Cumplimiento Normativo en Ciberseguridad para SectorAgroalimentario

Auditoría de Seguridad
Cumplimientode la Directiva **NIS2** y normativas **de Ciberseguridad**

Análisis de vulnerabilidades de su sistema y equpos
Procedimientosde actuación ante incidencias
Políticas de Seguridad para su plantiilla
Plan de Continuidad de Negocio

Especial Industria Agroalimentaria

No espere a que su empresa sea la próxima víctima de un ciberataque

LEX SUITE CONSULTING

CUMPLIMIENTO NORMATIVO AGROALIMENTARIO

609 37 36 92

Enrique López Navarrete

www.lexsuite.es

Tanto la **Directiva Europea de Ciberseguiridad NIS2**, como la próxima **Ley de Ciberseguridad y Gobernanza** española, de la cual **ya se ha aprobado el ante proyecto de Ley el pasado 20 de Enero** 2025 afectan de lleno a la actividad de todas las empresas y **cooperativas agroalimentarias con más de 50 trabajadores.**

La cadena agroalimentaria vive un momento de transformación acelerada: explotaciones agrícolas conectadas, sensores IoT en riego y clima, sistemas de trazabilidad en tiempo real, robots de clasificación, plataformas de logística y distribución que operan 24/7, integración con ERPs, facturación electrónica, control remoto de cámaras frigoríficas, etc. Todo eso ha convertido al sector en digital… y por tanto es vulnerable.

Hoy, un ciberataque ya no es solo "un problema informático". Es un riesgo directo para la continuidad del negocio: puede paralizar una central hortofrutícola en plena campaña, bloquear certificados de calidad y exportación, alterar datos de trazabilidad alimentaria o inutilizar sistemas de frío y atmósfera controlada que garantizan la conservación del producto.

En el sector agroalimentario, unas horas de parada pueden significar toneladas de género perdido, incumplimiento de contratos de suministro y daños reputacionales difíciles de recuperar.

Además, el sector ya no opera aislado. Forma parte de infraestructuras críticas: alimentación, logística, abastecimiento a gran distribución y, en muchos casos, exportación internacional. Eso lo convierte en objetivo de ciberdelincuencia organizada y de ataques que buscan provocar impacto económico, presión comercial o simplemente chantaje mediante ransomware.

En este contexto aparece **NIS2**, la nueva directiva europea de ciberseguridad. **NIS2** no se limita a "tener antivirus", sino que exige a las organizaciones implantar un sistema de seguridad robusto y demostrable: gestión de riesgos, control de accesos, continuidad de negocio, respuesta ante incidentes, protección de la cadena de suministro y obligaciones claras de reporte.

Dicho de otro modo: deja de ser aceptable improvisar cuando pasa algo; hay que estar preparado antes.

Para una empresa agroalimentaria, adaptarse a NIS2 no es solo cumplir con Europa. Es proteger la campaña, asegurar el suministro a clientes clave, garantizar la trazabilidad y mantener la confianza del mercado. Es pasar de "confiamos en que no nos pase" a "**hemos diseñado el negocio para seguir funcionando incluso si nos pasa**".

La seguridad ya no es un coste tecnológico adicional. Es parte de la calidad del producto, igual que la seguridad alimentaria o la certificación sanitaria. Y, a partir de ahora, será un criterio para trabajar con grandes clientes, cadenas de distribución y exportadores. ***Quien pueda demostrar resiliencia digital tendrá ventaja competitiva.*** Quien no, se expone a interrupciones, sanciones y pérdida de mercado.

Nuestro trabajo consiste precisamente en eso: ayudarle a estar preparado. No desde el lenguaje técnico, sino desde el negocio: proteger procesos críticos, personas, datos y operación diaria para que su empresa siga produciendo, cumpla con NIS2 y mantenga su posición en la cadena alimentaria, pase lo que pase.

LEX SUITE CONSULTING

CUMPLIMIENTO NORMATIVO AGROALIMENTARIO

¿Cómo implantar todo lo necesario?

