Programa

"En la intersección entre la innovación tecnológica y el sector agroalimentario, encontramos no solo eficiencia y productividad, sino también la capacidad de cultivar una resiliencia cibernética que protege nuestros negocios. Transforma los desafíos en oportunidades y conviértete en un Ciberresiliente"

Organiza	Consejo Andaluz de Cámaras de Comercio, Industria y Navegación de Andalucía
Asociado a:	Andalucía Agrotech y EDIH (European Digital Innovation Hubs Network)
Confinanciado por:	Unión Europea y la Consejería de Agricultura, Pesca, Agua y Desarrollo de la Junta de Andalucía

Título	Foro Ciberresilientes Agrotech
Fecha y lugar	25 de junio de 2024. Salón de actos de la Cámara de Comercio de Almería
Horario	De 10.00h a 14.00h
Colabora	Cámara de Comercio de Almería

Introducción

En un **mercado global altamente competitivo, la digitalización y la automatización son esenciales para la continuidad del negocio en el sector agroalimentario**. Sin embargo, estas innovaciones también traen consigo **nuevas vulnerabilidades cibernéticas que deben abordarse.** Este foro busca sensibilizar a los empresarios sobre estos riesgos y promover una **cultura de ciber-resiliencia.**

Al implementar nuevas tecnologías en nuestras operaciones, aumentamos lo que podríamos llamar nuestro **"área de vulnerabilidad".** Esto implica la introducción de nuevos elementos, como **sensores, sistemas, sondas, aplicaciones y conectores, que debido a su naturaleza o novedad pueden contener vulnerabilidades desconocidas.** Estas vulnerabilidades podrían ser **aprovechadas por ciberdelincuentes si no son identificadas y controladas** de manera efectiva.

Numerosas empresas dentro de la cadena alimentaria, incluyendo **granjas, plantas de procesamiento de alimentos y compañías de distribución,** están en proceso de digitalización, abordando proyectos respaldados por tecnologías digitales y sistemas. Estos proyectos incluyen la **implementación de prácticas de agricultura o ganadería de precisión, adopción del cuaderno digital de campo, automatización de líneas de producción, robotización de instalaciones, digitalización de almacenes y gestión telemática de clientes y proveedores.** Este momento marca una mayor exposición de las empresas a ciertos tipos de ataques que explotan las vulnerabilidades de las nuevas plataformas que aún no han sido debidamente aseguradas. **Muchas compañías aún no han actualizado sus políticas de seguridad y operación para hacer frente a los ciberataques, debido al desconocimiento por parte de los empleados sobre los nuevos riesgos asociados con los sistemas y herramientas implementadas.**

ÁMBITO AGROALIMENTARIO

Dentro del ámbito agroalimentario, la adopción de tecnología reciente expande las potenciales vulnerabilidades y opciones de ataque a las estructuras empresariales. A continuación, se detallan **algunos ejemplos de riesgos potenciales vinculados a estas nuevas tecnologías. Se recomienda llevar a cabo una evaluación de riesgo cibernético e implementar medidas adicionales de protección junto a las ya existentes en la empresa.**

Caso de Uso	Tecnologías Asociadas	Posibles Vectores de Ataque
Agricultura y Ganadería de Precisión	Inteligencia Artificial, IoT, GIS, Robótica, Espectrometría Multicanal, IP CAMs, Drones, Satélite, Termografía, Medición RFID	Ataques a equipos que almacenan o generan datos, captación de envío de datos no seguro (man-in-the-middle), Denegación de Servicio (DoS) con inhibidores de frecuencia
Cuaderno Digital de Campo	Dispositivos personales móviles (tablets/smartphones), WEB Apps	Configuración insuficiente de seguridad y conectividad, usurpación de identidad, vulnerabilidades en aplicaciones
Robotización en Líneas de Producción	Robots, SCADA, PLCs, HMIs, Plataformas MES	Vulnerabilidades en sistemas operativos y PLCs, configuraciones por defecto de controladores, sensores sin seguridad, políticas de acceso a consolas de operación HMI
Almacenes Automatizados	Robots móviles, Robots colaborativos, Plataformas SGA, Plataformas IA, CRM, ERP	Vulnerabilidades en PLCs y HMIs, conexión insegura entre tecnologías de la información (IT) y operacionales (OT), falta de segmentación de redes, políticas de acceso a Internet insuficientes

Monitorización y Telegestión	RIA, Gemelos Digitales, Inteligencia Artificial, Sensorización IIoT	Ataques de Denegación de Servicio Distribuido (DDoS), vulnerabilidades en estaciones de trabajo y servidores, configuración insuficiente de seguridad y conectividad, falta de aislamiento de redes OT

La ciber-seguridad se ha convertido en uno de los mayores retos, alineado con los incuestionables e incontables beneficios que la digitalización y el comercio electrónico supone para las organizaciones del presente.

