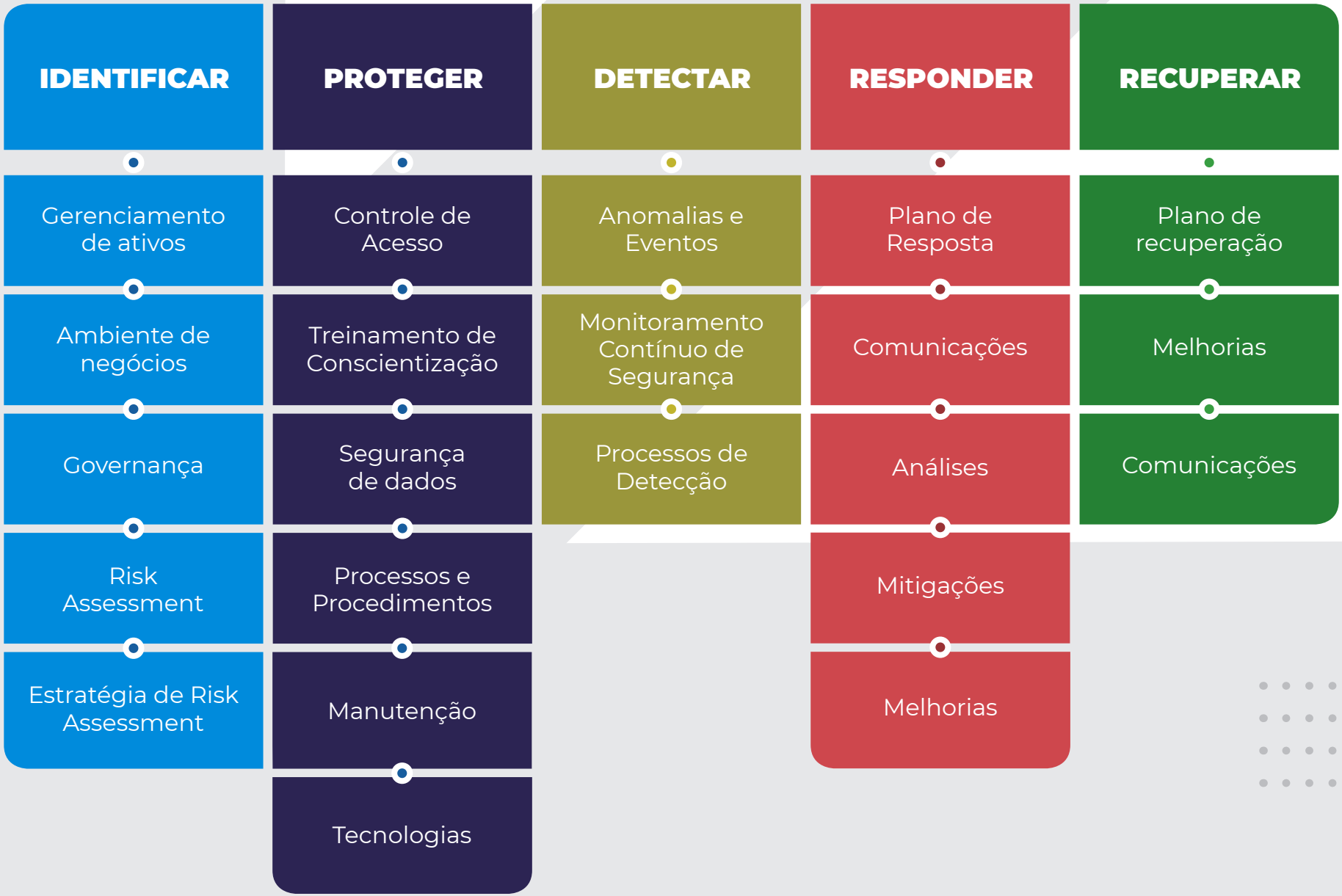
As atividades essenciais para esta função se sobrepõem um pouco às da fase anterior (Responder) e incluem:

As comunicações internas e externas são coordenadas durante e após a recuperação de um incidente de segurança cibernética

Garantir que a organização implemente processos e procedimentos de planejamento de recuperação para restaurar sistemas e/ou ativos afetados por incidentes

Implementação de melhorias com base nas lições aprendidas e revisões das estratégias existentes

NIST CYBER SECURITY FRAMEWORK



POR QUE DEVO ADOTAR O **NIST CYBERSECURITY FRAMEWORK**?

Primeiro, vamos dar um passo atrás e listar os problemas de segurança cibernética que provavelmente estão em primeiro lugar.

