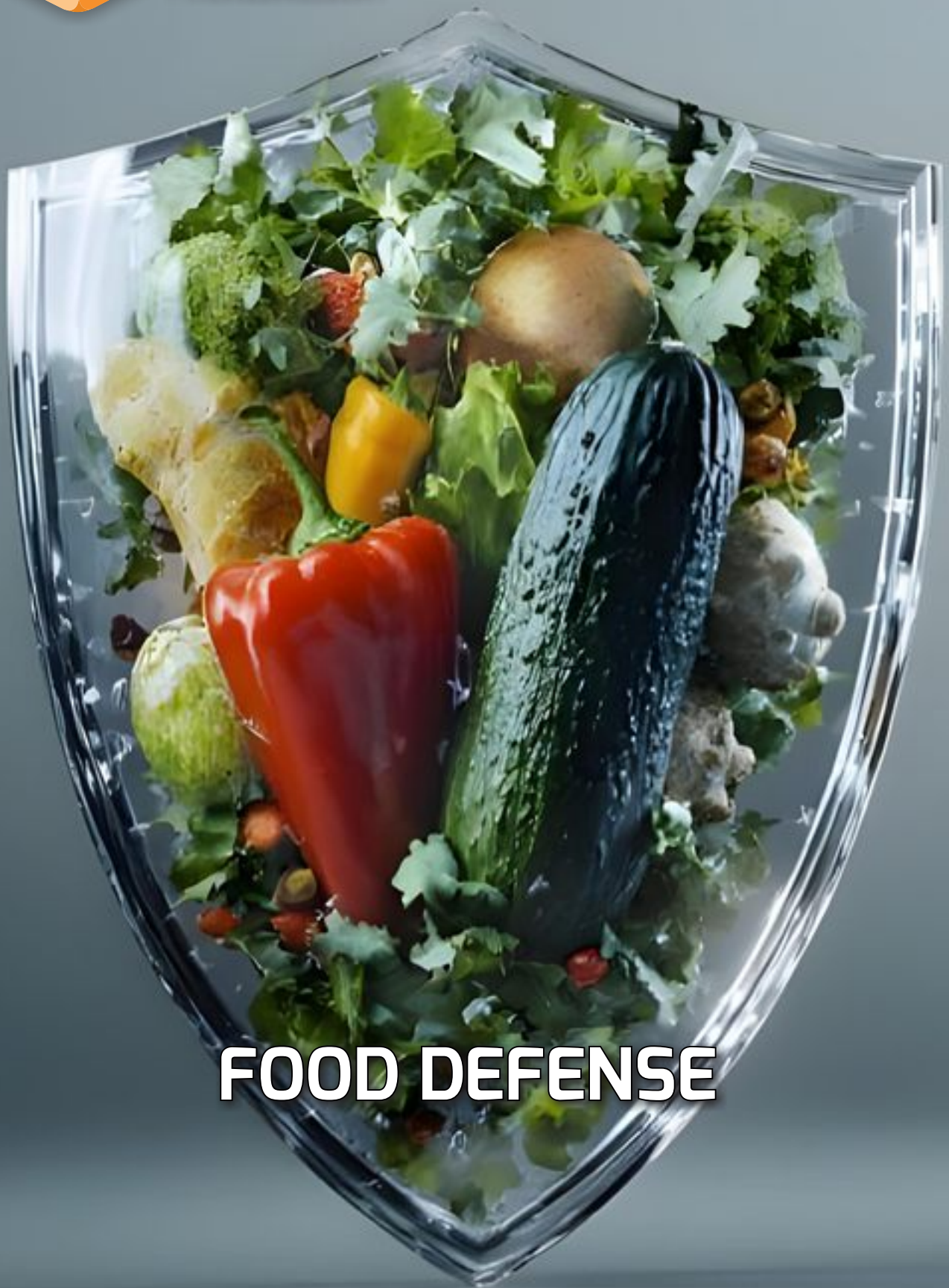
AES
FUNDACIÓN

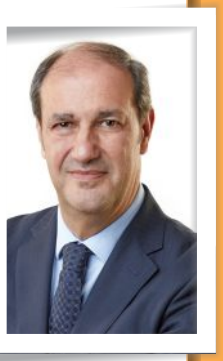


FOOD DEFENSE

Índice

Presentación

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.



Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en Publicaciones AES Fundación así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **"dinamizando la seguridad ciudadana"**

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

La elaboración de una Guía de Seguridad Electrónica de aplicación en Food Defense se enmarca en la habitual dinámica de trabajo del Área de Seguridad Electrónica de AES. Al igual que el resto de las iniciativas de las diferentes Áreas de trabajo de AES, esta surge como propuesta de uno de los miembros del Área. Dicha propuesta fue aprobada por unanimidad en una de las reuniones del Área y, de la misma forma que en otras ocasiones, se procedió a crear un grupo de trabajo que liderara la confección de dicha guía.

El espíritu del trabajo no es tanto elaborar un documento que recoja todos los detalles de aplicación, algo que habría resultado poco menos que inabordable en un breve espacio de tiempo, sino generar buenas prácticas en la industria y a la vez recopilar diferentes fuentes autorizadas que permitan al lector profundizar en la materia tanto como sea necesario.

Tras sucesivas versiones por parte del grupo de trabajo, con sus correspondientes revisiones y aportes por parte del resto de miembros del grupo, así como de otros grupos de trabajo involucrados en la materia, este trabajo ve finalmente la luz. Desde el Área de Seguridad Electrónica de AES tenemos el firme deseo de que sirva de guía y orientación para aquellos profesionales o empresas (asociados o no) que busquen la excelencia en el servicio diario que proporcionamos a nuestros clientes.

David del Rey

Coordinador del área de seguridad electrónica.

1 Introducción

Las empresas del sector alimentario y de bebidas son conscientes de que un solo incidente o accidente intencionado puede tener consecuencias desastrosas además de ocasionar un impacto negativo para la reputación empresarial.

Tras analizar diferentes incidentes de diferente relevancia acaecidos estos últimos años se evidencia que algunos de estos riesgos podrían haberse evitado si se hubiera aplicado una estrategia integral de defensa alimentaria en todo el proceso de fabricación y en toda la cadena de suministro.

Desde el Grupo de Trabajo de AES se considera prioritario el presente estudio para la correcta evolución del sector, la identificación de medidas que faciliten el incremento en la calidad de los servicios y soluciones de seguridad sobre las empresas involucradas en la producción y distribución alimentaria y de bebidas.

¿Qué es Food Defense?

El término Food Defense hace referencia a la prevención y defensa de los productos alimenticios frente a ataques intencionados de cualquier naturaleza, tanto internos como externos, invirtiendo en la mejora de la producción y la calidad

¿De dónde surge este concepto?

El concepto surge a raíz de la aprobación de la "Ley de Seguridad de la Salud Pública, Preparación y Respuesta contra el Bioterrorismo de 2002" aprobada en EE.UU. Tras el atentado a las Torres Gemelas del 11 de septiembre de 2001 en Nueva York, y el envío de una serie de cartas con esporas de ántrax que tuvo consecuencias mortales.

Estos hechos hicieron comprender que las amenazas de los terroristas podían extenderse a todos los ámbitos de la sociedad.

El objetivo del presente documento es la identificación, descripción y establecimiento del contexto, magnitud y cifras de negocio, mejores prácticas, entorno normativo, marco de trabajo y tecnología para abordar con flexibilidad y perspectiva las medidas de seguridad electrónica para la protección de negocios, personas e instalaciones relacionadas con el sector alimentario y de bebidas.

Quedan fuera del alcance de esta guía de aplicación otros aspectos relevantes, que también deben ser considerados en el diseño, implantación, gestión y mantenimiento de sistemas de seguridad, como los relacionados con la protección contra incendios y ciber-resiliencia de los sistemas de seguridad o la gestión de datos de carácter personal sujetos al Reglamento General de Protección de Datos (RGPD) como consecuencia de la implantación de sistemas de videovigilancia, biometría, etc.

Quedan fuera del alcance aspectos de cumplimiento de seguridad alimentaria, en lo relativo a la inocuidad, así como la definición de las políticas y procedimientos de seguridad operativa, formación y simulacros, así como la interpretación de lo establecido en las diferentes normas sectoriales (IFS, BRC, etc.) que deberán ser analizadas en su debido contexto con los responsables de calidad de cada empresa.

3.1. Principales cifras del sector alimentación y bebidas 2024-25

En España, la industria de alimentación y bebidas es la primera rama manufacturera del sector industrial, según los últimos datos de Estadística Estructural de Empresas del INE, con 178.923,3 M€ de cifra de negocios lo que representa el 27% del sector manufacturero, el 23,3% de las personas ocupadas y el 20,4% del valor añadido. Representa el 2,3% del PIB de España (en VAB) y que asciende a 25.741 M€(+4,9%).

El número de ocupados en la industria de alimentación, bebidas y tabaco asciende a **561.700 personas**, equivalente al 21,4% de la industria manufacturera y al 2,6% del total de la economía.

El número de empresas de la industria de alimentación y bebidas asciende a 27.896, según los últimos datos del Directorio Central de Empresas del INE, lo que representa el 17,9% de la industria manufacturera y el 15,9% de total industria. El 96,1% de ellas son empresas con menos de 50 empleados y el 77,7% cuentan con menos de 10 empleados.