DIAGNÓSTICO INICIAL

1. Realiza un **análisis de riesgos** para identificar los activos críticos y sus vulnerabilidades.

2. Elabora un **inventario de activos**, incluyendo hardware, software, datos y redes.

PLAN DE ACCIÓN

1. Define un **plan de seguridad** que cubra los controles técnicos, organizativos y operativos.

2. Asigna responsabilidades específicas dentro de tu equipo.

IMPLEMENTACIÓN

1. Contrata servicios de consultoría si no cuentas con personal especializado.

2. Prioriza los controles más críticos, como el cifrado, backups y gestión de accesos.

FORMACIÓN

1. Capacita a los empleados en ciberseguridad: reconocimiento de phishing, contraseñas seguras, etc.

2. Designa un **responsable de seguridad de la información (RSI)** para coordinar las acciones.

PRUEBAS Y AUDITORÍAS

1. Realiza simulaciones de ataques (pruebas de penetración y análisis de vulnerabilidades).

2. Evalúa la efectividad de los controles y ajusta según los resultados.

Imagina que entramos en tu empresa no solo como auditores, sino como bomberos preventivos y arquitectos a la vez. Nuestro trabajo no es poner parches: es hacer que, aunque alguien intente tirarte el sistema abajo, tu empresa siga funcionando.

Te explico el proceso de principio a fin, tal y como lo aplicamos.

01 Escaneo de vulnerabilidades del sistema y equipos

02 Creación del Plan Director de Seguridad

03 Diseño del Plan de Continuidad de Negocio

04 Protocolos y Procedimeintos ante incidentes

05 Implantación de medidas de seguridad y formación plantilla

LEX SUITE CONSULTING

CUMPLIMIENTO NORMATIVO AGROALIMENTARIO

1. Escaneamos todo tu entorno digital

El primer paso es encender las luces. Hacemos un escaneo completo de vulnerabilidades sobre toda tu infraestructura: servidores, equipos de oficina, ordenadores de planta, redes internas, accesos remotos, dispositivos industriales conectados, tablets de campo, routers, firewalls… todo.

Este análisis nos dice:

- qué puntos de entrada tiene un atacante,
- qué equipos están desactualizados o mal configurados,
- qué servicios están expuestos sin necesidad,
- qué credenciales son débiles o reutilizadas,
- y qué sistemas críticos podrían caer primero.

Es el equivalente digital a revisar todas las puertas, ventanas y llaves de una nave antes de dejarla sola por la noche.

Aquí no trabajamos con suposiciones. Trabajamos con evidencia técnica.

2. Creamos un Plan de Ciberseguridad a medida

Con toda la información técnica (escaneo + pentesting) y toda la información operativa (procesos críticos), diseñamos tu plan de ciberseguridad.

Nada genérico, nada sacado de internet.

Hablamos de **medidas específicas para su empresa**: refuerzo de accesos y contraseñas en los puestos que mueven datos sensibles, segmentación de redes para que un problema en oficina no llegue a producción, copias de seguridad verificadas y recuperables, protecciones específicas en equipos industriales que no pueden pararse cuando "Windows quiere reiniciar", control de quién accede desde fuera y cómo.

Este plan se ordena por prioridad, por coste y por impacto en el negocio: qué se debe hacer ya, qué se puede programar y qué se puede asumir como riesgo residual (siempre con ojos abiertos, no "a ciegas").

La mayoría de incidentes de ciberseguridad no empiezan con un hacker ruso en una cueva, empiezan con un click en un correo que parecía normal.

Por eso desarrollamos sus políticas de seguridad internas: normas de uso aceptable, gestión de contraseñas, uso de dispositivos personales, acceso remoto, descargas, manejo de USB, tratamiento de datos sensibles y respuesta ante sospechas de ataque.

Pero ojo: esto no es un PDF que se guarda en un cajón. El objetivo es que toda la plantilla sepa, de forma clara y sin lenguaje técnico:

- qué puede hacer,
- qué no puede hacer,
- y qué tiene que avisar inmediatamente.

La seguridad empieza en sistemas, sí, pero se sostiene en personas.

3. Diseñamos tu Plan de Continuidad de Negocio

Ciberseguridad sin entender el negocio es puro teatro. Por eso, mientras analizamos la parte técnica, hablamos con dirección y con las áreas clave (producción, logística, calidad, comercial, IT).

Queremos respuestas muy concretas:

¿Qué no puede parar bajo ningún concepto?

¿Cuántas horas de parada de la línea serían inasumibles en campaña?

¿Qué software es imprescindible para facturar, para trazar producto, para mantener la cadena de frío o para sacar el camión a las 6 de la mañana?

