NOTA TÉCNICA AVALIAÇÃO NIST CYBERSECURITY FRAMEWORK

REVISÃO 2.0

MAIO 2024

future

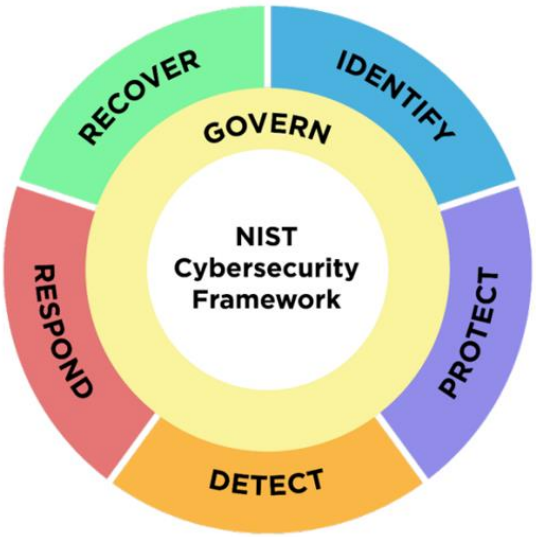
SUMMARY

Introdução

O Cybersecurity Framework do NIST 2.0 (CSF Framework) é um framework de segurança da informação que serve para avaliar o nível de maturidade do ponto de vista de segurança da informação de uma organização de uma forma geral.

Esta avaliação é realizada através de um questionário, que está dividido em 6 áreas (GV – Govern, ID – Identity, PR – Protect, DE – Detect, RS – Response e RC – Recovery) e estas áreas possuem subitens com questões relacionadas a fim de obter uma nota de 1-5 para avaliar o nível de maturidade de cada controle de segurança do ponto de vista de Política e do ponto de vista da Prática. De acordo com as respostas atribuídas a cada subitem é calculado a média para atribuir o nível de maturidade da área.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



A meta é que a empresa tenha pelo menos nível de maturidade nível 3 – Definido tanto para a Política, quanto para a Prática, conforme as expectativas da Tabela a seguir.

Tabela de Níveis de Maturidade

Nível	Expectativa da Política	Expectativa da Prática
1 – Inicial	A política ou o padrão NAO existe ou NÃO é formalmente aprovada pela organização.	O processo padrão e, portanto, a prática NÃO existe.
2 – Repetido	A política ou o padrão existe, mas ele NÃO é revisado há mais de 2 anos.	O processo existe, mas ele é executado informalmente.
3 – Definido	A política e o padrão existem com aprovação formal da organização. Exceções à Política são documentadas e aprovadas e ocorrem menos de 5% do tempo.	O processo formal existe e está documentado e as evidências são comprovadas na maior parte das atividades com exceções em menos de 10% do tempo.
4 – Gerenciado	A política e o padrão existem com aprovação formal da organização. Exceções à Política são documentadas e aprovadas e ocorrem menos de 3% do tempo.	O processo formal existe e está documentado e as evidências são comprovadas em todas as atividades com detalhamento das métricas do processo. As métricas mínimas estão estabelecidas. As exceções ocorrem em menos de 5% dos casos.
5 – Otimizado	A política e o padrão existem com aprovação formal da organização. Exceções à Política são documentadas e aprovadas e ocorrem menos de 0,5% do tempo.	O processo formal existe e está documentado e as evidências são comprovadas em todas as atividades com detalhamento das métricas do processo. As métricas mínimas estão estabelecidas. As exceções ocorrem em menos de 1% dos casos.