La tecnología facilita modelos de relación y negocio, antes impensables, al alcance de cualquier organización, independiente a su tamaño, localización o propósito, es imposible hoy en día que una organización exista sin que los procesos de negocio, su propuesta de valor y su comunicación estén apoyadas por la tecnología.

Esta realidad de la tecnología como facilitador y medio natural para el desarrollo de negocios comprende retos tanto en la transformación de las organizaciones por su manera de relacionarse con el mundo como a nivel de continuidad de negocio y contingencia en base a una pérdida de capacidades técnicas o de disponibilidad.

El dato, que es el estrato base y fundamento sobre el que se realizan todas las operaciones y negocios, el combustible que permite la realización de operaciones, tan sencillas como complejas y que lo convierten en información de valor para la toma de decisiones se ha configurado como uno de los principales activos para las organizaciones.

Los dispositivos conectados IOT y la tecnificación de los entornos de producción en el sector agroalimentario. **Dispositivos que ofrecen información vital, pero que suponen una mejora sustancial en la mecanización, sensórica e inteligencia de la producción, sin embargo, no están exentos de riesgos por su naturaleza conectada y la transmisión de datos, de carácter estadístico pero que pueden suponer un reto en la gestión de la continuidad de negocio.**

Objetivo del Foro

Incrementar e inculcar una cultura de ciber-resiliencia en la transformación digital, en la continuidad de negocio y el cumplimiento, así como la responsabilidad en el tratamiento de los datos personales a empresarios, como tú, del sector agroalimentario de Andalucía Oriental.

Ponentes

Julio de la Torre Hernández

Presentador - Dinamizador

Jesús Fernández Acevedo

Abogado y DPD - Especialista en Protección de datos

Isaac Carreras Verdugo

CEO en Solutia Cibersecurity - Especialista en ciberseguridad

Soraya García

Técnico Agricultura de precisión y teledetección en BrioAgro Especialista Agrotech

Fecha y Lugar

Fecha: 25 de junio

Horario: de 10.00h a 14.00h

Lugar: Salón de actos de la Cámara de Comercio de Almería

Agenda

10.00 a 10.15	Inaugura la jornada Jerónimo Parra Castaño – Presidente de la Cámara de Comercio de Almería y Antonio Mena Rubio - Delegado territorial de Agricultura, Pesca, Agua y Desarrollo Rural.
10.15 a 10.20	Introducción por parte de **Julio de la Torre** sobre **la estrategia de ciberresiliencia**, su impacto positivo y su aplicabilidad en el sector Agro.
10.20 a 11.00	Mesa redonda: **Prospectiva de la ciberseguridad.**
11.00 a 12.00	**Taller de ciberseguridad y normativas:** **Isaac Carreras Verdugo** – CEO en Solutia Cibersecurity y **Soraya García** – Brioagro
12.00 a 12.20	**Coffee Break**
12.20 a 13.15	**Taller práctico - Simulación de ciberataque. Caso Zero Day**
13.15 a 13.30	**Conclusiones**
13.30 a 13.40	Clausura del foro Ciberresilientes Agrotech: Mercedes León Lozano – Directora Gerente del Consejo Andaluz de Cámaras de Comercio, Industria, Servicios y Navegación.
13.40 a 14.00	**Networking**

Recursos para los asistentes

Tras el evento habrás obtenido la formación para implementar una **estrategia de ciberresiliencia** que asegure y proteja tu negocio. Además de otros recursos exclusivos para los asistentes como:

- **Manual de ciber resiliencia**, todo lo aprendido en un manual en formato digital que podrás consultar tantas veces como necesites.
- **Acceso a un informe de huella digital personal** para conocer posibles datos personales expuestos y que, directa o indirectamente, pueden repercutir en la seguridad de tu negocio.
- **Versión freemium del producto** privacybot, una herramienta que permite a tus clientes realizar la solicitud de sus derechos de protección de datos de una forma sencilla desde tu página web y a ti como empresario cumplir con las exigencias del Reglamento General de Protección de Datos (RGPD)

¡Reserva tu plaza!