¿Quién tiene la llave operativa si hay un bloqueo digital?

Con esto definimos tus procesos críticos de negocio: esas piezas que, si caen, te hacen perder producción, clientes o reputación. A efectos prácticos: sabemos qué hay que salvar primero cuando todo tiembla.

4. Protocolos y procedimientos ante incidentes

La pregunta honesta no es "*¿y si nos atacan?*". Es "cuando pase algo, *¿seguimos operando o nos vamos a casa?*"

Aquí construimos su plan de continuidad de negocio y respuesta ante ciberincidentes.

Esto incluye:

- **Procedimientos claros**: quién hace qué desde el minuto 0 del incidente.
- **Protocolos de contención**: cómo frenamos el daño para que no se propague.
- **Rutas alternativas de operación:** ¿podemos seguir produciendo manualmente mientras se recupera el sistema?, ¿podemos expedir?, ¿podemos facturar?, ¿podemos acreditar trazabilidad ante un cliente grande aunque el sistema principal esté caído?
- **Recuperación técnica:** cuánto tardamos en levantar copias de seguridad funcionales.
- **Comunicación:** a quién se avisa, con qué mensaje y en qué orden (dirección,socios, clientes críticos, aseguradora, legal, etc.).

Este plan es clave por dos motivos:

- Reduce el impacto económico directo de un ataque.
- Demuestra diligencia frente a clientes, auditorías, aseguradoras y, en el marco NIS2, autoridades competentes.

5. Implantamos medidas de mitigación

Imagina que tu empresa es una finca con varias naves. El pentest ha sido la inspección que nos dice dónde están las puertas que no cierran bien, qué candados están viejos y qué luces no funcionan. Ahora toca arremangarnos y arreglar, empezando por lo más urgente.

Con los resultados del análisis de vulnerabilidades en la mano, bajamos al terreno las contramedidas.

Ejemplos típicos:

- endurecer (hardening) configuraciones inseguras,
- cerrar puertos innecesarios,
- activar doble factor de autenticación donde no estaba,
- aislar máquinas antiguas que no se pueden actualizar pero que no deben estar accesibles desde toda la red,
- limitar privilegios de cuentas "con todo el poder",
- monitorizar accesos anómalos.
- formación de tu plantilla

Esto es quirúrgico: aplicamos la corrección adecuada a la debilidad detectada. Ni más, ni menos. Así reducimos tu superficie de ataque de forma directa.

No se trata de llenar la empresa de prohibiciones, sino de evitar despistes caros:

- Nada de abrir adjuntos sospechosos.
- Nada de "me llevo datos en un pendrive" sin permiso.
- Si algo huele raro, se avisa (mejor una falsa alarma que lamentarnos luego).

¿Cuál es el objetivo real de todo esto?

No es solo “estar más seguros”.

El objetivo es ciberresiliencia: la capacidad de su empresa para resistir un ataque, contenerlo rápido, recuperar su actividad esencial y seguir cumpliendo con clientes, normativas y contratos.

En otras palabras:

- Menos probabilidad de incidente grave.
- Menor impacto cuando ocurra.
- Menor tiempo de parada.
- Mayor confianza del mercado en ti.

Esto convierte la ciberseguridad en un activo operativo y comercial, no en un gasto técnico.

Te ayuda a seguir produciendo, incluso en el peor día. Y eso, en tu sector, es la diferencia entre “hemos tenido un susto” y “hemos perdido la campaña”.

Beneficios tangibles

- Menor tiempo de parada en campaña y menos género perdido.
- Cumplimiento NIS2 demostrable (diligencia debida, gestión de riesgos, continuidad, cadena de suministro).
- Mejores condiciones de ciberseguro y menor prima por controles activos.
- Ventaja comercial: responder cuestionarios de seguridad de grandes clientes con evidencias y SLAs.

Ayudamos a identificar y mitigar los riesgos legales asociados a la actividad de su empresa

Nuestra misión es proteger sus intereses

Garantizando el cumplimiento de la normativa de protección de datos y ciberseguridad

Si usted está interesado en nuestra solución, por favor , no dude en **concertar cita** con el Sr. **Enrique López** para una explicación detallada, en el teléfono **609 37 36 92**

LEX SUITE CONSULTING

CUMPLIMIENTO NORMATIVO AGROALIMENTARIO