Los subsectores más relevantes en cuanto a cifra de negocios son: Industria cárnica 41.337 M€(23,1%), Fabricación de bebidas 24.267 M€(13,6%), Productos de alimentación animal 19.988 M€(11,2%), Aceites y grasas 16.194 M€(9,1%), Productos lácteos con 15.534 (8,7%) y Preparación de frutas y hortalizas 14.748 M€(8,2%).

CIFRA DE NEGOCIOS, INVERSIÓN EN ACTIVOS Y VALOR AÑADIDO POR SUBSECTORES

SUBSECTORES	Cifra de negocios		Inversión en activos materiales		Valor añadido a coste de los factores	
	Millones euros	% s/ IA	Millones euros	% s/ IA	Millones euros	% s/ IA
Industria cárnica	41.337	23,1	1.320	21,1	6.586	21,1
Industria del pescado	7.968	4,5	254	4,1	1.233	4,0
Prep. y conservación frutas y hortalizas	14.748	8,2	537	8,6	2.675	8,6
Aceites y grasas	16.194	9,1	297	4,7	1.308	4,2
Productos lácteos	15.534	8,7	509	8,1	2.240	7,2
Molinería y almidones	5.613	3,1	129	2,1	647	2,1
Panadería y pastas alimenticias	12.757	7,1	479	7,7	4.024	12,9
Fabricación otros productos alimenticios	20.517	11,5	990	15,8	4.520	14,5
Productos de alimentación animal	19.988	11,2	449	7,2	1.946	6,2
Fabricación de bebidas	24.267	13,6	1.300	20,8	5.993	19,2
Total Industria Alimentaria	**178.923**	**100**	**6.264**	**100**	**31.172**	**100**

Fuente: Datos de la Estadística Estructural de Empresas Sector Industrial 2023 del INE.

En relación con el número de ocupados, los principales subsectores fueron Industria cárnica con un 24,6%, seguido por Panadería y pastas alimenticias (20,6%), Otros productos alimenticios (13,7%) y Fabricación de bebidas (12,7%).

PRINCIPALES INDICADORES DE LA INDUSTRIA ALIMENTARIA POR COMUNIDADES AUTÓNOMAS
(31 de Diciembre de 2023)

Comunidad Autónoma	Personal ocupado		Cifra de negocios		Inversión en activos materiales	
	Nº	%	Millones euros	%	Millones euros	%
Andalucía	62.307	13,0	23.074	13,3	710	11,8
Aragón	19.796	4,1	9.289	5,3	251	4,2
Principado de Asturias	7.553	1,6	2.623	1,5	79	1,3
Illes Balears	5.486	1,1	809	0,5	36	0,6
Canarias	10.855	2,3	1.932	1,1	80	1,3
Cantabria	6.284	1,3	1.883	1,1	42	0,7
Castilla y León	44.511	9,3	16.280	9,4	557	9,2
Castilla-La Mancha	30.935	6,4	12.197	7,0	437	7,2
Cataluña	98.748	20,5	40.333	23,2	1.217	20,1
Comunitat Valenciana	48.895	10,2	15.003	8,6	577	9,6
Extremadura	11.781	2,4	4.229	2,4	190	3,1
Galicia	36.322	7,6	13.380	7,7	601	9,9
Comunidad de Madrid	29.112	6,1	9.502	5,5	304	5,0
Región de Murcia	27.682	5,8	8.841	5,1	316	5,2
Comunidad Foral Navarra	18.406	3,8	6.394	3,7	257	4,2
País Vasco	13.815	2,9	5.313	3,1	251	4,1
La Rioja	8.178	1,7	2.671	1,5	140	2,3
Ceuta	129	0,0	16	0,0	0	0,0
Melilla	105	0,0	5	0,0	1	0,0
Total Industria Alimentaria	**499.094**	**100**	**178.923**	**100**	**6.264**	**100**

Fuente: *Datos de la Estadística Estructural de Empresas Sector industrial 2023 del INE.*

Fuente: INFORME ANUAL DE LA INDUSTRIA ALIMENTARIA ESPAÑOLA PERIODO 2024–2025
https://www.mapa.gob.es/es/alimentacion/temas/industria-agroalimentaria/20250428informeanualindustria2024-20251t2025_tcm30-212221.pdf

En lo relativo al comercio exterior alimentario, según el informe económico 2024[1], publicado por la Federación Española de Industrias de la Alimentación y Bebidas (FIAB), se observa que el valor de las exportaciones ascendió a 51.092 millones de euros con un superhábit comercial positivo de 16.090 millones de euros (16,9%).

[1] https://fiab.es/producto/informe-economico-iab-2024/

Los productos más significativos[2] son los correspondientes a **Aceite de oliva** con 6.580 M€, seguido por **Carne de porcino** 6.099 M€, **Vino total** 2.978 M€, **Carne de bovino** 1.389 M€, Preparaciones de alimentación animal 1.333 M€ y Preparaciones alimenticias diversas 1.329 M€ y Resto de aceites No de oliva 1.296 M€.

España se mantiene como uno de los principales exportadores de la industria de alimentación y bebidas a nivel mundial y en quinta posición entre los principales exportadores de la Unión Europea, solo por detrás de Países Bajos, Alemania, Francia e Italia, según datos de FoodDrinkEurope.

En cuanto al ranking de los principales **países de destino** de las exportaciones de la industria de alimentación y bebidas española en 2023, la **Unión Europea** continuó siendo el principal socio comercial para las exportaciones del sector, con un peso del 60,6**%** del total.

[2] Informe anual de Comercio exterior 2023 MAPA. Datos provisionales

Principales destinos exportadores				
Millones de Euros	2024	2023	Tasa de Cto	Peso 2024
FRANCIA	7.457,1	7.203,9	3,5	14,6%
ITALIA	6.290,4	5.522,5	13,9	12,3%
PORTUGAL	5.773,4	5.571,1	3,6	11,3%
EE.UU	3.365,9	2.745,6	22,6	6,6%
ALEMANIA	2.896,5	2.989,7	-3,1	5,7%
REINO UNIDO	2.812,3	2.647,7	6,2	5,5%
CHINA	1.788,2	1.836,1	-2,6	3,5%
PAISES BAJOS	1.598,8	1.514,9	5,5	3,1%
JAPÓN	1.305,3	1.137,5	14,8	2,6%
POLONIA	1.122,0	1.105,7	1,5	2,2%
BÉLGICA	1.083,1	1.054,0	2,8	2,1%
COREA DEL SUR	743,0	729,8	1,8	1,5%
MARRUECOS	734,1	778,0	-5,6	1,4%
MÉXICO	682,5	542,2	25,9	1,3%

Fuente: Data Comex. Ministerio de Economía Comercio y Empresa

En los cuatro primeros puestos se destacan **Francia** (7.457 M€), **Italia** (6.290M€), **Portugal** (5.773 M€) y **Alemania** (2.896 M€), acumulando crecimientos con respecto al año anterior que, en el caso de Alemania llegaron hasta el 16%.

En cuarto lugar y primer socio extracomunitario se encuentra **Estados Unidos** (3.365 M€), **Reino Unido** (2.812 M€), le sigue **China**, ya como el primer país asiático del ranking, con un valor de 1.788 M€ y un retroceso del -2,6% que refleja la bajada de sus importaciones de porcino tras la superación en el país de la situación de la fiebre porcina, así como el aumento de medidas proteccionistas con trabas para la importación de alimentos y bebidas. Completan el ranking de los primeros destinos **Países Bajos** (1.598 M€), **Japón** (1.305M€) y **Polonia** (1.122 M€).

3.2. Normativa y Regulación

Aunque muchas normativas del sector alimentario en España no mencionan explícitamente las medidas de seguridad electrónica, los **Planes de Seguridad del Operador** (bajo la Ley 8/2011), los requisitos de **higiene y trazabilidad** (Real Decreto 1021/2022) y la **Ley de Seguridad Privada** (Ley 5/2014, de 4 de abril) establecen un marco donde estas soluciones suelen ser necesarias.

De forma complementaria a las guías de buenas prácticas publicadas por las diferentes agencias y autoridades, de cara al diseño, implantación y soporte de soluciones de seguridad electrónica en operadores del sector alimentario y de bebidas, desde AES se recomienda la consulta a la "Guía de aplicación grado 3 y 4" disponible en la siguiente dirección https://www.aesseguridad.es/documentacion/AES_Guia_Interpretacion_WEB.pdf

3.2.1. Sectorial

Reglamento (CE) 852/2004 sobre higiene de los productos alimenticios. Aplicable a todas las empresas alimentarias en España. Exige la implementación de medidas para prevenir la contaminación de alimentos, lo que podría incluir sistemas de seguridad electrónica (cámaras de vigilancia en zonas críticas o control de accesos en áreas restringidas).

Real Decreto 1021/2022, de 13 de diciembre, por el que se regulan determinados requisitos en materia de higiene de la producción y comercialización de los productos alimenticios en establecimientos de comercio al por menor.

