2019

White paper series
Publicação 5

NIST CYBERSECURITY FRAMEWORK

Uma abordagem abrangente da cibersegurança

OEA Mais direitos para mais pessoas

aws

— NIST CYBERSECURITY —
FRAMEWORK

Uma abordagem abrangente
da cibersegurança

CRÉDITOS

Luis Almagro

Secretário-Geral
da Organização dos Estados
Americanos (OEA)

Equipe técnica da OEA

Farah Diva Urrutia
Alison August Treppel
Belisario Contreras
Santiago Paz
Fabiana Santellán
Kerry-Ann Barrett
Nathalia Foditsch
Diego Subero
David Moreno
Mariana Cardona
Jaime Fuentes
Miguel Ángel Cañada

Equipe técnica da AWS

Abby Daniell
Michael South
Andres Maz
Melanie Kaplan
Min Hyun

CONTEÚDO

1. Introdução

Por conta do incremento continuado do número de incidentes de cibersegurança nos EEUU, o presidente Barack Obama, em 12 de fevereiro de 2013, emite a ordem executiva 13636 [1] onde pede ao Instituto Nacional de Padrões e Tecnologias (NIST) o desenvolvimento do Quadro de cibersegurança para a proteção de infraestruturas críticas, aquilo que hoje é conhecido como o Cybersecurity Framework (CSF). Os EEUU identificam 16 setores de infraestruturas críticas, estes são: setor químico; instalações comerciais; comunicações; manufatura crítica; presas/barragens; base industrial de defesa; serviços de emergência; energia; serviços financeiros; comida e agricultura; instalações governamentais; saúde e saúde pública; tecnologia da informação; reatores nucleares, materiais e resíduos; sistemas de transporte; sistemas de água e águas residuais. [18]

O Framework foi concebido sob as premissas de identificar as normas e diretrizes de segurança aplicáveis em todos os setores de infraestrutura crítica, dando uma abordagem flexível e repetível, que permite a priorização de atividades e aponta para a obtenção de um bom rendimento das infraestruturas, permanecendo rentável para o negócio.

É, sem dúvida, uma ferramenta para a gestão de riscos de cibersegurança, que habilita a inovação tecnológica e se ajusta a qualquer tipo de organização (sem importar o rubro ou tamanho).

O Framework tomou como estratégia se basear em padrões da indústria já aceites pelo ecossistema de cibersegurança (NIST SP 800-53 Rev.4 [2], ISO/IEC 27001:2013 [3], COBIT 5 [4], CIS CSC [5], dentre outros). Apresentam-se como uma estratégia de abordagem simples da governança da cibersegurança, permitindo transferis facilmente conceitos técnicos aos objetivos e necessidades do negócio. O seu desenvolvimento foi sob uma metodologia de participação, onde todas as partes interessadas (governo, indústria, academia) puderam participar e fornecer melhorias.

A principal inovação do CSF é deixar do lado padrões rígidos, que era a norma nesse momento; mas não foi o primeiro em desenvolver uma iniciativa para a proteção das infraestruturas críticas. A OTAN já tinha desenvolvido uma série de manuais dirigidos para a proteção de infraestruturas críticas para a defesa nacional, como ocaso do "Manual do Quadro de Trabalho de Cibersegurança Nacional" (National Cyber Security Framework Manual) [14]. Isto não quer dizer que o CSF de NIST exclua estes documentos, pelo contrário, os complementa e os melhora.

A grande diferença apresentada pelo CSF a respeito dos seus antecessores é a sua simpleza e flexibilidade; simplicidade para poder transmitir uma estratégia técnica nos termos que o negócio compreenda, e flexibilidade para se adaptar a qualquer organização. Esta diferença tem feito que, até hoje, a indústria e a comunidade técnica de todo o mundo tenham visto e aceite este quadro. Empresas, academia e governos têm adoptado de maneira voluntária o CSF como parte da sua estratégia de cibersegurança. Inclusive, organizações líderes na geração de normas e padrões tem incorporado o CSF, como por exemplo ISACA e ISO. Particularmente, ISO gerou a ISO/IEC TR 27103:2018 [6] que dá orientação sobre como aproveitar os padrões existentes em um quadro de cibersegurança, em outras palavras, como utilizar o CSF.

