Seguridad y Ayudas para la implantación del Cuaderno Digital de Campo

Jornadas Demostrativas “Cuaderno Digital de Campo: Soluciones Innovadoras”
4 de Mayo 2023

José Manuel Fresno
Director Area de Digitalización

artica
ideas • ingeniería • innovación

artica



Más de 25 años de experiencia

Somos una firma de referencia en servicios de Consultoría técnica e Ingeniería, orientada a formular e implementar soluciones óptimas para Industrias alimentarias, logísticas y afines de alto estándar sanitario, entre otros sectores.

Tres unidades de negocio para estructurar nuestros servicios: **Ingeniería, Consultoría para la Innovación y Digitalización.**


Nuestras áreas de especialización y servicios

Ingeniería

- Estudio y definición de proyectos
- Etapa de Proyecto (metodología BIM)
- Etapa de Ejecución
- Ingeniería Inversa
- Asistencia tras el cierre del Proyecto
- Project Management
- Diagnóstico y Estudio de Situación
- Plan de Actuación por Fases
- Trabajos y Proyectos Especiales

Consultoría para la Innovación

- Financiación Proyectos Nacionales
- Financiación Proyectos Internacionales
- Ayudas a la inversión Innovadora
- Fiscalidad I+D+i
- Comunicación de la Innovación
- Gestión Integral de la Innovación
- Diagnóstico de Actividades I+D+i
- Gestión de Plataformas y Clusters
- Gestión Next Generation EU

Digitalización

- Consultoría Madurez Digital
- Consultoría Conectividad e Integración de Sistemas
- Consultoría Redes y Comunicaciones entornos Producción
- Consultoría Renovación entorno IT
- Ciberseguridad Entorno Industrial
- Inteligencia aplicada a la Industria
- Automatización de Procesos
- Monitorización inteligente
- Fabrica Digital. Modelo 3D. Soluciones BIM

DIGITALIZACION

Soluciones para la Transformación Digital

Catálogo de Soluciones Artica+i

Consultoría y Estudios

- Estudio Madurez Digital
- Consultoría de Sistemas, adopción de soluciones Cloud, renove tecnológico. Integración entornos producción no conectados
- Consultoría orientada a mejora del proceso productivo. Establecimiento de Objetivos y definición de métricas
- Consultoría Seguridad y Redes Integración IT-OT

Aplicaciones para Dinamización de Negocio

- Portales WEB,
- Tienda Online
- ERP, CRM, BPM…

Digitalización en los entornos de Producción.

- Rendimiento producción, previsión de fabricación, estimación precios objetivo,…)
- Valoración fallo potencial y situaciones de riesgo. Consola Central de Alarmas. Control de Calidad
- Modelado y digitalización 3D. BIM (Building Information Modeling)
- Gemelos Digitales (Entrenamiento y Formación operarios, Mantenimiento asistido, Operación remota de entornos

Inteligencia aplicada a Entornos Industriales. Soporte en toma de Decisión. Monitorización Inteligente

- Análisis predictivo (Rendimiento producción, previsión de fabricación, estimación precios objetivo,…)
- Valoración fallo potencial y situaciones de riesgo. Consola Central de Alarmas. Control de Calidad
- Automatización de procesos . (Aplicaciones M2M , B2M) Programación de API´s, control Stock-fabricación

Ciberseguridad.

- Consultoría y Auditorías de Seguridad / Análisis de Riesgos
- Segmentación / Conexión Redes IT-OT / Protección Perimetral/ Antimalware/ Seguridad en la nube
- Soluciones DLP / EDR/ UEBA / Plan de Continuidad/ Respaldo de Datos
- Seguridad Gestionada / Monitorización y Gestión de Incidentes

Punto de Partida….

Estamos sumergidos en un avanzado proceso de **Transformación Digital**, en el que la tecnología evoluciona a un ritmo vertiginoso.

Supone una **revolución en todos los procesos** de cualquier empresa: comunicación interna, relación con los proveedores, logística, producción, marketing, atención al cliente, selección y formación de personal, internacionalización, innovación, etc…

Es cada vez más frecuente el **uso de dispositivos móviles y servicios en la nube** para el desarrollo de nuestra actividad. Estos avances tecnológicos aportarán oportunidades y beneficios proporcionando nuevos modelos de negocio, nuevas formas de interacción con los clientes y nuevas formas de trabajo para los empleados

Ciberseguridad

Punto de Partida….