Real Decreto 127/2022, de 15 de febrero, por el que se establecen requisitos de higiene para la producción primaria y operaciones conexas. Incluye requisitos de protección en entornos de producción primaria (por ejemplo, granjas, fábricas de pienso), que pueden complementarse con medidas electrónicas de seguridad.

Real Decreto 695/2022, de 23 de agosto, por el que se establecen medidas para el control del bienestar de los animales en los mataderos mediante la instalación de sistemas de videovigilancia.

Ley 26/2007, de 23 de octubre, de Responsabilidad Medioambiental. Exige medidas de prevención en empresas con riesgos de impacto ambiental, como fábricas de alimentos. Los sistemas de detección temprana de fugas, incendios o intrusiones podrían integrarse como parte del plan de prevención.

3.2.2. Infraestructuras y Entidades Críticas y Esenciales

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Aplicable a empresas del sector alimentario que hayan sido declaradas infraestructuras críticas. Requiere la elaboración de Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE), que incluyen medidas de seguridad física y electrónica para mitigar riesgos.

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (trasposición de la Directiva NIS). Aplica a operadores esenciales, incluidos los del sector alimentario crítico. Obliga a garantizar la seguridad de sistemas de información, que puede incluir protección de sistemas SCADA o IoT en fábricas.

Directiva NIS 2 (Directiva (UE) 2022/2555 del parlamento europeo y del consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (aplicable en 2024). Refuerza la ciberseguridad de operadores esenciales y sistemas tecnológicos conectados a entornos críticos.

Directiva CER, Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas.

ISO/IEC 27001 es ahora el estándar internacional más reconocido para sistemas de gestión de seguridad de la información. En él se detallan los requisitos para establecer, implementar, mantener, supervisar y mejorar un sistema de este tipo y está diseñado para ser compatible y armonizado con otras normas de sistemas de gestión reconocidas.

3.2.3. Marcos y guías de buenas prácticas voluntarias

FSMA (Food Safety Modernization Act): Las empresas que exportan alimentos a Estados Unidos deben verificar su adaptación a los mandatos promulgados por la Ley de Modernización de Inocuidad de los Alimentos, el programa de Verificación de Proveedores Extranjeros (Foreign Supplier Verification Programs - FSVP) y demás regulaciones establecidas por la FDA (Food and Drug Administration), USDA (United States Department of Agriculture) u otras agencias.

Y más concretamente, en el contexto FSMA, la norma "Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration" establece un marco de trabajo para cubrir el riesgo de delincuencia ideológica, e intenta mitigar el "impacto a gran escala en la salud pública".

GFSI (Global Food Safety Initiative): De igual modo las empresas acogidas a la Iniciativa Mundial de Seguridad Alimentaria deben estar certificadas en alguno de los estándares voluntarios de certificación de sistemas de gestión de inocuidad alimentaria, tales como el Food Safety System Certification (FSSC 22000), el British Retail Consortium (BRC), el International Food Standard (IFS), etc...

Norma ISO 22000: Sistemas de Gestión de la Seguridad Alimentaria. Aunque no es obligatoria, incluye directrices que pueden aplicarse a sistemas electrónicos como parte de la prevención de riesgos en seguridad alimentaria.

BSI PAS 96:2017 –Food Defence. Guía para proteger la cadena alimentaria frente a sabotajes e intromisiones, incluyendo el uso de medidas electrónicas de seguridad.

ASIS dispone de una comunidad temática de "Food Defense and Agriculture" donde los profesionales de esta industria comparten material, se reúnen y debaten. En la actualidad no existe una guía o standard específico para "Food Defense" pero en el siguiente link existen guías y estándares complementarios que pueden servir como referencia para la planificación y desarrollo de una estrategia de seguridad en este ámbito.

https://www.asisonline.org/publications--resources/standards--guidelines/

La industria alimentaria considera la seguridad de sus productos como su preocupación principal. A lo largo de los años, la industria y los reguladores han desarrollado sistemas de gestión de seguridad alimentaria lo que significa que grandes brotes de intoxicación alimentaria son ahora bastante inusuales en muchos países.

Estos sistemas suelen utilizar como referencia la metodología de Análisis de Peligros y Puntos de Control Crítico (APPCC) del inglés (HACCP) tal como establece el artículo 5 del Reglamento (CE) nº 852/2004, donde, dispone que los operadores de empresa alimentaria deben crear, aplicar y mantener un procedimiento permanente basado en los principios del análisis de peligros y puntos de control crítico («procedimientos basados en el APPCC» o «APPCC»). Estos procedimientos deben ser suficientemente flexibles para poder aplicarse en todas las situaciones sin poner en peligro la seguridad alimentaria, para más información consultar https://www.aec.es/conocimiento/centro-del-conocimiento/appcc/

APPCC ha demostrado ser eficaz contra accidentes de contaminación, favoreciendo la inocuidad y seguridad alimentaria, sin embargo, los principios APPCC no permiten detectar o mitigar de forma eficiente amenazas de origen deliberado a un sistema o proceso, tales amenazas incluyen ataques deliberados de contaminación, sabotaje, robo y fraude.

El factor común detrás de todos estos actos deliberados son las personas. Estas personas pueden pertenecer a la plantilla de la propia empresa, pueden ser empleados de un proveedor auxiliar, o pueden ser personas ajenas sin conexión con la industria alimentaria. La cuestión clave es su motivación, pueden tener como objetivo causar daño a la salud humana, la reputación de la empresa, u obtener ganancias financieras a expensas del negocio. En cualquiera de estas situaciones existe una exposición evidente de la empresa a los riesgos de origen deliberado y se deben establecer las medidas alineadas con una cultura de prevención.

En un mundo cada vez más digitalizado, las empresas alimentarias no son la excepción en la adopción de tecnologías avanzadas para optimizar sus operaciones. Sin embargo, esta transformación también las hace vulnerables a los ciberataques, una amenaza que muchas veces se subestima.

4.1. Estrategia híbrida frente a amenazas de seguridad alimentaria

El propósito más importante de una estrategia de defensa alimentaria es ayudar a aumentar la seguridad del consumidor, pero también se debe considerar la protección de la marca y la rentabilidad de la empresa.

Evaluar, acceder, alertar y auditar (las cuatro A en inglés: Assess, Access, Alert and Audit) de la defensa alimentaria son los componentes centrales de un programa proactivo de defensa alimentaria para ayudar a las empresas y proveedores de alimentos a implementar los controles preventivos necesarios.

Una sólida estrategia de defensa alimentaria, implementada en toda la estructura organizativa de la empresa, las instalaciones y la cadena de suministro, puede ayudar a proteger mejor a los empleados, reducir los riesgos operativos y proteger el valor para los accionistas. “Las crisis de reputación son uno de los principales riesgos a los que se enfrentan las empresas, hoy en día, y va más allá del riesgo legal”.

Un programa híbrido y proactivo de defensa alimentaria puede prevenir actos vandálicos, sabotajes, interceptación, alteración malintencionada de alimentos y ciberataques, ayudando a las empresas a evitar, o ser alertadas sobre:

- Desvíos de materia prima, ingredientes y/o productos.
- Contaminación inadvertida o intencional en la planta.
- Fallos o desviaciones en los protocolos/procesos, dentro de las plantas y en la cadena de suministro.
- Acceso incontrolado de personal no autorizado, visitantes y contratistas dentro de las instalaciones de producción o áreas de almacenamiento.
- Datos sensibles en riesgo: Las empresas alimentarias manejan una gran cantidad de datos sensibles, desde fórmulas y procedimientos hasta información de proveedores y clientes. Un ataque cibernético podría comprometer esta información, llevando a pérdidas económicas significativas y dañando la reputación de la empresa.
- Interrupción de la actividad: Un ciberataque puede paralizar completamente las operaciones de una empresa alimentaria. Por ejemplo, un ransomware que bloquea el acceso a los sistemas de producción o un ataque DDoS que hace caer la plataforma de ventas en línea. Las consecuencias pueden ser catastróficas, desde pérdidas de producción hasta una interrupción total del negocio.

Aunque puede ser difícil lograr la protección de la cadena de suministro de un extremo a otro, algunos riesgos pueden reducirse significativamente combinando ventajas metódicas, procedimentales y tecnológicas.

4.2. Plan de defensa alimentaria PDA

Toda estrategia debe incluir un plan de acción o programa de actividades que permita la implantación y seguimiento de las medidas y controles que garanticen el cumplimiento de los compromisos de negocio, normativo, regulatorio, etc. en los diferentes ámbitos de operación de las empresas del sector agroalimentario y de bebidas.

Como se indica anteriormente sobre la metodología APPCC, ampliamente aplicada en el sector alimentario, es un hecho que los sistemas de gestión de inocuidad alimentaria son incompletos y no permiten garantizar la seguridad de los alimentos y las bebidas, y de sus cadenas de suministro, frente a ataques malintencionados que generan contaminación o interrupción del producto y por ello, el Plan de Defensa Alimentaria (PDA) ha pasado a ser una parte indispensable en la correcta gestión de cualquier etapa de la producción, almacenamiento, transporte o distribución del alimento. Recordar lo indicado en el capítulo de "Normativa" donde el Sector de la Alimentación es un Sector Estratégico dentro del Programa Europeo y Plan Nacional de Protección de Infraestructuras Críticas (PEPIC / PIC).