2. NIST Cybersecurity Framework (CSF)

2.1. História do CSF

O processo de desenvolvimento do Framework iniciou nos EEUU com a Ordem Executiva número 13636, publicada em 12 de fevereiro de 2013. A Ordem Executiva começou os esforços para compartilhar informação sobre ameaças de cibersegurança e para a constituição de uma série de abordagens atuais e bem-sucedidas, um quadro para a redução dos riscos da infraestrutura crítica. Através desta Ordem Executiva, NIST se encarregou do desenvolvimento do "Cybersecurity Framework".

Alguns dos requerimentos para o seu desenvolvimento foram: Identificar as normas e diretrizes de segurança aplicáveis em todos os setores de infraestrutura crítica; Fornecer uma abordagem prioritário, flexível, repetível, baseada no rendimento e rentabilidade; Ajudar na identificação, avaliação e gestão do risco cibernético; Incluir orientação para a medição do desempenho da implementação do Quadro de Cibersegurança; e Identificar áreas de melhoramento que devem ser abordadas através da colaboração futura com setores particulares e organizações que desenvolvem padrões.

Criação do Framework

O Framework foi, e ainda é, desenvolvido e promovido através do compromisso continuado e com a contribuição das partes interessadas do governo, a indústria e a academia. Para desenvolver o Framework, durante um ano, o NIST utilizou uma Solicitação De Informação (RFI) e uma Solicitação De Comentários (RFC), bem como uma ampla difusão e oficinas em todo os EEUU para: (i) identificar as normas de cibersegurança existentes, diretrizes, quadros e melhores práticas que eram aplicáveis para o aumento da segurança dos setores de infraestrutura crítica e outras entidades interessadas; (ii) especifique brechas de alta prioridade para as quais se necessitaram padrões novos ou revisados; e (iii) desenvolver planos de ação em colaboração através dos quais essas brechas possam ser abordadas.

Para a atualização do CSF para a versão 1.1 cuja publicação foi feita em abril de 2018, o NIST continuou com a sua estratégia de elaboração participativa dando passo a especialistas e indústria, bem como a governos e empresas não estadunidenses; como exemplo, o governo do Israel e a empresa Huawei Technologies participaram. [17]

2.2. Estrutura do CSF

O Cybersecurity Framework (CSF) consta de três componentes principais:

- Framework Core
- Níveis de implementação (Tiers)
- Perfis

Framework Core

O Core é uma série de atividades e resultados de cibersegurança desejados, organizados em Categorias e alinhados com Referências Informativas sobre padrões aceites pela indústria. É desenhado para ser intuitivo e atuar como uma camada de tradução para permitir a comunicação entre equipes multidisciplinares através do uso da linguagem simplista e não técnica.

O Core é constituído por três partes: Funções, Categorias e Subcategorias. Inclui cinco **funções** de alto nível: Identificar, Proteger, Detectar, Responder e Recuperar.

O seguinte nível para abaixo são as 23 **categorias**, divididas nas cinco funções. Foram desenhadas para cobrir a abrangência dos objetivos de cibersegurança para uma organização, sem serem demasiado detalhadas, cobrindo temas relativos aos aspectos técnicos, às personas e aos processos, com foco nos resultados.

As **subcategorias** são o nível mais profundo de abstração no Core. Há 108 Subcategorias, que são declarações baseadas em resultados que oferecem considerações para a criação ou melhoria de um programa de cibersegurança. Levando em conta que o Framework é orientado aos resultados e não estabelece a forma como uma organização deve alcançar esses resultados, permite implementações baseadas no risco que se adaptam às necessidades das diversas organizações.

Níveis de implementação do CSF

Os níveis descrevem o grau no qual as práticas de gestão de riscos de cibersegurança de uma organização exibem as características definidas no Framework. Os níveis vão de Parcial (Nível 1) a Adaptativo (Nível 4) e descrevem um grau cada vez maior de rigor, e quão bem integradas estão as decisões de risco de cibersegurança em decisões de risco mais amplas, e o grau no qual a organização compartilha e recebe informação de cibersegurança de fontes externas.

