CyberSecurity Governance and Privacy Forum

(Spanish Model & Exchange of Experince)

19-22 February, 2024

Hyatt Regency Hotel, Madrid, Spain

Jesus Castellanos

International IT security consultant, Relational Tools S.L.

Director of Product and Design of

Cybersecurity Services

CDPP Certified Data Privacy Professiona

ITIL Certified Service Strategyl

ICA Sistemas y Seguridad, Spain

Victor Betrán Paños

CEO Grupo BG Media

Lecturer in Esade, ISDE and EUHT

Digital and communications Security Expert

SME Certified Management SGE900

International Standard, Spain

Ivan San Ciriaco Frutos

Professional with Experience in the Armed Forces

of the Spanish Ministry of Defense

Certified, Spanish Cybersecurity Institute (INCIBE)

National Security Scheme by CCN-CERT

Certified LPIC 101 and 102-500, Spain

Asunción De Ávila

Head of Cybersecurity Operations at ICA Systems

Project Manager, Group ICA

IBM Certified Deployment Professional

Security Qradar QVM, SPAIN

Tel: +965 22455719 Fax: +965 22455728 Cell/WhatsApp: +965 90939008 P.O. Box 2277 Safat 13023, Kuwait

Email: marketing@consulenzakw.com Web: www.consulenzakw.com

1.1 Forum Description

Nowadays, more and more Inistitutions suffer financial damage because hackers from various origins abuse vulnerabilities in a process, system, network, application or infrastructure. These are Nation state actors, hackers commissioned by companies to steal Intellectual property, Hackers who use an environment as a test object, crackers who do damage to get ransom or just script kiddies who find something. But even hackers who get hacked again can pose a risk.
In addition, Cyber security, information security and privacy are often seen as separate disciplines for which different people are also responsible for in a Inistitutions (Chief Information Security Officer (CISO), Computer Emergency Response Team (CERT) or Data Protection Officer (DPO)). However, these disciplines can all be well integrated based on risk management and information security management systems, like Cobit 5 and ISO27001. During this training you will receive concrete information about what is (legal, technical and organizational) expected of you with regard to Cyber security and how you can get started with this in practice. The trainers draw up an effective (cyber) security and privacy approach with you that integrates people, processes and technology. Together with you, they look for the balance where privacy and security reinforce each other instead of opposing them. During the training you work on cases and assignments where the theory is linked to your daily practice.

1.2 Prior Knowledge

We expect from the attendees and senior officials that they understand the basics of information security in working and thinking levels, some insight into management systems and basic knowledge of the new GDPR legislation would be desirable. Some technical knowledge of networks, systems and applications is an advantage.

1.3 Trainer

Your highly experienced and leading trainers are experts in the field of cybersecurity and privacy and work together with several universities worldwide. Next to that they are able to assist you with advice and many tips and practical examples.

1.4 Program Topics

- Introduction and household announcement
- Information security and Cyber Security
- Financial transfers and secure payment systems
- The role of a baseline measurement, audit, control or review.
- ASSIGNMENT: SCOPING
- Human aspects around information security.
- Standards and frameworks for Cyber Security.
- Risk management, Information Security Management System.
- Selection of security measures.
- Privacy aspects of information security.
- The risk of interfacing systems and data.
- Data breach reporting obligations.
- ASSIGNMENT: EXAMPLE DATA BREACH.
- Privacy issues within organizations.
- Security Incident and incident response.
- Privacy and Governance.
- Business Continuity , Audits and results.
- Security Scans, - DEMO: How to hack a user account.
- Penetration testing and Red Team / Blue Team testing.
- Access control (Identity Management & Access Control / IAM).

1.5 Forum Topics schedule

Day 1: 19 February, 2024

- Information security and Cyber Security
- Human aspects around information security
- Standards and frameworks for Cyber Security
- Risk management
- Information Security Management System (ISMS)
- Selection of security measures

Day 2: 20 February, 2024

- CyberSecurity Privacy
- Data Data breach reporting obligation
- Privacy issues within organizations
- Financial transfers and secure payment systems
- Security Incident and incident response

Day 3: 21 February, 2024

- CyberSecurity Governance
- KPIs for ensuring privacy
- Audits and results , Security Scans
- Penetration testing and Red Team / Blue Team testing
- Access control (Identity Management & Access Control / IAM)

Day 4: 22 February, 2024

- General Discussion
- Questions and Inquiries
- Attendance Certificates

CONSULENZA GLOBAL
CONSULTATIONS & CONFERENCE
INTERNATIONAL TRAINING