El objetivo fundamental de un PDA es, precisamente, reducir los riesgos de adulteraciones, contaminaciones deliberadas, violaciones del empaquetado, así como cualquier otra acción u omisión maliciosa, criminal o terrorista en la cadena de producción y suministro de alimentos, tomado en cuenta las posibles amenazas internas y externas a la organización.

En el siguiente enlace https://www.fda.gov/food/food-defense-tools/food-defense-plan-builder está disponible la herramienta **"Food Defense Plan Builder"**, desarrollada por la Administración de Alimentos y Medicamentos de EE. UU. (FDA), de ayuda a los propietarios y operadores de instalaciones de alimentos a crear planes de defensa alimentaria personalizados. Estos planes ayudan a las instalaciones a cumplir con los requisitos reglamentarios y proteger contra la adulteración intencional.

Para el proceso de transporte y almacenamiento de mercancías en tránsito se recomienda consultar el marco de trabajo y certificaciones TAPA https://tapaemea.org/standards-trainings/ que cubren los riesgos específicos para garantizar la resiliencia de la cadena de suministro: FSR –Facility Security Requirements; TSR –Trucking Security Requirements, PSR –Parking Security Requirements, CSS –Cyber Security Standard.

En el presente caso se propone la aplicación de la estrategia Evaluar, acceder, alertar y auditar para la gestión de riesgos del sector alimentario y de bebidas a partir de la siguiente metodología flexible:

4.2.1. Evaluación

Partiendo del hecho de que la inocuidad de los alimentos se refiere a la contaminación accidental de productos alimenticios durante su procesamiento y almacenamiento, por agentes biológicos, químicos y físicos y no a la contaminación deliberada; el plan de Análisis de Peligros y Puntos Críticos de Control (APPCC) no debería usarse como sustituto del Plan de Defensa Alimentaria (PDA), porque no todos los puntos críticos de control serán iguales. No obstante, crear un PDA no requiere elaborar otro documento al estilo del APPCC. Seguramente, parte de la información utilizada para crear un PDA ya existe de manera implícita o explícita en el APPCC implantado.

Actualmente, la mayoría de las evaluaciones de riesgos están enfocadas a la seguridad alimentaria, sin embargo dadas las amenazas y vulnerabilidades adicionales de la defensa alimentaria, la complementariedad de conocimientos en metodologías y tecnologías de seguridad da lugar a una evaluación de riesgos más efectiva orientada a la preparación de un PDA identificando los siguientes principios para su diseño:

- **Principio 1:** **Entender claramente qué debe protegerse.**

  El conocimiento de las amenazas y de lo que protegerse contribuye a asegurar que las medidas de control se apliquen donde sean más eficaces.

- **Principio 2:** **Aplicar el nivel de seguridad más alto a los componentes más críticos.**

  Los medios y medidas de seguridad adoptados tienen que ser adecuados con los puntos críticos de las instalaciones y con la gravedad, probabilidad y alcance del posible perjuicio.

- **Principio 3:** **Utilizar un enfoque estratificado.**

  Salvaguardar las instalaciones, el personal y el proceso productivo de una amplia gama de amenazas requiere el uso de múltiples enfoques para reducir al mínimo las vulnerabilidades identificadas, teniendo como objetivo último prevenir, evitar o mitigar daños, pánico, desconfianza... en las personas; por ello es recomendable establecer anillos concéntricos de protección:

  - siendo el control de acceso a las instalaciones el anillo exterior,
  - el control de entradas autorizadas en planta el siguiente anillo, y
  - el anillo interior representaría los procesos y procedimientos diseñados para reducir los riesgos operativos.

- **Principio 4:** **Reducir el riesgo a un nivel aceptable.**

  No es posible eliminar todos los riesgos de la defensa alimentaria ni tampoco es económico hacerlo, por lo que deben considerarse los factores coste-beneficio para cada medida de protección propuesta. Siempre se debe mantener el equilibrio entre las medidas propuestas y su eficacia operativa, ya que por muy costosas que sean estas medidas, si no son eficientes no alcanzarán el objetivo propuesto.

- **Principio 5:** **La seguridad debe contar con un firme respaldo por parte de la dirección de la empresa.**

  La defensa alimentaria, al igual que la seguridad alimentaria, empieza por el compromiso básico de la organización con el proceso. La implicación y soporte por parte de la dirección de la empresa es crucial para el éxito de un programa PDA, teniendo este el mismo nivel de relevancia que la inocuidad de los alimentos y el control de la calidad.

Evaluación inicial

Un primer chequeo de verificación de la situación de partida y una posterior identificación de las áreas críticas que podrían ser los blancos más probables de un ataque, a partir de alguna de las metodologías de análisis de riesgos generales o específicas incluidas en la ISO-31010 o través de un método de análisis como CARVER + Shock, que ponga de manifiesto las potenciales amenazas tanto internas como externas, muestre las vulnerabilidades y proponga las posibles medidas de defensa alimentaria (PDA) incluyendo, de forma no exhaustiva, aspectos tales como:

Seguridad exterior

- Medios y medidas existentes de protección y control perimetral exterior.
- Medios y medidas existentes de protección y control de las vías de acceso a las instalaciones / edificaciones.
- Procedimientos de autorización de accesos de personas y vehículos al interior de las instalaciones.

Seguridad interior

- Medios y medidas existentes de protección y control en el interior de las instalaciones / edificaciones.
- Medios y medidas existentes de protección y control en el interior de las zonas restringidas de las instalaciones / edificaciones.
- Medios y medidas existentes de protección y control de los sistemas /servicios públicos de suministro.
- Medios y medidas de seguridad TIC.

Seguridad del almacenamiento

- Medios y medidas existentes de protección de los lugares de almacenamiento y control de movimientos de productos acabados, materiales o sustancias peligrosas.

Seguridad en el transporte y recepción

- Medios y medidas existentes de protección y control del estacionamiento, carga y descarga de los medios de transporte con productos primarios, terminados u otros materiales empleados en el procesamiento de alimentos.

Inocuidad del agua y del hielo

- Medios y medidas existentes de protección y control de vigilancia en los depósitos y líneas de suministro de agua y hielo para los procesos productivos y mantenimiento.

Seguridad en el manejo de la correspondencia y paquetería

- Medios y medidas existentes de protección y control para garantizar la seguridad en la recepción, manejo y entrega de la correspondencia y paquetería.

Seguridad del personal

- Medios y medidas existentes de protección y control para garantizar el personal cumple con los requisitos de seguridad y defensa alimentaria.

4.2.2. Accesos

Controlar el acceso a áreas e instalaciones a través de las puertas de entrada es solo una medida mínima o comienzo de lo que un control de accesos puede hacer para ayudar a proteger mejor una instalación de producción.

La adulteración deliberada de alimentos puede provenir tanto de personal externo, como interno: grupos organizados bioterroristas o activistas, competidores comerciales, visitantes, contratistas, empleados resentidos o infiltrados, etc. La prevención del acceso no autorizado a los puntos críticos de control y el seguimiento del movimiento a través de esas áreas también debe ser parte de una iniciativa integral de defensa alimentaria. Los puntos críticos de control incluyen, entre otros posibles:

- Almacenamiento de materia prima;
- Almacenes de productos terminados;
- Áreas de procesamiento;
- Embalaje y almacenamiento de etiquetas;
- Instalaciones de almacenamiento de sustancias químicas y materiales peligrosos;
- Laboratorios.
- Muelles de envío y recepción;
- Zonas de alérgenos;
- Zonas libres de alérgenos;

4.2.3. Alerta

Históricamente, las iniciativas de seguridad y protección se han centrado principalmente en las instalaciones de producción pero en los últimos años, se ha evidenciado que las amenazas de defensa alimentaria pueden provenir de cualquier parte de la cadena de suministro. De hecho, un alto porcentaje de los robos de carga se producen en camiones mientras están en tránsito.

Los delincuentes no se preocupan por proteger la seguridad de los alimentos cuando los revenden en la cadena de suministro. Por lo tanto, es más importante que nunca tomar medidas para proteger toda la cadena de suministro, tanto dentro de la planta como para las mercancías en tránsito.

4.2.4. Auditoria

Bajo el sistema actual, los controles de los procesos y calidad de la industria alimentaria suelen ser realizados por inspectores internos de primera parte y por auditorías alimentarias de segunda parte llevadas a cabo por equipos de auditores especializados en una amplia gama de conocimientos, por ej.: en biotecnología, química, ingenierías agroalimentarias, medioambiente, TIC, calidad, logística, PRL, etc. No obstante lo anterior, es lógico pensar que dicha especialización deba evolucionar con el tiempo, a medida que evoluciona la comprensión de la defensa de los alimentos a través de medios y medidas de seguridad física, electrónica y cibernética a aplicar.

Los actuales sistemas de auditorías no son ajenos a fallas derivadas de, por ej.: errores de apreciación o estimación, saber cuándo será la visita del auditor, conocimiento de los elementos que un auditor verificará, etc. A este respecto el muestreo aleatorio y la auditoría de estándares y procedimientos operativos específicos con las nuevas tecnologías CCTV pueden ayudar a mejorar el cumplimiento al verificar que se sigan los procedimientos establecidos en todo momento.