1. Você se preocupa **com riscos e vulnerabilidades invisíveis**.
2. Você **não tem um inventário preciso** dos ativos que precisam ser protegidos.
3. **Sua equipe gasta muito esforço** perseguindo itens que não terão impacto, enquanto você gostaria que eles se concentrassem no risco real.
4. Você **quer saber como lidar** com itens de risco com suas ferramentas atuais e o que está disponível no mercado.
5. Seus colegas fora da equipe de segurança **não entendem o risco cibernético** e, portanto, não conseguem entender tarefas críticas de mitigação.
6. Seu conselho está começando a perguntar sobre a **quantificação dos resultados de redução de risco** do plano estratégico de segurança cibernética que sua equipe está executando. “Estamos em conformidade com o **NIST**?”

A estrutura pode ajudá-lo com esses desafios. Com ela você será capaz de alavancar os aprendizados de pessoas que abordaram com sucesso problemas semelhantes.

O objetivo da estrutura é ajudá-lo a priorizar investimentos e decisões em segurança cibernética, além de raciocinar sobre a maturidade do seu programa e fornecer uma estrutura para conversas com as partes interessadas, incluindo a alta administração e seu conselho de administração.

USANDO O PACOTE DE APLICATIVOS DO **NIST NO ARCHER**

O pacote de aplicativos **Archer NIST- Aligned Cybersecurity Framework** fornece diretrizes diretas para **abordar e gerenciar riscos de segurança cibernética**. Os proprietários de perfis podem catalogar o estado atual, priorizar e definir o escopo dos elementos do perfil e definir seus resultados de estado desejados ou direcionados para o programa de segurança cibernética de sua organização.

Os avaliadores, então, avaliam esses perfis em relação às categorias do Cybersecurity Framework. Avaliações anteriores podem ser arquivadas para comparação com o perfil atual e medir o progresso. **Relatórios e painéis fornecem uma visão clara do estado atual da segurança cibernética** e do progresso que está sendo feito em direção ao estado desejado de segurança cibernética.

Com a oferta do Archer NIST- Aligned Cybersecurity Framework, **agências governamentais e empresas do setor privado podem avaliar e medir sua postura de segurança cibernética**, abordar lacunas e relatar a postura de segurança cibernética de uma maneira significativa que seja compreendida por todas as partes interessadas.

BENEFÍCIOS

- A metodologia concisa permite que as organizações entendam como seus esforços de segurança cibernética se comparam às orientações e fontes autorizadas do NIST.
- A linguagem comum garante uma comunicação clara dos requisitos e do progresso entre todas as partes interessadas, incluindo a equipe de segurança de TI, gerenciamento, parceiros, contratados, fornecedores e outros.
- A aplicação do NIST Cybersecurity Framework versão 1.1, lançada em abril de 2018 , e as melhores práticas de gerenciamento de risco melhoram a segurança cibernética e a resiliência da infraestrutura crítica, independentemente do tamanho da organização ou do nível de sofisticação da segurança cibernética.

CARACTERÍSTICAS PRINCIPAIS

- Priorizar e definir o escopo dos objetivos e prioridades de negócios da organização.
- Criar um perfil atual que indique o progresso em direção aos resultados desejados.
- Acompanhar as versões da biblioteca do NIST Cybersecurity Framework para avaliações de segurança cibernética.
- Avaliar o risco do ambiente operacional e identificar a probabilidade e o impacto de um evento de segurança cibernética.
- Identificar um perfil de destino que descreva os resultados de segurança cibernética desejados da organização.
- Analisar o perfil atual em relação ao perfil alvo por função, categoria, nível ou processo de negócios para determinar lacunas.
- Implementar um plano de ação para identificar as etapas necessárias para corrigir as lacunas.

SOBRE A **ATHENA SOLUÇÕES INTELIGENTES**

Somos uma consultoria com foco em **GRC | IRM – Governança, Riscos e Compliance, Segurança da Informação e LGPD**, formada por profissionais certificados e altamente experientes na condução de serviços e implementação de soluções próprias e de parceiros.

Utilizamos soluções robustas, líderes no quadrante mágico do Gartner e com ampla presença na nossa região.

Em nosso portfólio – Athena Professional Services – atuamos fortemente com **Implementação de Soluções, Serviços Pós Implementação de Soluções, Auditorias e Gap Analysis, Treinamentos e Consultoria**, com clientes de todos os segmentos de mercado em todo o país.

Nosso desafio é **construir soluções inteligentes e inovadoras** para ofertar ao mercado o que há de mais moderno e atualizado em GRC | IRM, Segurança da Informação e LGPD.

athenasolucoes.com

Fontes:

- Centro de Recursos de Roubo de Identidade (ITRC)
- NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework
- Relatório “2022 Cost of a Data Breach”
- “Cybersecurity Ventures”
- ESET

ATHENA
SOLUÇÕES INTELIGENTES