Situación Ciberseguridad 2022

El avance en el proceso de Digitalización de las organizaciones amplia la **superficie de exposición** a los ciberataques de forma exponencial.

La **superficie de ataque global** es de naturaleza dinámica: se expande y cambia constantemente

El **phishing por correo electrónico** y la **ingeniería social** siguen siendo los medios más comunes y fiables para acceder ilegalmente a una red

El **malware aumentó un 358**% y el **ransomware un 435% en 2020,** y el incremento ha continuado con igual ritmo en 2021 y 2022

Solo **el 57% de los ataques de ransomware** han sido mitigados con éxito mediante la **restauración de copias de seguridad**.

El **40% de las PYMEs** que se enfrentaron a un ciberataque experimentaron **al menos ocho horas de inactividad**. El tiempo de inactividad representa gran parte de los daños financieros globales de una violación de la seguridad. (CISCO Systems 2022)

Cada vez hay más ataques dirigidos a las pequeñas y medianas empresas. **Mientras que el 43% de los ciberataques van dirigidos a las pequeñas empresas**, sólo el 14% se considera preparado, consciente y capaz de defender sus redes y datos. (Accenture)

Los daños del **ransomware** a nivel mundial y el pago de rescates sumaron más de **20.000 millones de dólares** en 2021. Se espera que esta cifra aumente a **más de 265.000 millones** de dólares en 2031. (Cloudwardas.net)

Los **ciberdelincuentes pueden penetrar** de forma fiable en el **93% de las redes** de las organizaciones. (pentesting analysis Positive Technologies)

Punto de Partida….

Conclusiones Ciberseguridad 2022

No es posible garantizar las **seguridad absoluta**.

Año tras años se bate el record en número de ciberataques!!

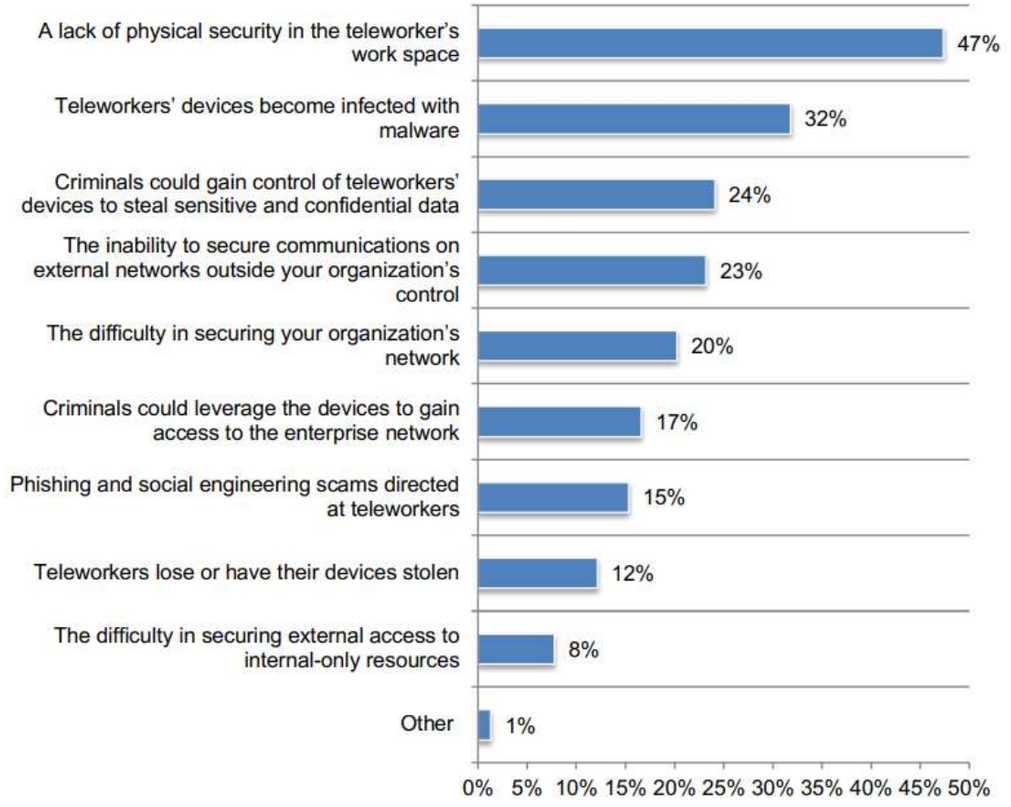
Cualquier organización es hoy en día un objetivo para los Ciberdelincuentes Las pymes no están al margen de este entorno tecnológico

Los planes de protección de las empresas deben ir orientados a **reducir el riesgo** de sufrir un ciberataque y **minimizar el impacto** que éstos puedan producir.