Al hilo de lo anterior, las auditorías de control y equipos de defensa alimentaria se pueden ver fortalecidos con la adopción de otros servicios de seguridad adaptados a las necesidades específicas de la operativa de cada planta de producción.

4 La seguridad en la industria alimentaria

4.3. La ciberseguridad dentro del plan de Food Defense

Según indica INCIBE en su web *"La ciberseguridad en el sector agroalimentario"*,[3] para realizar la digitalización y automatización de los procesos productivos, las empresas del sector agroalimentario tienen que implementar nuevos dispositivos, como por ejemplo sensores, sondas, routers, etc. Esta implementación trae muchas ventajas, gracias a la conectividad proporcionada por la industria 4.0, permitiendo que se tenga un control de todo lo que sucede en tiempo real.

El gran problema de la implementación de estos dispositivos es el aumento de exposición al mundo exterior, que provoca que las posibilidades de sufrir un ciberataque sean mucho más altas. A continuación, se explican diversos puntos que permitirán comprender la exposición real que tiene el sector agroalimentario a sufrir un ciberataque:

- Se trata de un sector crítico para la sociedad, lo que, sumado a la tendencia de ciberataques contra la cadena de suministro, lo convierte en un objetivo principal para los ciberdelincuentes.
- La baja madurez en ciberseguridad que presenta este sector, como por ejemplo la falta de procedimientos o políticas, provoca que sea más susceptible a los ataques.
- Su falta de adaptación a la continua evolución de la tecnología: se trata de un sector más enfocado a la productividad y menos en la ciberseguridad, como, por ejemplo, las comunicaciones entre dispositivos no securizadas, las configuraciones vulnerables de los dispositivos o contar con más servicios expuestos.
- En este sector las empresas que lo forman en su mayoría son pymes, micro pymes y autónomos, lo que puede provocar que no tengan suficiente madurez en ciberseguridad.

En la mayoría de las organizaciones, la red no está diseñada para la ciber protección y las amenazas pueden provenir de varias fuentes. El acceso a los sistemas por parte de los ingenieros requiere la actualización de los equipos. Es esencial que se mantenga libre de virus y otros programas maliciosos.

Las organizaciones también necesitan entender la importancia del elemento del comportamiento humano. Una empresa puede tener los sistemas físicos más seguros, pero a veces los hackers utilizan la vulnerabilidad del empleado, para engancharlos con ingeniería social. Y como todos sabemos, cualquier sistema o cadena es tan fuerte como su eslabón más débil. Y normalmente el eslabón más débil son los comportamientos humanos y por eso es importante tener también un sistema de gestión integral y robusto.

[3] https://www.incibe.es/incibe-cert/blog/la-ciberseguridad-en-el-sector-agroalimentario

5 Medidas de seguridad

Existe un amplio catálogo de medidas de seguridad que permiten proteger a la industria alimentaria de las amenazas descritas anteriormente, algunas basadas en tecnología tradicional del ámbito de la seguridad electrónica (videovigilancia, control de accesos, sistemas de detección de intrusión, etc.) y otras que aprovechan los factores habilitadores que suponen el procesado de señales en el "Edge", interoperabilidad de sistemas a través del "Cloud", gestión unificada y automatización en el proceso de respuesta.

Desde 2011, la FDA publica la base de datos "Food Defense Mitigation Strategies Database" que contiene una extensa lista de medidas de mitigación (físicas, técnicas, procedimentales y organizativas) que pueden ser útiles para reducir las vulnerabilidades a la contaminación intencionada que puedan existir en el entorno de la instalación. La base de datos de la FDA se puede explorar por categorías (por ejemplo, transporte, manipulación de materiales, embalaje, procesamiento, tipos de actividades clave, almacenamiento, transporte/distribución). Para más información consultar la web:

https://www.hfpappexternal.fda.gov/scripts/fooddefensemitigationstrategies/index.cfm

5.1. Sistema de control de accesos

Los sistemas de control de accesos permiten restringir el acceso no autorizado a zonas sensibles o críticas, garantizando la seguridad de los productos, materias primas y personal de la planta. No sólo protege la integridad de las instalaciones y los procesos, sino que asegura que sólo el personal autorizado tenga acceso a las zonas críticas y cuadros de mando y control, donde se manipulan, procesan o almacenan alimentos, evitando así la contaminación intencional, sabotajes u otros riesgos asociados con accesos no autorizados.

5.1.1. Principales usos y aplicaciones

El uso de un sistema de control de accesos no debe limitarse al acceso a las instalaciones, sino que debe estar alineado con las zonas de riesgo más alto, donde las consecuencias de un acceso no autorizado podrían tener un impacto directo en la seguridad alimentaria.

1) **Restricción de acceso a zonas sensibles**, como laboratorios de control de calidad, líneas de producción, almacenes de materias primas o productos elaborados, zonas de embalaje, cuadros de mando y control, etc. Sólo el personal autorizado podrá acceder a dichas instalaciones.

2) **Protección de los puntos de entrada.**

3) **Identificación y autenticación del personal**, utilizando métodos seguros como tarjetas de proximidad, códigos de acceso o sistemas biométricos.

4) **Control de visitas y proveedores**, utilizando credenciales temporales restringidas a zonas específicas.

5) **Bloqueo automático de los puntos de acceso**, en caso de detección de un sabotaje o contaminación intencionada, a fin de contener la amenaza.

6) **Registro y trazabilidad de los accesos**, de forma que se pueda saber quién accedió a una zona, cuándo lo hizo y cuánto tiempo permaneció en dicha zona, en caso de auditoría de trazabilidad de las personas que accedieron a zonas sensibles, o de análisis forense en caso de necesitar investigar un incidente o una brecha de seguridad.

5.1.2. Recomendaciones fundamentales

El sistema de control de accesos debe ser seguro, robusto y flexible, permitiendo adaptarse a las diferentes necesidades a nivel operativo que puedan surgir.

1) **Identificar las zonas críticas y los puntos de acceso**, a fin de poder ubicar los puntos de control y las distintas áreas a definir, como por ejemplo:

- Accesos perimetrales de la instalación
- Control de vehículos (incluyendo personal y vehículos de transporte)
- Zonas de oficinas
- Zonas de carga y descarga de vehículos
- Zonas de almacenamiento de materias primas
- Líneas de producción
- Zonas de embalaje y etiquetado
- Zonas de almacenamiento de productos elaborados
- Laboratorios de calidad o investigación
- Puntos de control de seguridad alimentaria donde se tomen muestras
- Zonas de manipulación de productos peligrosos o con equipamiento sensible
- Cuarto de servidores o CPD (centro de proceso de datos)
- Cuadros de mando y control
- Salas de control
- Zonas de residuos peligrosos
- Zonas refrigeradas
- Sistemas de agua
- Zonas de almacenamiento de EPIs (equipos de protección individual)
- Salidas de emergencia

2) **Utilizar un sistema jerárquico con diferentes perfiles** de acceso para distintas zonas y tipos de usuario (personal de laboratorio, personal de producción, proveedor, subcontratista, etc.).

3) **Utilizar métodos de autenticación robustos:**

- Utilizar credenciales únicas, como tarjetas de proximidad con protocolos seguros que no permitan el copiado, tokens en dispositivos móviles o sistemas biométricos que ofrezcan un nivel alto de precisión y que prevengan la suplantación de identidad (huella dactilar, iris, y/o reconocimiento facial).
- Utilizar sistemas de autenticación multifactor para acceder a zonas críticas o de mayor riesgo (p.ej. que se tenga que usar una credencial más un código).
- En caso de usar códigos, asegurarse que sean robustos, actualizarlos frecuentemente, y que el sistema permita detectar intentos recurrentes de adivinación del código.

4) **Controlar las zonas de acceso peatonal**, instalando lectores en todas las puertas de acceso a las áreas con acceso restringido, así como cerraduras electrónicas que se puedan controlar de forma remota. En los puntos de acceso exterior a las instalaciones, utilizar torniquetes o puertas de seguridad.

5) **Controlar las zonas de acceso de vehículos** (coches y/o camiones), con barreras automáticas y/o sistemas de lectura de matrículas.

6) **Monitorizar en tiempo real los accesos**, a través de una plataforma centralizada que permita saber en todo momento quién está accediendo, a dónde y por qué motivo. Dicha plataforma debe poder alertar cuando se produzca un acceso no autorizado, así como modificar de forma remota los permisos de acceso para evitar que el posible intruso pueda seguir accediendo a zonas restringidas.

7) **Integrar el sistema de control de accesos con otros sistemas de seguridad**, a través de plataforma de integración, como p.ej. los sistemas PSIM (Physical Security Information Management), que permita una gestión centralizada y una respuesta automática en caso de incidentes.

8) **Registrar de forma detallada todos los eventos de acceso**, incluyendo hora y día de entrada y salida, la identificación del usuario, y la zona(s) a las que accedió.

9) **Cumplir con las normativas y regulaciones a nivel de protección de datos**. Esto incluye la gestión segura de datos biométricos o de cualquier otra información personal que se registre.