Mesmo se o NIST ressalta que os níveis não necessariamente representam níveis de maturidade, na prática são semelhantes. O mais importante é as organizações determinarem o nível desejado (não todos os controles devem ser implementados no nível mais alto), garantindo que o nível selecionado cumpre pelo menos com os objetivos da organização, reduz o risco de cibersegurança em níveis aceitáveis, têm um custo admissível e são fáceis de implementar.

Perfis

Os perfis são o alinhamento único de uma organização dos seus requerimentos e objetivos organizacionais, a tolerância ao risco e os recursos em relação aos resultados desejados do Framework Core. Os perfis podem ser utilizados para a identificação de oportunidades para melhorar a postura de cibersegurança comparando um perfil "atual" com um perfil "objetivo".

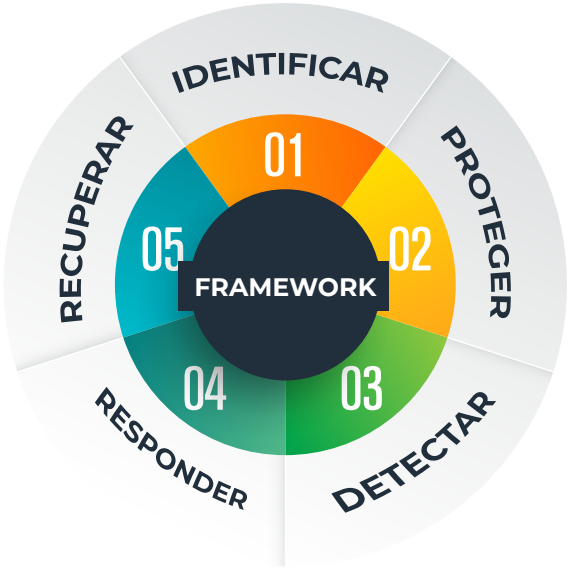
A identificação do perfil atual permite às organizações realizar uma revisão objetiva (sem implicar isso uma auditoria formal ou outras avaliações técnicas) do seu programa de cibersegurança em relação ao CSF e conhecer com certeza qual é a sua situação atual de segurança.

Levando em conta a avaliação do risco organizacional, os requerimentos de cumprimento e os objetivos organizacionais, é possível crias um perfil objetivo, que, em comparação com o perfil atual, informará a estratégia de liderança e as prioridades para a contratação, capacitação, mudanças de políticas, mudanças de procedimentos e aquisição de tecnologia.

2.3. Funções do CSF

As cinco funções incluídas no Framework Core são:

1. Identificar
2. Proteger
3. Detectar
4. Responder
5. Recuperar



As Funções são o nível mais alto de abstração incluído no Framework. Elas atuam como a coluna vertebral do Framework Core no qual se organizam o resto dos elementos.

Estas cinco funções foram selecionadas porque elas representam os cinco pilares principais para um programa de cibersegurança bem-sucedido e holístico. Elas ajudam às organizações a expressar facilmente a sua gestão do risco de cibersegurança em um alto nível e possibilitam decisões de gestão de riscos.

Identificar

Ajuda no desenvolvimento de um entendimento organizacional para a administração do risco de cibersegurança dos sistemas, das pessoas, dos ativos, dos dados e das capacidades. A compreensão do contexto empresarial, os recursos que respaldam as funções críticas e os riscos relativos à cibersegurança permitem a uma organização se centrar e priorizar os seus esforços, conforme a sua estratégia de administração de riscos e às suas necessidades comerciais.

Proteger

Descreve as medidas de segurança adequadas para garantir a entrega de serviços das infraestruturas críticas. Esta função contempla a capacidade de limitar ou conter o impacto de um potencial evento de cibersegurança.

Detectar

Define as atividades necessárias para a identificação da ocorrência de um evento de cibersegurança., permitindo o descobrimento oportuno dos próprios.