Debe de considerarse el **refuerzo de las medidas de seguridad cuando decidamos adoptar** nuevas tecnologías**.** (P.E. Web 3.0 –> autenticación Multifactor, Sistemas basados en Inteligencia Artificial → Análisis periódico de vulnerabilidades, Cifrado de datos,…)

Las **inversiones en Ciberseguridad** deben ir en consonancia con el **valor de los activos a proteger** y el **riesgo considerado aceptable** en cada organización.

Preocupación sobre Riesgos de Seguridad en organizaciones
(fuente Ponemon Institute 2021 - 2022)



Protección de la Información

Vulnerabilidades a tener en cuenta:

Las **vulnerabilidades en el entorno TIC**, se corresponden a lagunas o debilidades presentes en la red, las aplicaciones y en general en cualquier sistemas de información de la organización relacionadas con bugs de las aplicaciones, configuraciones erróneas de puertos, hosts, servicios, etc…

La tendencia a las transacciones basadas en **servicios WEB** hacen que tengamos que poner especial atención a las vulnerabilidades en las comunicaciones , plataformas y mecanismos relacionados con nuestras propias webs o con webs de terceros..

OWASP (Open Web Application Security Project)
Top 10 Vulnerabilities 2023

1. **Broken Access Control**
2. **Cryptographic Failures**
3. **Injection**
4. **Insecure Design**
5. **Security Misconfiguration**
6. **Vulnerable and Outdated Components**
7. **Identification and Authentication Failures**
8. **Software and Data Integrity Failures**
9. **Security Logging and Monitoring**
10. **Server-Side Request Forgery**

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Principales amenazas: El **phishing** se coloca como el incidente más frecuente, cerca de 17.000 casos. **Malware,** más de 14.000 incidentes. R**ansomware**, cerce de 450 incidentes.

1. Phishing - Ingeniería social: aprovechar el error humano para acceder a información o servicios

Consiste en engañar a las víctimas para que abran documentos, archivos o correos electrónicos maliciosos, visiten sitios web y, de este modo, concedan acceso no autorizado a sistemas o servicios. El ataque más común de este tipo es el **phishing** (siuplantación de identidad a través del correo electrónico) o el **smishing** (a través de mensajes de texto) Se percibe procesos de **vishing (intevienen mensajes de voz)**.

Cerca del 60% de los ataques en Europa, Oriente Medio y África incluyen un componente de **ingeniería social,**
En cuanto a los incidentes que han afectado a ciudadanos y empresas:

- **uno de cada tres ha sido debidos a una filtración de datos,** tanto información sensible o protegida, como datos confidenciales que son robados por una persona no autorizada.

- **dos de cada cinco se han tratado de vulnerabilidades o fallos de sistemas tecnológicos**.

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

2. Malware: software diseñado para dañar o controlar de forma ilícita un sistema

El malware incluye virus, gusanos, troyanos y programas espía. Tras descender en todo el mundo coincidiendo con la pandemia en 2020 y principios de 2021, su difusión aumentó en gran medida a finales de 2021, cuando los trabajadores comenzaron a volver a la oficina.

El aumento del malware también se atribuye al cryptojacking (el uso secreto del ordenador de una víctima para crear criptodivisas ilegalmente) y al malware del Internet de las Cosas (malware dirigido a dispositivos conectados a internet, como routers o cámaras).

Según ENISA en los seis primeros meses de 2022 se produjeron más ataques al **Internet de las Cosas que en los cuatro años anteriores.**

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

3. Ransomware: Los ciberdelincuentes toman el control de los datos de alguien y exigen un rescate para restaurar el acceso

En 2022, los ataques de ransomware fueron la principal ciberamenaza. A día de hoy son ataque de alta sofisticación y complejidad.

Según una encuesta citada por ENISA que se realizó a finales de 2021 y en 2022, más de la mitad de los encuestados o sus empleados sufrieron ataques de ransomware.

Los mismos datos muestran que la mayor demanda de ransomware creció de 13 millones de euros en 2019 a 62 millones de euros en 2021 y el rescate medio pagado se duplicó de 71.000 euros en 2019 a 150.000 euros en 2020. .

