Gustavo Javier Speranza

Cybersecurity & Transformational Manager

Hey there! I'm a cybersecurity enthusiast with more than 11 years of hands-on experience working in various information security roles. Currently, I'm the Sr. Manager, LATAM Information Security Officer at The Walt Disney Company, where I get to expand the company's security program in the LATAM region and work closely with awesome tech and business teams.

Throughout my career, I've dived into many aspects of cybersecurity, such as governance, risk management, vulnerability management, and assessments. I've also led security initiatives and made sure everything stays on the right side of the law while spreading the word about the importance of staying secure in the digital world.

I've always enjoyed creating a positive and inclusive work environment, supporting my team members, and building great relationships with everyone involved. I also love sharing my knowledge and insights on cybersecurity through my blog, 0dayroot.net.

I'm all about staying ahead of the game, safeguarding what matters most, and always looking for ways to improve in the ever-changing world of information security. I truly believe in teamwork, learning, and creativity to make a real difference in this exciting field!

https://gussj.github.io

Schedule time with me

Email me

Download PDF

Subscribe to resume

updates

Experience

The Walt Disney Company

Sr. Manager, LATAM Information Security Officer • Jun, 2022 — Present

Responsible for extending and localizing the enterprise security program in the LATAM region, and act as a subject matter leader for regional technology and business teams.

- Analysis of known and emerging threats to determine risks against TWDC assets
- Security Programs leader
- Creation, maintenance, governance and communication of security policies and standards across TWDC
- Act as SME for technology and business
- Assessment and audit of compliance against the security policies and standards
- Overseeing control assurance, monitoring, and remediation
- Assurance that TWDC assets are effectively managed and monitored to meet TWDC security criteria
- Managing information security risk
- Ensuring alignment with legal and regulatory requirements
- Delivering information security awareness, education, and training
- Publishing the status of Corporate's information security posture

Kimberly-Clark

Global Cybersecurity Architect, Engineer & Technology Risk Manager • Aug, 2018 — Jun, 2022

Leader of Global Cybersecurity Architects, Engineers & Technology Risk Team in Kimberly-Clark.

- Information security governance and management

- Security Programs leader
- Budget Planning
- Act as SME for technology and business
- Analysis of known and emerging threats to determine risks against assets
- Creation, governance and communication of security policies and standards
- Assessment and audit of compliance against the security policies and standards
- Risk Analysis in complex environments
- Development, coaching, recruiting, training and retaining staff
- Deployment and configuration of identity and access management solutions to enhance security and streamline user authentication processes.
- Implementation of security platforms to establish and maintain robust network security measures, including firewall configuration and threat prevention.
- Implementation and management of CASB to enforce data protection policies and secure cloud-based applications and services.
- Technology Stack:
    - OT Environment (Purdue Model, automation, sandboxing)
    - Palo Alto
    - Okta
    - Azure
    - CSPM
    - Splunk
    - Zscaler

KPMG Argentina

Head of Security • Apr, 2013 — Aug, 2018

CyberSecurity Manager for KPMG Argentina.

- Vulnerability Management
- Security Programs leader
- Act as SME for Regional and Global CyberSecurity consulting
- Manage the development of strategic IT risk insight programs through detailed industry research and partnerships
- Design and execution of high quality, thorough cybersecurity maturity assessments and threat risk assessments
- Network & infrastructure security
- Cyber transformation
- Data protection

DIP

CISO • Jun, 2010 — Apr, 2013

Chief Information Security Officer for a government agency.

- Oversees the development and implementation of Enterprise Information Security programs/services/initiatives, including strategies, plans, methods, tools, and processes to advance the overall security framework and to ensure the protection of all enterprise information assets through advanced, mature, state-of-the-art capabilities.
- Provides leadership in executing programs, services or initiatives to deliver on the strategy
- Develop an enterprise Information Security Program strategy and the roadmap aimed at proactively identifying and remediating security risks.
- Provided leadership of concurrent project initiatives and service improvements aimed at building a corporate culture of information and technology security awareness and risk mitigation.
- Design and execution of high quality, thorough cybersecurity maturity assessments and threat risk assessments
- Leads the section and its staff to support an environment and culture of service excellence which respects diversity, encourages all employees to work together to achieve results and contribute to a healthy, rewarding and productive working environment.
- Developed and managed relationships and consultation with stakeholders impacted by section programs, services and initiatives to identify trends, issues and priorities.
- Manages relationships with service providers, external vendors and partners.

Education

Universidad de Palermo

Bachelor in Cybersecurity • 2022 — 2025

In Progress

Cybersecurity Bachelor

ISTEA

Tecnicatura Superior en Soporte de Infraestructuras • 2014 — 2016

Completed

This career arises with the aim of providing a vocational training oriented to the infrastructure of a company. Now there is this new career for all those who work or want to work in the area of Server Administration, Operating Systems, Networks and Computer Security that grants them an official title of national validity and a technical training oriented to this activity. This is an associate degree.

Sans

Securing Web Apps, APIs, and Microservices (SEC522) • 2024

In Progress

Web Applications are increasingly distributed. What used to be a complex monolithic application hosted on premise has become a distributed set of services incorporating on-premise legacy applications along with interfaces to cloud-hosted and cloud-native components. Because of this coupled with a lack of security knowledge, web applications are exposing sensitive corporate data.

Microsoft

Azure Security Engineer (AZ-500) • 2024

Completed

Implement, manage, and monitor security for resources in Azure, multi-cloud, and hybrid environments as part of an end-to-end infrastructure.

Amazon Web Services

Security Engineering on AWS • 2024

Completed

Security Engineering on AWS will enable you with the skills and knowledge to safeguard your organization's reputation and profits, and improve security operations.