Responder

Inclui atividades necessárias para tomar medidas em relação a um incidente de cibersegurança detectado, desenvolvendo a capacidade de conter o impacto de um potencial incidente.

Recuperar

Identifica as atividades necessárias para a manutenção dos planos de resiliência e para a restauração de qualquer capacidade ou serviço que possa ter se deteriorado por conta de um incidente de cibersegurança. Esta função é compatível com a recuperação oportuna das operações normais para reduzir o impacto de um incidente de cibersegurança.

2.4. Versões e mecanismos de evolução

O CSF foi desenvolvido e promovido através do compromisso continuado e com a contribuição das partes interessadas no governo, na indústria e na academia. Isto inclui um processo público aberto de revisão e comentários, oficinas e outros mecanismos de participação.

A seguir, a gráfica apresenta a evolução do Cybersecurity Framework:

3. ¿Como usar o CSF?

O CSF se apresenta como uma ferramenta que permite administrar os riscos de cibersegurança de forma flexível e adaptável à realidade de qualquer organização, sem importar o tamanho ou rubro.

É importante ressaltar que o Framework não coloca novos controles nem processos, mas sim agrupa os controles colocados pelos principais padrões da indústria, internacionalmente reconhecidos como o NIST SP 800-53, ISO 27001, COBIT 5, dentre outros). Portanto, não substituirá os processos e controles já implementados na organização, mas a mesma continuará utilizando aquilo que já implementou e eventualmente complementará os próprios, para apresentar uma estratégia com uma abordagem executiva, orientada a resultados.

3.1. Estratégia para adotar o CSF

A seguir, apresentam-se três estratégias possíveis, colocadas no Framework [11], para o uso do CSF, sem serem as únicas.

Revisão básica de práticas de cibersegurança

Uma organização pode utilizar o Framework como uma parte chave do seu processo sistemático de gestão do risco de cibersegurança; ele não é desenhado para substituir os processos existentes, mas sim para determinar as brechas na sua abordagem atual de risco de cibersegurança e desenvolver um roteiro para a melhoria, permitindo a optimização dos custos e resultados.

Criação ou melhora de um programa de cibersegurança

O Framework é desenhado para complementar as operações de negócio e de cibersegurança existentes; e é possível tomá-lo como base para a criação de um novo programa de cibersegurança ou como ferramenta para a melhora de um programa existente.

Os seguintes 7 passos podem guiar a criação de um novo programa de cibersegurança ou melhorar um programa existente. Estes passos devem ser repetidos conforme necessário para melhorar e avaliar de forma continuada a cibersegurança:

Passo 1: Priorizar e determinar o escopo. É preciso identificar os objetivos de negócios bem como as prioridades de alto nível da organização. Com essa informação é possível determinar o alcance do programa de cibersegurança: qual linha de negócio ou processos serão abordados.

Passo 2: Orientação. Identificam-se os sistemas e ativos vinculados al alcance, aos requerimentos legais ou normativos, bem como à abordagem de risco geral.

Passo 3: Criar um perfil atual. É feita uma avaliação do programa de cibersegurança para criar um perfil atual, essa avaliação indicará quais resultados de categoria e subcategoria do Framework Core estão sendo atingidas atualmente. É fundamental que essa avaliação inclua Pessoas (quantidade de pessoal, funções de trabalho, habilidades e capacitação para profissionais de segurança e conhecimento geral do usuário), Processos (estratégia, políticas, procedimentos, manual x automatização, canais de comunicação com as partes interessadas, etc.), e Tecnologia (capacidades, configurações, vulnerabilidades, patches, operações e contratos de suporte, etc.).

Passo 4: Realizar uma avaliação de riscos. É realizada uma análise do entorno operativo para discernir a probabilidade de um evento de cibersegurança e o impacto que esse evento poderia ter na organização. É importante as organizações identificarem os riscos emergentes levando em conta a identificação das vulnerabilidades dos ativos e a informação de ameaças de cibersegurança de fontes internas e externas para a obtenção de uma melhor compreensão da probabilidade e o impacto dos eventos de cibersegurança. Embora este passo se foca na identificação de riscos de cibersegurança, é importante que este processo esteja alinhado com a avaliação de riscos organizacionais, bem como à avaliação de riscos de negócio para que exista uma retroalimentação nas avaliações.