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

4. Amenazas contra los datos: atacar las fuentes de datos para obtener acceso no autorizado y divulgación

La economía actual produce enormes cantidades de datos de gran importancia para, entre otros, las empresas y la inteligencia artificial, lo que interesa a los ciberdelincuentes. Las amenazas contra los datos pueden clasificarse principalmente en **violaciones de datos** (ataques intencionados de un ciberdelincuente) y **fugas de datos** (divulgación involuntaria de datos).

El dinero sigue siendo la motivación más común de estos ataques. En el 10% de los casos el motivo es el espionaje.

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

5. Amenazas contra la disponibilidad - denegación de servicio: ataques que impiden a los usuarios acceder a datos o servicios

Estas son algunas de las amenazas más críticas para los sistemas informáticos y su alcance y complejidad aumentan. Una forma común de ataque es sobrecargar la infraestructura de red y hacer que un sistema no esté disponible. Los ataques de denegación de servicio afectan cada vez más a las redes móviles y a los dispositivos conectados. Se utilizan con frecuencia en la ciberguerra entre Rusia y Ucrania. Los sitios web relacionados con la pandemia de Covid-19, como los destinados a vacunarse, también han sido blanco de ataques.

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

6. Amenazas contra la disponibilidad - amenazas contra internet: amenazas contra la disponibilidad de internet

Incluyen bloqueo de acceso por Denegación de Servicio (DDoS) afectando tanto a los sistemas, a las infraestructuras físicas por destrucción de la infraestructura de internet, o por saturación de tráfico o bloqueo provocado de los sistemas que intervienen en la comunicación , como se ha visto en los territorios ucranianos ocupados desde la invasión, así como la censura activa de sitios web de noticias o medios sociales.

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

7. Desinformación/mal uso de la información: difusión de información engañosa

El aumento del uso de las plataformas de redes sociales y los medios de comunicación en línea ha conllevado al incremento de las campañas de difusión de desinformación (información falsificada a propósito) y desinformación (compartir datos erróneos) para causar miedo e incertidumbre.
Rusia ha utilizado esta tecnología para manipular la percepción de la guerra.
La tecnología **Deepfake** permite generar audio, vídeo o imágenes falsos que casi no se distinguen de los reales. Los robots que se hacen pasar por personas reales pueden perturbar las comunidades en línea inundándolas de comentarios falsos

Protección de la Información

Resumen del Informe de 2022 de la Agencia de la Unión Europea para la Ciberseguridad (ENISA)

8. Ataques a la cadena de suministro: atacar la relación entre organizaciones y proveedores

Se trata de una combinación de dos ataques: contra el proveedor y contra el cliente.
Las organizaciones son cada vez más vulnerables a este tipo de ataques, debido a la creciente complejidad de los sistemas y a la multitud de proveedores, que son más difíciles de supervisar

Protección de la Información

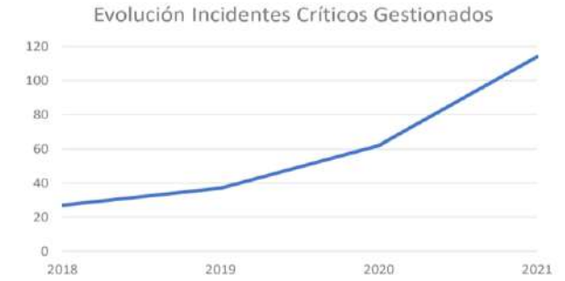
INSTITUTO NACIONAL DE CIBERSEGURIDAD

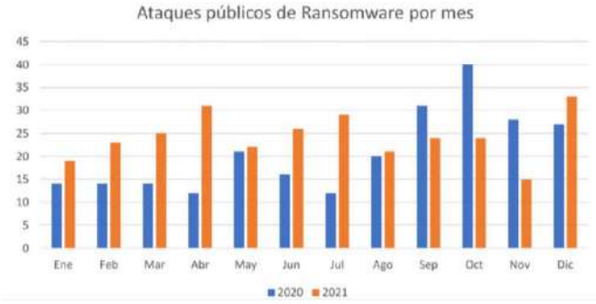
Balance Ciberseguridad en España en 2022

El Centro de Respuesta a Incidentes de Seguridad del Instituto Nacional de Ciberseguridad (Incibe-CERT) gestionó 118.820 ciberincidentes en 2022, un **nueve por ciento** más que en el año anterior. Más de 110.000 de los incidentes afectaron a ciudadanos y empresas, 546 a operadores estratégicos y 7.980 a la Red Académica y de Investigación Española.

