November 04, 2023

COMMENTS ON NIST CYBERSECURITY FRAMEWORK 2.0 CORE DRAFT

Submitted to:
National Institute of Science and Technology

Submitted By:
Roberto Puyó Valladares
Government Digital Transformation | CIO | Senior LA ISO/IEC 27001 | CISM | CRISC | C|CISO | Past-President Information Systems Security Association (ISSA) Lima, Perú Chapter

Thank you for the opportunity to contribute to the NIST CYBERSECURITY FRAMEWORK 2.0 CORE DRAFT. From the perspective of Latin American professionals,

I believe that people are one of the main pillars of security. Therefore, consistently enhancing security controls for human resources throughout their involvement in a company is of utmost importance.

Please do not hesitate to contact me if you have any questions. I am happy to keep collaborating with NIST on this project.

Category	Subcategory	Implementation Examples (Suggestions by Roberto Puyó)	Discussion
Roles, Responsibilities, and Authorities (GV.RR)	GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)	Ex5. Conduct periodic police and judicial background checks on employees who are assigned to sensitive roles.	Regularly conducting law enforcement and court background checks on personnel assigned to sensitive roles is essential to safeguard the organization's integrity and maintain trust. This proactive approach ensures that those with a record of criminal activity are not placed in positions that could compromise security or sensitive information, thus reducing risks and enhancing the overall safety and credibility of the company.
		Ex6. Consider regularly assessing the emotional well-being of employees in cybersecurity-sensitive positions.	Regularly assessing the emotional well-being of employees in cybersecurity-sensitive positions is vital to maintain a resilient and efficient security team. This not only addresses potential stressors but

Category	Subcategory	Implementation Examples (Suggestions by Roberto Puyó)	Discussion
			also improves their overall job satisfaction and performance, ultimately contributing to a more robust and secure organizational environment.
		Ex7. Define a formal accountability process that includes actions to be taken against personnel who do not comply with the cybersecurity policies and procedures.	Implementing a formal process for accountability in cybersecurity is important for protecting sensitive data and maintaining the integrity of your organization's digital assets. This will ensure everyone is aware of the consequences of non-compliance, acting as a strong deterrent against security breaches, and an essential part of building a solid defense against cyber threats.
		Ex8. Cybersecurity awareness should be required when granting access to critical assets to staff.	Ensuring that staff have a good understanding of cybersecurity is crucial before granting access to important assets. It helps to protect our digital infrastructure, lower risks, and safeguard confidential data from potential threats.