Passo 5: Criar um perfil objetivo. É preciso focar o esforço na avaliação das Categorias e Subcategorias do Framework que descrevem os resultados desejados de cibersegurança da organização, levando sempre em conta a missão e objetivos do negócio, bem como aqueles requerimentos vinculados ao cumprimento legal ou normativo. As organizações também podem desenvolver suas próprias Categorias adicionais baseadas nos requerimentos de negócio, bem como nos requerimentos das partes interessadas externas, como as entidades do setor, os clientes e os sócios empresariais; sem esquecer que os não são apenas de corte técnico ou tecnológico, mas também associados ao pessoal e capacitação, políticas, procedimentos e outras necessidades administrativas.

Passo 6: Determinar, analisar e priorizar as brechas. Compara-se o Perfil Atual e o Perfil Objetivo para determinar as brechas. A seguir, cria um plano de ação priorizado para abordar as brechas (que refletem os promotores, os custos e os benefícios, e os riscos da missão) para atingir os resultados no Perfil Objetivo. Depois, a organização determina os recursos necessários para a abordagem das brechas, que incluem os fundos e a força laboral.

Passo 7: Implementar o plano de ação. Determinam-se quais ações tomar para abordar as brechas, caso houverem, identificadas no passo anterior e depois ajusta às suas práticas atuais de cibersegurança para atingir o Perfil Objetivo. É importante que as ações incluam todas as aristas da governança da cibersegurança: Pessoal (contratações, capacitação, formação, etc.); Tecnologia (soluções atuais, soluções comerciais disponíveis, novos desenvolvimentos, inovação, etc.) e Processos (políticas, processos e procedimentos adequados à necessidade e realidade da organização).

Comunicação dos requerimentos de cibersegurança às partes interessadas

O Framework pode oferecer um canal para expressar os requerimentos de cibersegurança aos sócios de negócio, clientes e provedores; particularmente aos provedores de serviços ou produtos vinculados à infraestrutura crítica da organização.

3.2. Principais desafios

O CSF tem o grande desafio de se adaptar a diversos setores, indústrias e até países. Ele não utiliza nenhum padrão específico para satisfazer os controles de cibersegurança, mas se abstrai deles aplicando uma abordagem conceptual e sugerindo uma lista de múltiplos padrões possíveis para satisfazer os requerimentos do controle. Assim, é possível ser utilizado em diversos âmbitos como Infraestruturas Críticas, Governo ou setor privado.

Claramente vai depender em grande medida do início de cada organização na hora de implementar o CSF para identificar quais são os principais desafios que deverão ser abordados pelas próprias. Em termos gerais, há alguns desafios que geralmente acontecem na maioria das organizações, esses desafios estão associados ao compromisso da alta direção para a adopção de uma estratégia de cibersegurança, a cultura do risco organizacional [16] e a falta de profissionais qualificados para poder liderar estes processos [15].

De acordo com o relatório da OEA "Cibersegurança: Estamos preparados na América Latina e o Caribe?" [12] publicado em 2016, os aspectos vinculados à política e à estratégia de cibersegurança dos países é um dos aspectos a reforçar em toda a região da América Latina e o Caribe; entendemos que a adopção deste tipo de enquadramentos pode contribuir positivamente para a elaboração das estratégias de cibersegurança dos governos (particularmente, na proteção das suas infraestruturas críticas) e no fortalecimento dos processos de colaboração regional.

4. Casos de estudo

O CSF é atualmente um quadro reconhecido pela comunidade técnica que contempla as melhores práticas no tocante à cibersegurança. Este quadro foi adotado por diversos países como parte da sua estratégia em cibersegurança e alguns deles até foram incluídos na sua legislação nacional. Dentro da série de países que adotaram o CSF é possível encontrar: Bermudas, Estados Unidos, Israel, Itália, Japão, Reino Unido, Suíça e Uruguai [13].