10) **Mantener y actualizar el sistema de control de accesos** de forma regular para garantizar su correcto funcionamiento, y asegurar que las versiones de software y hardware de los elementos del sistema de control de accesos no presenten vulnerabilidades, y permitiendo la integración con nuevas tecnologías de autenticación o control que puedan surgir.

11) **Realizar auditorías periódicas del sistema de control de accesos**, para verificar que todos los permisos son adecuados y que los usuarios tengan acceso sólo a las zonas que les corresponda en cada caso en función de su rol.

5.2. Sistema de videovigilancia

Los sistemas de videovigilancia son de gran utilidad en la implantación de un plan de defensa alimentaria, ya que permiten monitorizar y grabar en tiempo real todo lo que sucede en la instalación, garantizando la seguridad de la cadena de suministro y protegiendo los alimentos de cualquier tipo de contaminación o sabotaje.

5.2.1. Principales usos y aplicaciones

Los sistemas de videovigilancia ofrecen actualmente una tecnología avanzada que ayuda a mantener un entorno de producción más seguro y alineado con las normativas de seguridad alimentaria.

1) **Visualización en tiempo real de las zonas sensibles o críticas**, como las líneas de producción, zonas de almacenamiento de materias primas o productos elaborados, etc. Hacer especial hincapié en la supervisión de los paneles de control, ya que son puntos desde donde se podrían realizar sabotajes intencionados causando un gran daño.
2) **Protección del perímetro de la instalación**, con alertas automáticas basadas en analíticas de vídeo en caso de detección de intrusión no permitida.
3) **Visualización y control de las zonas de acceso**, para tener un control visual de las mismas.
4) **Sistema de lectura de matrículas**, para la entrada y salida de vehículos.
5) **Control de calidad en las líneas de producción**, permitiendo detectar contaminaciones involuntarias debido a incumplimientos o fallos en los procesos.
6) **Ofrecer análisis de vídeo** para ayudar a mejorar la eficiencia operativa, mantener el cumplimiento y usarlo como una herramienta de capacitación de empleados.
7) **Aumentar el cumplimiento de los protocolos estándar de manipulación** de productos, higiene y desinfección, limpieza, uso de EPIs e identificaciones autorizadas, etc.
8) **Garantizar el cumplimiento de los procedimientos de bienestar animal** para evitar problemas con la capacidad, registro y trazabilidad.
9) **Análisis forense**, en caso de necesitar investigar un incidente o una brecha de seguridad.
10) **Protección de la cadena de suministro**, pudiendo monitorizarse también los productos durante el transporte.

5.2.2. Recomendaciones fundamentales

El sistema de videovigilancia debe de ser proactivo y fácil de integrar y usar, ofreciendo una protección de las zonas vulnerables a sabotajes, y de manipulaciones (intencionadas o no), además de un sistema de prevención de robo.

1) **Identificar las zonas sensibles o críticas**, asegurándose que las cámaras cubran dichas zonas, sin interferir con el funcionamiento de la planta o instalación:
   - Perímetro de la instalación
   - Zonas de entrada/salida de vehículos
   - Zonas de almacenamiento de materias primas
   - Líneas de producción
   - Zonas de embalaje y etiquetado
   - Zonas de almacenamiento de productos elaborados
   - Zonas de oficina
   - Laboratorios de calidad o investigación
   - Puntos de control de seguridad alimentaria donde se tomen muestras
   - Zonas de manipulación de productos peligrosos o con equipamiento sensible
   - Cuarto de servidores o CPD (centro de proceso de datos)
   - Zonas con materiales valiosos
   - Zonas de residuos peligrosos
2) **Utilizar cámaras de alta resolución**, para poder visualizar detalles tanto de los posibles intrusos como de cualquier acción o manipulación que pueda realizar. Recomendable utilizar al menos cámaras de 4 MP.
3) **Utilizar cámaras con visión nocturna**, mediante el uso de luz infrarroja, luz blanca, sistemas de iluminación híbridos, cámaras con sensores de baja luminosidad, o cámaras térmicas, que permitan la visualización de noche, en zonas oscuras o con baja iluminación.
4) **Utilizar cámaras PTZ** en aquellas zonas donde se necesite realizar un seguimiento más detallado, como las zonas de entrada, apoyo en puntos perimetrales o en zonas de almacenamiento críticas.
5) **Utilizar cámaras con analíticas de vídeo**, en aquellos lugares donde se requiera una detección temprana de una intrusión o presencia no autorizada en una zona, generando una alarma que permita una rápida reacción.

6) **Utilizar sistemas de grabación** dimensionados según las necesidades de los periodos de almacenamiento (recomendado 30 días para las zonas críticas), así como con sistemas de redundancia (RAID, Cloud) para evitar perder grabaciones en caso de producirse un fallo en los soportes de grabación o un sabotaje intencionado.

7) **Utilizar protocolos de transmisión de vídeo cifrados**, para evitar que sean interceptados durante su transmisión, de forma que se impida el acceso no autorizado a la visualización, o a posibles alteraciones del contenido.

8) **Controlar el acceso** a las visualizaciones y grabaciones sólo por el personal de seguridad o personal autorizado, creando perfiles de acceso según roles.

9) **Integrar el sistema de videovigilancia con otros sistemas de seguridad**, a través de plataforma de integración, como p.ej. los sistemas PSIM (Physical Security Information Management).

10) **Cumplir con las normativas y regulaciones a nivel de protección de datos**.

11) **Mantener y actualizar el sistema de videovigilancia** de forma regular, incluyendo la limpieza de las cámaras, así como la actualización de los firmwares de todos los elementos del sistema (para corregir posibles vulnerabilidades o para añadir nuevas funcionalidades o mejoras).

5.3. Sistemas de detección de intrusión

Los sistemas de detección de intrusión ayudan a prevenir accesos no autorizados a zonas sensibles o críticas, evitando así posibles actos de sabotaje o contaminación intencional. Además, proporciona protección frente a robos en las instalaciones.

5.3.1. Principales usos y aplicaciones

Los sistemas de intrusión no sólo mejoran la seguridad de las instalaciones, sino que ayudan a garantizar la integridad de los alimentos.

1) **Protección del perímetro de la instalación**, mediante el uso de diferentes sensores, como p.ej. detectores de exterior PIR (infrarrojo pasivo) o doble tecnología (PIR + microondas), barreras de haces infrarrojos, barreras de microondas, sensores de vibración en vallas, sensores de presión instalados bajo tierra o en superficie, o sensores de fibra óptica.

2) **Protección de las zonas sensibles o críticas**, como las líneas de producción, zonas de almacenamiento de materias primas o productos elaborados, etc. Controlar especialmente las zonas donde estén los paneles de control, para detectar la presencia en dichas áreas.

3) **Protección de la instalación fuera del horario laboral**, para detectar intrusiones cuando las instalaciones están vacías.

4) **Protección de la cadena de suministro**, pudiendo instalar sensores de apertura y/o movimiento en los vehículos de transporte.

5) **Disuasión frente a posibles sabotajes**, ya que la presencia de sistemas de detección de intrusiones actúa como un elemento disuasorio (si las instalaciones están protegidas, se reduce el riesgo de intentos de contaminación intencionados).

6) **Registro y trazabilidad** de los eventos de intrusión, que permitan revisar incidentes pasados, o identificar patrones de comportamiento sospechosos.

5.3.2. Recomendaciones fundamentales

El sistema de detección de intrusión debe ser robusto,

1) **Proteger el perímetro exterior,** tanto el vallado (con sensores como los indicados anteriormente en el punto 5.3.1), como las puertas (con contactos magnéticos) y ventanas (también con contactos magnéticos, detectores de rotura de cristales o detectores de cortina).

2) **Proteger las zonas interiores críticas**, como**:**

   - ✓ Zonas de almacenamiento de materias primas
   - ✓ Líneas de producción
   - ✓ Zonas de embalaje y etiquetado
   - ✓ Zonas de almacenamiento de productos elaborados
   - ✓ Zonas de oficina
   - ✓ Laboratorios de calidad o investigación
   - ✓ Zonas de manipulación de productos peligrosos o con equipamiento sensible
   - ✓ Cuarto de servidores o CPD (centro de proceso de datos)
   - ✓ Zonas con materiales valiosos
   - ✓ Zonas de residuos peligrosos

3) **Utilizar la mejor tecnología que se adapte a cada caso de uso**, y en aquellas zonas más críticas, ubicar varios sensores y combinar diferentes tecnologías para asegurar la detección.

4) **Ubicar los sensores de forma correcta** de acuerdo a sus características, a fin de evitar falsas alarmas debidas a una mala instalación.

5) **Utilizar sistemas acústicos y visuales**, mediante el uso de sirenas o luces estroboscópicas, para alertar de una posible intrusión, y actuar como medio disuasorio.

6) **Utilizar un panel de control que disponga de doble vía de transmisión** (Ethernet y red móvil), para garantizar que las señales de alarma se transmitan de manera confiable al centro de control y/o a la central receptora de alarmas (CRA).

7) **Notificar los eventos en tiempo real,** tanto al centro de control y/o central receptora, como al personal de seguridad.

8) **Integración de imágenes o vídeo para la verificación de alarmas**, bien mediante el uso de detectores de movimiento con cámara integrada, o de sistemas de videovigilancia integrados con el sistema de intrusión. Esto aportará una verificación visual al evento de alarma generado por el sensor.

