Enginyers Industrials de Catalunya

14-3-2022

Ciberseguridad y Continuidad de Negocio

Organiza: GT Business Continuity de la Comisión Gestión Empresarial

Contenido:

En el reciente contexto 2020 -2022 las amenazas reales tipo “black swan” (bacteriológicas, de déficit materia prima, encarecimiento de la energía, ciberataques, de supply chain, meteorológicas, con un efecto interdependencia) han eclosionado, y han impactado en la actividad de las empresas llegando en muchas ocasiones a la disrupción de sus operaciones, afectando al suministro de servicios y producción destinado a sus clientes. Una empresa con proyección y de cara para hacer frente a sus retos y objetivos deberá, sino disponer de un propio “Business continuity System ”, si disponer de planes de Continuidad Operacional hacer frente a eventos disruptivos , para garantizar su actividad, y competitividad en un mercado y contexto totalmente cambiante.

En la jornada 14-3-2021 visualizaremos el VECTOR CIBERSEGURIDAD como amenaza para la continuidad, visualizando, en empresas de primer nivel tanto nacionales como internacionales, como están preparadas tanto desde el punto de vista preventivo, como para el correctivo a través de sus Planes de Recuperación (Recovery Plan) a activar junto alcomité de Crisis al desatarse el incidente disruptivo.

Se visualizarán las 2 diferentes vertientes IT, OT así como su interrelación; la IT centrado en los propios servidores y equipos informáticos de oficina con sus ERP, cloud y equivalentes, como la OT centrada en operaciones (maquinaria, unidades móviles logísticas, devices) con sus respectivos PLC , SCADA, sensores , así como la propia interconexión OT-IT .

En la parte preventiva en IT visualizaremos desde redundancia de equipos de alta disponibilidad, gestión y cambio de contraseñas, servicios de alerta temprana vía SOC (security operations center). En OT; políticas de actualización de vulnerabilidades, disposición y actualización del firmware de los diferentes “ devices “, segmentación de sistemas & arquitectura de la red, la utilización de ISA/ IEC 62443 , tendencias de certificación ciber de productos,.....

En la correctiva centrada en los “Recovery PLans”, o los planes de recuperación con sus tiempos de recuperación objetivos (RTO) detallando el como disponemos la organización, personas, equipos, y comunicaciones para remontar gradualmente los sistemas y en definitiva la actividad critica o esencial de la empresa.

Todo ello se visualizará bajo un prisma de integración de sistema apoyado en los estándares internacionales ISO- 27001--Seguridad de la información, e Iso-22301 --Continuidad de negocio, que en definitiva nos dan un marco y garantías de éxito.

En la segunda parte de la jornada visualizaremos y complementaremos con aspectos de Integridad y Confiabilidad de los datos, a la vez que veremos el apoyo que disponen las empresas para con los organismos oficiales tanto en materia preventiva y de guías, como especialmente en materia correctiva y/o situaciones de crisis.

En definitiva, aprenderemos a conocer pautas y consejos para implementar sistema de continuidad de las operaciones y de negocio, en esta ocasión bajo la amenaza ciber, y con la premisa de alcanzar Ciberesiliencia para nuestra entidady/O unidad empresarial .

Ponentes: **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,**

Lugar y Horarios: 10h-14h en vía Laietana 39 Planta 5 Col·legi Enginyers Industrials Superiors de Catalunya.Barcelona-

Inscripciones