A seguir, apresentamos o estudo de dois desses casos com adopções de abordagem diferentes.

4.1. **Reino Unido -** Uma abordagem aberta

O Reino Unido conta com Quadro de Políticas de Segurança (HMG Security Policy Framework - SPF) [7] que é de cumprimento obrigatório para todos os departamentos de governo. Para colaborar na implementação do referido Quadro, foi desenvolvida uma série de guias que abordam os diversos aspectos da segurança, como o Padrão Mínimo de Cibersegurança (MCSS - Minimum Cyber Security Standard) [8].

O Padrão Mínimo de Cibersegurança é um desenvolvimento conjunto entre o governo do Reino Unido e o Centro Nacional de Segurança Cibernética (NCSC); ele foi publicado em junho de 2018 e é a aproximação mais próxima à CSF na normativa britânica.

Esse padrão define as medidas de segurança mínimas que os departamentos do Reino Unido devem implementar em relação à proteção da sua informação, tecnologia e serviços digitais para cumprir com as suas obrigações de SPF e Estratégia Nacional de Segurança Cibernética.

Este padrão toma as cinco funções do CSF (Identificar, Proteger, Detectar, Responder e Recuperar) e, embora algumas das funções e categorias, bem como a redação de cada uma delas têm sido modificadas, em geral são muito fieis ao CSF original.

As funções colocadas pelo MCSS são:

1. **Identificar:** Os departamentos devem implementar processos adequados de governança da cibersegurança.
2. Os departamentos identificarão e classificarão a informação sigilosa que tiverem.
3. Os departamentos devem identificar e classificar os serviços operacionais chave que fornecem.
4. A necessidade de os usuários terem acesso à informação sigilosa ou serviços operacionais chave deve ser entendida e administrada de forma continuada.

5. **Proteger:** O acesso à informação sigilosa e serviços operativos chave apenas será fornecido aos usuários ou sistemas identificados, autenticados e autorizados.

6. Os sistemas que administram informação sigilosa ou serviços operacionais chave devem estar protegidos contra a exploração de vulnerabilidades conhecidas.

7. As contas altamente privilegiadas não devem ser vulneráveis a ataques cibernéticos comuns.

8. **Detectar:** Os departamentos devem tomar medidas para detectar ataques cibernéticos comuns.

9. **Responder:** Os departamentos devem ter uma resposta definida, planejada e provada para os incidentes de cibersegurança que afetem a informação confidencial ou os serviços operativos chave.

10. **Recuperar:** Os departamentos devem ter processos bem definidos e provados para garantir a continuidade dos serviços operativos chave no caso de falha ou compromisso.

Igual do que o CSF, o MCSS deixa aberta de forma deliberada a implementação das diretrizes, já que se entende que tentar definir uma abordagem de cibersegurança única em diversas indústrias, plataformas e situações é quase impossível. Nesse sentido, as empresas são promovidas a interpretar o padrão de forma independente e adaptar os seus próprios processos de segurança para garantir o seu cumprimento.

4.2. **Uruguai** - Uma abordagem guiada

O Quadro de Cibersegurança de Uruguai (MCU) [9], tem como o seu objetivo principal a geração de confiança no uso da tecnologia, unificação de todos os recursos existentes em relação à cibersegurança, e sustentar a evolução do governo digital do Uruguai. Igualmente, procura promover uma visão integrada e multisetorial da cibersegurança, apostando ao aprimoramento continuado da segurança da informação e a contribuir para a definição de planos de ação.

A sua implementação esteve baseada no Core do CSF v1.0 (ISO/IEC 27001:2013, ISO 27799:2016 [10], COBIT 5 e NIST 800-53 rev.4), além disso contou com o trabalho de especialistas em segurança da informação, consultoras internacionais e a academia. Assim que elaborado o primeiro rascunho do MCU, ele foi elevado para a consideração da Universidade da República, donde foi analisado e apresentou às suas recomendações. Depois disso, foi elevado para a consideração de consultores privados do país e foram recolhidos também os seus comentários. Por fim, em agosto de 2016 foi publicada a sua versão 1.0

Hoje já foi utilizado para o diagnóstico e avaliação de todos os Ministérios do Governo Central, Governos Departamentais, Instituições de Saúde e instituições financeiras.