9) **Disponer de protección frente a manipulaciones** tanto en el panel de control como en todos los dispositivos del sistema, a fin de detectar cualquier sabotaje de los mismos, así como de cualquier intento de sabotaje de las comunicaciones inalámbricas o cableadas del panel y/o de los dispositivos.

10) **Utilizar protocolos de comunicación cifrados**, no sólo entre el panel de control y el centro de control y/o CRA, sino también entre el propio panel y los dispositivos de intrusión (ya sean cableados o inalámbricos), a fin de evitar intentos de manipulación de las señales o reemplazo de dispositivos.

11) **Integrar el sistema de intrusión con otros sistemas de seguridad**, a través de plataforma de integración, como p.ej. los sistemas PSIM (Physical Security Information Management).

12) **Mantener y actualizar el sistema de intrusión** de forma regular, con mantenimientos preventivos regulares que garanticen el correcto funcionamiento de todos los elementos del sistema, así como de la actualización del firmware para incorporar nuevas funcionalidades o corrección de vulnerabilidades.

5.4. Sistemas de seguimiento de activos valiosos y rastreo en movilidad

Los sistemas de seguimiento de activos valiosos y rastreo en movilidad son herramientas tecnológicas que desempeñan un papel importante en la implementación de un plan de defensa alimentaria, ya que permiten monitorear y proteger activos críticos, como materias primas, productos terminados, equipos o vehículos, lo que ayuda a prevenir actos de sabotaje, contaminación intencional o robos.

5.4.1. Principales usos y aplicaciones

1) **Monitorización de materias primas y productos terminados**, permitiendo rastrear la ubicación y el estado en tiempo real.

2) **Protección de vehículos de transporte** mediante GPS, alertando en tiempo real de posibles desviaciones no autorizadas, que puedan indicar un intento de contaminación intencional.

3) **Ubicar e inmovilizar vehículos en tiempo real** para prevenir el robo de carga.

4) **Protección de activos críticos**, monitorizados mediante tecnologías de RFID o GPS.

5) **Control de acceso a activos críticos**, por ejemplo utilizando etiquetas RFID que requieren una autorización para ser retiradas o movidas.

6) **Garantizar la seguridad de los alimentos en toda la cadena de suministro**, p.ej. utilizando sensores IoT para monitorizar la temperatura y humedad y garantizar así que no se rompe la cadena de frío.

7) **Mejora en la eficiencia operativa**, al optimizar la gestión de inventarios y reducir pérdidas por robos o extravíos.

8) **Registro y trazabilidad**, útil en caso de auditorías o detección de irregularidades.

5.4.2. Recomendaciones fundamentales

Un sistema de seguimiento de activos valiosos y rastreo en movilidad debe integrar diversas tecnologías avanzadas, como RFID, GPS e IoT, para ofrecer una solución integral de monitoreo, protección y trazabilidad.

1) **Identificar los activos valiosos** mediante etiquetas RFID (Radio Frequency Identification), que permite el seguimiento en tiempo real de los activos, tanto dentro de las instalaciones como en el transporte. Las etiquetas RFID pueden proporcionar información detallada sobre el estado del producto, su ubicación y su trayecto.

2) **Identificación de activos menos valiosos** con opciones más económicas como códigos de barras o códigos QR, que pueden ser escaneados en puntos de control para asegurar su seguimiento.

3) **Proteger los activos frente a manipulaciones**, p.ej. utilizando cierres electrónicos o sellos de seguridad inteligentes.

4) **Integrar múltiples alertas y centralizar su gestión y control** a través del Centro de Operaciones de Seguridad (COS) y la Central Receptora de Alarmas (CRA).

5) **Integración con sistemas ERP**

6) **Cumplir con las normativas y regulaciones a nivel de protección de datos,** en el caso de que se rastreen empleados o se recopilen datos sensibles.

7) **Mantener y actualizar el sistema de seguimiento de activos valiosos y rastreo en movilidad**, asegurándose que los dispositivos de rastreo (etiquetas RFID, dispositivos GPS, sensores IoT, etc.) funcionan correctamente y están calibrados, actualizando el software para mejorar la seguridad y añadir nuevas funcionalidades.

5.5. Sistema de gestión centralizada de seguridad y emergencias (PSIM)

Los sistemas de gestión centralizada de seguridad y emergencias, conocidos como PSIM (Physical Security Information Management), son plataformas software que integran y gestionan múltiples sistemas de seguridad en una única interfaz.

Con independencia de que los sistemas tengan una supervisión centralizada por parte del cliente (bien en local o de forma remota), es fundamental que los principales sistemas de seguridad (como intrusión, incendio o vídeo) estén conectadas a una Central Receptora de Alarmas que reciba, gestione y actúe ante las señales de alarma provenientes de los sistemas de seguridad.

5.5.1. Principales usos y aplicaciones

1) **Integración de diferentes sistemas de seguridad,** principalmente:
   - Sistemas de control de accesos
   - Sistemas de videovigilancia
   - Sistemas de detección de intrusiones
   - Sistemas de geolocalización
   - Sistemas de detección de incendios
   - Sistemas de alarma y notificación
2) **Monitorización en tiempo real de las zonas críticas**, como líneas de fabricación, zonas de almacenamiento, zonas de acceso, etc.
3) **Incluir una solución de planimetría** que permita la personalización de cada proyecto, ubicando los diferentes elementos de cada subsistema en los planos de la instalación, aportando una interfaz gráfica rápida y sencilla a la hora de tramitar alarmas o realizar acciones sobre los distintos elementos.
4) **Gestión de incidentes y emergencias**, pudiendo activar protocolos de respuesta automáticos y notificándolo a los agentes y autoridades pertinentes.
5) **Detección temprana de amenazas**, al integrar los sistemas de intrusión con los de videovigilancia.
6) **Gestión de visitas y proveedores**
7) **Generación de informes**, útiles p.ej. en auditorías.
8) **Análisis de datos**, para identificar patrones o mejorar los protocolos.

5.5.2. Recomendaciones fundamentales

Un sistema de gestión centralizada de seguridad y emergencias ayuda a mantener la seguridad de los activos alimentarios, prevenir incidentes, y mejorar la capacidad de respuesta ante cualquier amenaza que pueda comprometer la seguridad alimentaria.

1) **Integrar todos los sistemas de seguridad y emergencias de la instalación en una única interfaz**, permitiendo a los operadores visualizar y gestionar de manera centralizada toda la información y alarmas.

2) **Monitorizar en tiempo real todos los sistemas de seguridad**, pudiendo los operadores acceder a la visualización de cada subsistema o elemento por separado en todo momento.

3) **Disponer de un sistema de automatización de respuestas** que se pueda configurar en base a las necesidades de cada instalación.

4) **Recopilar y almacenar los datos** para facilitar la toma de decisiones.

5) **Generar informes detallados** sobre eventos, incidentes y respuestas.

6) **Permitir realizar análisis predictivos** basados en los datos recopilados.

7) **Permitir realizar simulacros**, actuando sobre el estado de los sistemas y comprobar así que los procedimientos son correctos.

8) **Integrar el rastreo y trazabilidad de activos valiosos**.

9) **Permitir una escalabilidad y flexibilidad** frente a futuras ampliaciones o cambios en los protocolos o normativas.

10) **Cumplir con las normativas y regulaciones a nivel de protección de datos.**

11) **Mantener y actualizar el sistema de gestión centralizada de seguridad y emergencias** para garantizar el correcto funcionamiento del PSIM y mantenerlo actualizado y protegido frente a fallos de ciberseguridad. Las actualizaciones deben planificarse para evitar interrupciones en el servicio.

5.6. Interoperabilidad con sistemas de control de señales técnicas y PCI

Los sistemas de control de las señales técnicas aseguran que los procesos de almacenamiento, manipulación y generación de productos alimentarios se realicen de forma adecuada.

Así mismo, los sistemas de protección contra incendios en fábricas y sistemas de distribución alimentaria están diseñados para prevenir, detectar y mitigar incendios. Estos sistemas incluyen detectores de humo y calor, rociadores automáticos, extintores y alarmas. Su propósito fundamental es salvaguardar vidas humanas, proteger bienes y asegurar la continuidad del negocio.

Se recomienda que, en fase de diseño o actualización de los sistemas de control de proceso o PCI, se considere **la interoperabilidad con los sistemas de seguridad** descritos en los puntos anteriores.

Este enfoque integral, a partir de la centralización de señales e interoperabilidad entre sistemas permite la gestión unificada de espacios, personas, maquinaria y mercancías, claves para un mayor control y mejora en la capacidad de respuesta ante posibles incidentes.

Esta gestión es compatible con la normativa y los procesos de seguridad desarrollados desde los Centros de Control de seguridad de las plantas de producción o por determinadas CRAs, previa formación y especialización de los operadores, ingenieros y personal de soporte.

En cualquier caso, en lo referente a interoperabilidad, ya sea entre los sistemas de seguridad o con el resto de sistemas presentes en las plantas de producción, se recomienda, como mejores prácticas, seguir las pautas establecidas en la guía de AES “Guía de interpretación instalaciones grado 3 y 4“
https://www.aesseguridad.es/documentacion/AES_Guia_Interpretacion_WEB.pdf en lo referente a la aplicación de la norma UNE 50398.

