Technical Conference 14-3-2022

Cybersecurity and Business Continuity

Organized: GT Business Continuity, Business Management Comission at Enginyers Industrials de Catalunya

Content:

In the recent context 2020 2022 the real threats type "black swan" (bacteriological, raw material deficit, increase in energy prices, cyberattacks, supply chain, meteorological, with an interdependence effect) have hatched, and have impacted on the activity of companies, often disrupting their operations, affecting the supply of services and production for their customers. A company with projection and face to face its challenges and objectives must, if not have its own "Business continuity System", it must have Operational Continuity Plans to face disruptive events, to guarantee its activity, and competitiveness in a totally changing market andcontext.

On the day 14-3-2021 we will visualize the VECTOR CYBERSECURITY as a threat to continuity, visualizing --in first-level companies both national and international-- how they are prepared both from the preventive point of view, as for the corrective through their Recovery Plans (Recovery Plan) to activate together with the Crisis Committee when the disruptive incident is unleashed.

The 2 different IT and OT aspects as well as their interrelationship will be visualized; IT focused on the servers themselves and office computer equipment with their ERP, cloud and equivalents, such as OT focused on operations (machinery, mobile logistics units, devices) with their respective PLCs, SCADA, sensors, as well as the OT-IT interconnection itself.

In the preventive part in IT we will visualize from redundancy of high availability equipment, management and change of passwords, early warning services via SOC (security operations center). In OT; vulnerability update policies, disposition and update of the firmware of the different "devices", segmentation of systems & network architecture, the use of ISA / IEC 62443, trends of cyber product certification,...

In the corrective focused on the "Recovery PLans", or the recovery plans with their objective recovery times (RTO) detailing how we have the organization, people, equipment, and communications to gradually raise the systems and ultimately the critical or essential activity of

the company.
All this will be visualized under a prism of system integration supported by the international standards ISO- 27001--Information Security, and Iso-22301 --Business Continuity System , which ultimately give us a framework and guarantees of success.

In the second part of the day we will visualize and complement with aspects of Integrity and Reliability of the data, while we will see the support that companies have for official bodies both in preventive matters and guides, as well as especially in corrective matters and / or crisis situations.

In short, we will learn to know guidelines and tips to implement a system of continuity of operations and business, this time under the cyber threat, and with the premise of achieving Cybersilience for our entity and / or business unit.

Speakers: **Francisco Lázaro-- RENFE,** Glenn Rittereiser- **MAERSK ,** Oriol Torruella **- Agencia de Ciberseguretat de Catalunya ,** Daniel Mercader **AEPD -Agencia Española de Protección de Datos ,** MA.Estruga **- GT Business Continuity-COEIC,** Ignasi Fontanals **, i** Sergi Gil **- GT Business Continuity-COEIC**

Place and timetable: 10h-14h Vía Laietana 39, 5th floor. Enginyers Industrials Superiors de Catalunya . Barcelona

Inscriptions

MAERSK

renfe

AGÈNCIA DE
CIBERSEGURETAT
DE CATALUNYA

Enginyers
Industrials de Catalunya