Adequação do CSF ao MCU

Embora o MCU toma todo o núcleo do NIST CSF v1.0, implementa apenas um conjunto de subcategorias, deixando para etapas posteriores a implementação das subcategorias restantes.

Esse Quadro apresenta uma série de **requerimentos** que incluem boas práticas sobre governança da segurança, gestão de riscos, controle de aceso, segurança das operações, gestão de incidentes e continuidade do negócio associados às diversas subcategorias do NIST CSF; além disso, inclui **perfil** de organização e um **modelo de maturidade** com o qual as organizações poderão definir as linhas de ação para melhorar a sua cibersegurança. Tais requerimentos têm adequações para organismos da Administração Central do Uruguai e para instituições de saúde; hoje, trabalha-se na adequação para instituições financeiras.

Requerimentos próprios
O MCU propõe uma série de 65 requerimentos gerados a partir dos controles ISO/IEC 27001 e da normativa uruguaia vinculada à cibersegurança.

Perfil de organização
As organizações se dividem em três perfis: básico, padrão e avançado. A designação do perfil é dada pela percepção do risco tecnológico. É importante esclarecer que apenas o perfil avançado inclui a totalidade das subcategorias adoptadas pelo MCU.

Priorização de subcategorias
Entendendo que as organizações não são todas iguais, e que dependendo do seu perfil poderiam ter que priorizar a implementação de algumas subcategorias antes do que outras; o MCU prioriza a abordagem das subcategorias do CSF com o intuito de facilitar a abordagem e a elaboração dos planos de ação.

Modelo de maturidade
Este modelo permite às organizações avaliar a sua posição atual e estabelecer conforme à sua priorização a meta de maturidade em cada subcategoria apresentada. Em termos gerais, os níveis estabelecem:

- **Nivel 0:** Ações vinculadas à cibersegurança quase ou totalmente inexistentes.

- **Nivel 1:** Há algumas iniciativas sobre cibersegurança. Abordagens ad-hoc. Alta dependência do pessoal. Atitude reativa diante de incidentes de segurança.

- **Nivel 2:** Há certas diretrizes para a execução das tarefas. Existe dependência do pessoal. Tem-se avançado no desenvolvimento dos processos e documentação das tarefas.

- **Nivel 3:** É caracterizado pela formalização e documentação de políticas e procedimentos. Governança da cibersegurança. Métricas de acompanhamento.

- **Nivel 4:** O Responsável da Segurança da Informação (RSI) tem uma função chave no controle e melhora do SGSI. Realiza-se o controle interno. Trabalha-se na melhora continuada. A cibersegurança está alinhada com os objetivos e estratégias da organização.

Qualquer organização pública ou privada poderá usar o documento como ferramenta de autoconhecimento e melhora dos seus níveis de segurança. Até hoje, a sua adopção não é obrigatória, embora é previsto em curto prazo a sua obrigatoriedade para alguns setores críticos.

5. Conclusões

As ameaças de cibersegurança continuam crescendo e afetam a todas as organizações sem importar o rubro ou tamanho.

Embora o CSF foi concebido inicialmente como uma ferramenta para a avaliação da cibersegurança nas Infraestruturas Críticas dos EEUU, a sua abordagem, agnóstica do ponto de vista dos padrões e requerimentos tecnológicos, tem demonstrado que se adapta perfeitamente a diversos setores e países, e resulta de fácil adopção nos processos de auditoria.

O CSF pode ser utilizado para gerar um novo programa de cibersegurança ou como uma ferramenta para a análise da brecha de programas de cibersegurança existentes e melhorá-los. Ele está estruturado de forma a permitir uma abordagem integrada da governança da cibersegurança, alinhando essa abordagem facilmente às necessidades do negócio.