Archer Academy

Developing Archer Power Users and Business Analysts • 2023

Completed

This course will teach participants how to "Think Archer" and to effectively create Archer specific business requirements and map workflows. The course fosters the development of Archer Power-users and Business Analysts within your organization to bridge the knowledge-gap between standard Archer Users and System Administrators.

Universidad Siglo 21

Systems and Network Security Audits • 2014 — 2015

Completed

Aimed at security officers, auditors, security professionals, site administrators and anyone involved in the integrity of the network infrastructure.

ADACSI

BIA - Business Impact Analysis • 2018

Completed

This Workshop provides a method to carry out a business impact analysis (BIA) within an organization, based on what is indicated in the international standard ISO 22317, and developing the activities with practical examples that will provide the participants with the knowledge initial to perform this task within your own organization. Through this Workshop, good practices and guidelines are recommended that will help establish, implement and maintain a formal and documented process for business impact analysis. In turn, there is no uniform procedure for conducting this analysis, but from this activity you receive the necessary help to design a BIA process that suits your needs and your organization.

Cybrary

Advanced Penetration Testing • 2017

Completed

Aggressive systems require aggressive hackers. Advanced Penetration Testing training embodies that notion. It's an intense approach to the world of exploitation and pentesting set in the highest security environments around. In our free online Advanced Penetration Testing training class, you'll learn how to challenge traditional practices and use alternate methods and software in penetration testing. Cover how to attack from the web using cross-site scripting, SQL injection attacks, remote and local file inclusion and how to understand the defender of the network you're breaking into to. You'll also learn new tricks for exploiting a network and the post-exploitation process—how to backdoor SSH logins, enable RDP/VNC and additional data exfiltration techniques. It's a headfirst dive into the world of advanced pentesting, and there are no life jackets—only binaries

Neosecure

FIREWALL "7.1" CONFIGURE EXTENDED FEATURES(EDU-205) • 2016

Completed

Firewall "7.1" Configure Extended Features is the next-level, follow-on course to Firewall "7.1" Install, Configure, and Manage (EDU-201). The two-day, instructor-led Firewall "7.1" Configure Extended Features course expands on 201 course topics while introducing many new features and functions of Palo Alto Networks next-generation firewalls.

Neosecure

FIREWALL 7.1 INSTALL, CONFIGURE, AND MANAGE(EDU-201) • 2016

Completed

The Firewall "7.1" Install, Configure, and Manage three-day, instructor-led course will enable the student to install, configure, and manage the essential features of Palo Alto

Networks® next-generation firewalls.

Universidad CAECE

Certification in Information Security Management • 2012

Completed

Information Security Management, is a Business and Technical Training specialization, designed for all professionals, professionals of the area and students with the desire to grow and develop in a new discipline within the Information Sciences - Information Security - and who exercise or aspire to hold management positions that require the knowledge and skills necessary for the role of CSO, Chief Security Officer.

EducacionBIZ

Executive Program in Project Management • 2015

Completed

The Executive Program outlines the methodology proposed by the Project Management Institute (PMI) to manage projects as a Project Manager. Organizations live from and through projects. These are born, develop and meet certain goals and their proper planning and control depends on whether they are successful or not. In this course you will acquire the necessary knowledge for the professional management of projects and you will know in detail the processes that compose it, which will allow you to direct projects, regardless of their type or the industry in which you perform, applying the best practices in the market. During the course will be developed all the documents necessary to manage professionally from start to finish a project.

ETEK-Reycom

Computer Hacking Forensic Investigator • 2012

Completed

CHFI (Computer Forensic Investigator Hacking) is the official certification of forensic investigator accredited by the EC-Council. The objective of this certification is to acquire practical knowledge, to detect attacks by a hacker and to properly extract the evidence to report cyber crimes, as well as conducting audits to prevent future attacks. Computer forensics is the application of methods and techniques to obtain, analyze and preserve digital evidence that can be eliminated or altered. This allows to gather evidence to advance a criminal action.

ISACA

Ethical Hacking & Penetration Testing • 2011

Completed

CentralTech

CISSP • 2011

Completed

It is a high-level professional certification awarded by the International Information Systems Security Certification Consortium (ISC) 2, with the aim of helping companies recognize professionals with training in the area of information security. CISSP is considered one of the most representative credentials in the field of computer security worldwide.

ETEK-Reycom

Risk Management ISO 27005 2008 • 2012

Completed

CentralTech

MCITP EA • 2012

Completed

The Microsoft Certified IT Professional (MCITP) certification helps validate that an individual has the comprehensive set of skills necessary to perform a particular job role, such as database administrator or enterprise messaging administrator. MCITP certifications build on the technical proficiency measured in the Microsoft Certified Technology Specialist (MCTS) certifications. Therefore, you will earn one or more MCTS certifications on your way to earning an MCITP certification.

SENA

Computer Controls and Security • 2012

Completed

The audit should begin with the administrative part and then follow the applications part evaluating all the elements related to the systems but not before having analyzed everything related to personnel, equipment purchase, planning, control, etc.

SENA

Networking and Security • 2012

Completed

Instituto Dr. Mariano Moreno

High school in Economics and Management of organizations • 2004

Completed

Languages

Spanish

Native

English

Advanced - TOEIC 870

Certifications

CHFI (Computer Hacking Forensics Investigator)

EC-Council • 2014

Certificate Number ECC13248628089

Skills

Experience 5+ years

- AD Admin
- Splunk
- Symantec EPP
- DLP (Microsoft)
- Palo Alto Firewall
- Qualys

Experience 4 years

- OKTA
- Microsoft CASB
- Prisma CSPM
- Azure Security Architect
- Zscaler

Experience 1 year

- Wiz CSPM
- Crowdstrike

- Tenable