5.7. Ciberseguridad: acciones clave

Es esencial que las empresas alimentarias no solo se enfoquen en la seguridad física de los productos, sino también en la seguridad digital, se deben proteger los datos y asegurarse de que las operaciones puedan continuar incluso frente a la amenaza de un ciberataque.

Los sistemas y equipos de TI deben minimizar los riesgos para proteger a las empresas, lo que puede implicar la delimitación o aislamiento de los sistemas vulnerables. El perimetrado es una forma de protección de datos en la que se construyen protecciones alrededor de aplicaciones en línea y subredes para reducir los riesgos de seguridad.

Se debe considerar que multitud de ciberataques se producen por error de los empleados. Para poder solucionar este problema, es muy importante la formación y concienciación de los empleados. Para ello, pueden realizarse sesiones formativas y de concienciación sobre los problemas que puede conllevar un ciberataque y buenas prácticas de cómo se podrían evitar.

En el caso de que el riesgo siga siendo alto, las empresas deben adoptar las medidas de protección más adecuadas mediante la aplicación de las mejores prácticas, como por ejemplo, la implantación de un sistema de gestión basado en normas internacionales como ISO/IEC 27001, que permite desarrollar un enfoque sólido y estructurado para gestionar los riesgos y proteger los activos sensibles.

5.7.1. Recomendaciones fundamentales

En lo referente a la aplicación de medidas y controles de **ciberseguridad sobre sistemas de seguridad,** para complementar y profundizar a lo indicado en los puntos anteriores, se recomienda seguir las pautas establecida en las siguientes guías:"

- **"Guía Sobre Controles De Seguridad En Sistemas OT"** del Ministerio del Interior.
- **"EINSE 10/21. Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física"** del Grupo de Trabajo de AEINSE, "Ciberseguridad aplicada a los Sistemas de Seguridad Física".
- **"ENISA Threat Landscape 2023"** y siguientes**,** en todo lo relativo a la cadena de suministro (Supply chain) disponible en la web https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Algunas de esas acciones podrían ser:

- Implementación de autenticación multifactor, sobre todo para acceder a datos confidenciales o a cuentas personales.
- Realización de copias de seguridad de los dispositivos y datos más importantes de la empresa que permitan seguir con la producción de forma rápida y sencilla ante un incidente.
- Actualización de sistemas: mantener todos los sistemas, no solo los de IT, sino también los de OT y de Seguridad Física, y todas las aplicaciones de software actualizadas para protegerse contra las amenazas más recientes.
- Implementar tecnologías y dispositivos específicos de ciberseguridad, como por ejemplo cortafuegos, IDS, antivirus, etc. Todo esto te permitirá tener una mayor visibilidad y control de todos los activos que se pueden introducir en tus dispositivos. Además, la gestión de accesos externos deberá realizarse mediante métodos comúnmente aceptados en la industria, como una VPN. Las redes inalámbricas también son un punto a tener en cuenta ya que su uso puede ser aprovechado en un ataque ya sea interfiriendo en las señales, denegando el uso de la red, o interceptando las diferentes credenciales.
- La securización y bastionado[4] de los dispositivos es un aspecto muy importante para que los dispositivos posean ya una seguridad de base. Dentro de este punto, se contemplan la eliminación de servicios que no se utilicen, la implementación de métodos de seguridad en las comunicaciones, el cierre de los puertos vulnerables o no utilizados y la implementación de protocolos seguros. Así mismo, la reducción de usuarios, la gestión de roles y permisos y las cuentas de administrador también se encontrarían asociadas al bastionado de los equipos.
- Auditorías regulares: realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.
- Simulacros de ciberataque: implementar simulacros de ciberataques para evaluar la efectividad de los protocolos de respuesta y mejorar donde sea necesario.
- Formación continua: capacitar al personal en prácticas seguras y concienciar sobre la importancia de la ciberseguridad.

[4] El bastionado de equipos, también conocido como "hardening", es un proceso de seguridad informática que consiste en asegurar un sistema informático reforzando sus defensas contra ataques. Esto se logra eliminando o desactivando componentes y funciones innecesarias, configurando adecuadamente el sistema y aplicando parches de seguridad para minimizar las vulnerabilidades que podrían ser explotadas por atacantes.

En términos más simples, el bastionado busca reducir la superficie de ataque de un sistema, es decir, la cantidad de puntos débiles que un atacante podría aprovechar para comprometer el sistema

6 Glosario de términos

AES: Asociación Española de empresas de Seguridad

AEINSE: Asociación Española de Ingenieros de Seguridad

APPCC: Análisis de Peligros y Puntos de Control Crítico, ver HACCP.

BRC: del inglés British Retail Consortium, la norma BRC es un sistema de seguridad alimentaria desarrollado por la distribución minorista británica.

CARVER + Shock: (Criticality / Accessibility / Recuperability / Vulnerability / Effect / Recognizability) es una metodología para evaluar vulnerabilidades y priorizar objetivos en la seguridad de alimentos, o en general, en la seguridad de cualquier sistema o infraestructura.

CCTV: Circuito Cerrado de Televisión

COS: Centro de Operaciones de Seguridad

CPD: Centro de Procesos de Datos

CRA: Central Receptora de Alarmas

EPI: Equipo de Protección Individual

FDA: Food and Drug Administration, Administración de Alimentos y Medicamentos de EE. UU.

FSMA: Food Safety Modernization Act

FSSC 22000: Food Safety System Certification

GFSI: (Global Food Safety Initiative) significa "Iniciativa Mundial de Seguridad Alimentaria" y es una organización que identifica y reconoce programas de seguridad alimentaria que cumplen sus estándares.

GPS: Global Positioning System, en español, "Sistema de Posicionamiento Global". Es un sistema de navegación por satélite que permite determinar la posición de un objeto en la Tierra con alta precisión, usando las señales transmitidas por una red de satélites en órbita terrestre.

HACCP: del inglés Hazard Analysis and Critical Control Point o APPCC en español, es un sistema de gestión de la seguridad alimentaria que identifica, evalúa y controla los peligros biológicos, químicos y físicos en los procesos de producción de alimentos.

IDS: del inglés Intrusion Detection System o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas.

IFS: abreviatura de International Featured Standards, es un protocolo privado de seguridad alimentaria, desarrollado por grandes distribuidores europeos, con el objetivo de garantizar la seguridad y calidad de los productos alimenticios y los procesos de producción.

IT: del inglés Information Technology, Tecnología de la Información se refiere al uso de computadoras y redes digitales para almacenar, transmitir y manipular datos.

OT: del inglés Operation Technology, Tecnología Operacional (OT) se refiere al conjunto de hardware y software que supervisa y controla los equipos físicos, procesos y eventos en entornos industriales.

IoT: por sus siglas en inglés Internet of Things, el Internet de las Cosas (IoT, por sus siglas en inglés) es una red de dispositivos físicos (objetos, vehículos, etc.) que se conectan a internet y pueden comunicarse entre sí y con otros sistemas.

ISO: International Organization for Standardization, que en español significa "Organización Internacional de Normalización". Es una organización independiente y no gubernamental que reúne a expertos de todo el mundo para desarrollar normas internacionales, también conocidas como normas ISO.

IEC: del inglés International Electrotechnical Commission, es una organización internacional que desarrolla y publica normas internacionales en el ámbito de la tecnología eléctrica, electrónica y relacionadas.

PSIM: por sus siglas en inglés Physical Security Information Management, la gestión de información de seguridad física (PSIM) es una categoría de software que proporciona una plataforma y aplicaciones creadas por desarrolladores de middleware, diseñadas para integrar múltiples aplicaciones y dispositivos de seguridad no conectados y controlarlos a través de una interfaz de usuario integrada.

PTZ: del inglés Pan-Tilt-Zoom, significa Panorámica, Inclinación y Zoom. Donde Pan significa rotar, una cámara PTZ es una cámara controlable que puede moverse en 3 ejes.

QR: Quick Response

RAID: del inglés Redundant Array of Independent Disks, significa una agrupación de discos duros que se utiliza para mejorar el rendimiento, la capacidad de almacenamiento y la fiabilidad de los datos. Es un método para combinar varios discos duros físicos como si fueran una sola unidad lógica.

RFID: del inglés Radio Frequency Identification, o Identificación por Radiofrecuencia. Es una tecnología que utiliza ondas de radio para identificar y rastrear objetos, personas o animales de forma automática.

VAB: o Valor Agregado Bruto, es un indicador económico que mide el valor de todos los bienes y servicios producidos en un área económica, menos el valor de los bienes y servicios utilizados en su producción. En otras palabras, representa la contribución de cada unidad de producción, industria o sector al Producto Interno Bruto (PIB)

VPN: del inglés Virtual Private Network, Red Privada Virtual, es una herramienta que crea una conexión segura y privada a internet, ocultando la dirección IP y encriptando los datos. Esto te permite navegar con mayor anonimato y seguridad, protegida de posibles amenazas en línea.

Elaborado por el Área de
Seguridad Electrónica de:

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225

www.aesfundacion.es
patronato@aesfundacion.es

@FundacionAES AES Fundación aes_fundacion_