As subcategorias do CSF foram mapeadas aos controles dos principais padrões da indústria, permitindo uma consolidação dos próprios, e oferecendo uma abordagem flexível e clara.

Por fim, o CSF tem que ser percebido como uma ferramenta de gestão de riscos de cibersegurança que permite a avaliação da efetividade dos controles e a rentabilidade dos próprios.

Os programas de cibersegurança melhor sucedidos são aqueles que não estão baseados simplesmente na aplicação de controles técnicos, mas sim que definem uma estratégia, um quadro, para abordar cada uma das funções essenciais de cibersegurança: identificar o contexto, proteger os sistemas e ativos, detectar os desvios, responder antes incidentes e recuperar as operações do negócio. Em resumo, a cibersegurança é um problema do negócio que apenas pode ser resolvido com uma una visão holística das Pessoas, Processos e Tecnologia.

6. Referências

[1] Casa Blanca (2013), *Orden ejecutiva 13636:* https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[2] NIST (2013), *NIST 800-53 Rev.4:* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

[3] ISO (2013), *ISO/IEC 27001:* https://www.iso.org/standard/54534.html

[4] ISACA (2012), *COBIT 5:* http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

[5] CIS (2018), *Critical Security Controls (CSC):* https://www.cisecurity.org/controls/

[6] ISO (2018), *ISO/IEC TR 27103:* https://www.iso.org/standard/72437.html

[7] Gobierno de Reino Unido (2013), *Marco de Políticas de Seguridad de Reino Unido:* https://www.gov.uk/government/collections/government-security

[8] Gobierno de Reino Unido (2018), *Marco de ciberseguridad de Reino Unido:* https://www.gov.uk/government/publications/the-minimum-cyber-security-standard

[9] AGESIC (2018), *Marco de Ciberseguridad de Uruguay:* https://www.agesic.gub.uy/innovaportal/v/5823/1/agesic/marco-de-ciberseguridad-v40.html

[10] ISO (2016), *ISO 27799:* https://www.iso.org/standard/62777.html

[11] NIST (2018), *CSF v1.1 (en español):* https://www.nist.gov/sites/default/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

[12] OEA (2016), *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?:* https://publications.iadb.org/es/publicacion/17071/ciberseguridad-estamos-preparados-en-america-latina-y-el-caribe

[13] NIST, *Adaptaciones internacionales del CSF:* https://www.nist.gov/cyberframework/international-resources

[14] OTAN (2012), *National Cyber Security Framework Manual:* https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf

[15] ISC2 (2017), 2017 *Global Information Security Workforce Study - Benchmarking Workforce Capacity and Response to Cyber Risk (LATAM):* https://iamcybersafe.org/wp-content/uploads/2017/06/LATAM-GISWS-Report.pdf

[16] Deloitte (2016), *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información:* https://www2.deloitte.com/pe/es/pages/risk/articles/la-evolucion-de-la-gestion-de-ciber-riesgos-y-seguridad.html

[17] NIST (2018), RFC - *Cybersecurity Framework Draft Version 1.1:* https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11

[18] Homeland Security, *Sectores de infraestructura crítica:* https://www.dhs.gov/cisa/critical-infrastructure-sectors

7. Fontes

NIST, *Sitio web oficial del CSF*:
https://www.nist.gov/cyberframework/

NIST, *Historia y creación del CSF:*
https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

NIST, *Estructura del CSF:*
https://www.nist.gov/cyberframework/online-learning/components-framework

NIST, *Funciones del CSF:*
https://www.nist.gov/cyberframework/online-learning/five-functions

NIST, *Evolución del CSF:*
https://www.nist.gov/cyberframework/evolution

AWS, *NIST Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud*:
https://d1.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.246c0a886c7d16d2b370c20a04f99511d212613a.pdf

— NIST CYBERSECURITY —
FRAMEWORK

Uma abordagem abrangente
da cibersegurança

2019

White paper series
Publicação 5

OEA | Mais direitos para mais pessoas

aws

NIST CYBERSECURITY FRAMEWORK

Uma abordagem abrangente da cibersegurança