En concreto, en lo relacionado con los incidentes a ciudadanos y empresas, **uno de cada tres fueron una filtración de datos sensibles**, y dos de cada cinco pertenecieron a vulnerabilidades de sistemas tecnológicos.

Durante 2022, Incibe documentó **26.431 nuevas vulnerabilidades**, un **20 por ciento más** que en el año anterior.





Protección de la Información

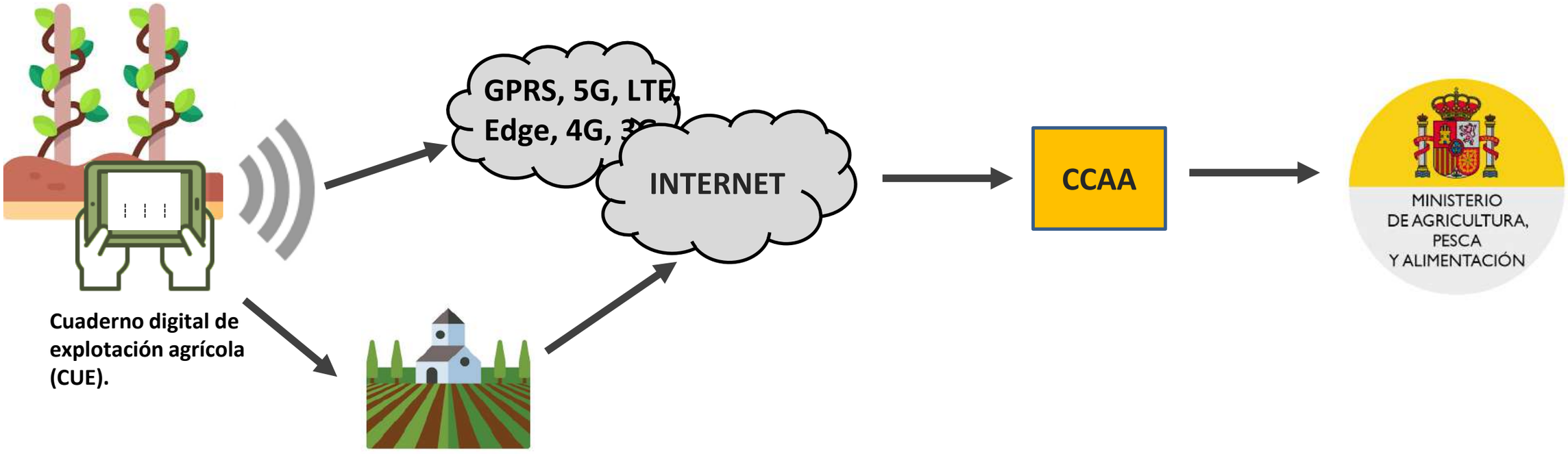
Seguridad en el Plan de Digitalización agrícola en España

El 27 de diciembre se publicó en el BOE el Real Decreto que regula el uso del Cuaderno Digital, por el que se establece y regula el Sistema de información de explotaciones agrícolas y ganaderas y de la producción agraria (SIEX), que pretende integrar gran parte de los Registros autonómicos de explotaciones agrícolas (REA) y establece fechas de implantación del Cuaderno digital de explotación agrícola (CUE).

1. Sistema de registro digitalizado
2. Obligatoriedad (desde 1 Sep 2023)
3. Registro de actividad completo
4. Contener información Detallada
5. Permitir Trazabilidad
6. Plataforma Digital Centralizada y Segura

Garantizar la Confidencialidad
Garantizar la Integridad
Garantizar la Disponibilidad
Garantizar la Autenticidad

Protección de la Información



Debes contar con una **herramienta ágil para crear todos los registros de la forma más automática posible y que te ayude a cumplir con todas las regulaciones** recogidas en el Real Decreto, ….

No debes olvidar establecer un **procedimiento de captación y envío de Datos** que garantice su **seguridad.**

Protección de la Información

10 buenas prácticas para mejorar la Ciberseguridad

1. Definir **políticas y procedimientos** para establecer el Nivel de Seguridad óptimo necesario en la empresa y un **plan de respuesta ante incidentes**
2. Establecer una **clasificación adecuada de la información** y aplicar el **control de acceso** correspondiente
3. Configurar de un sistema de **copia de Seguridad** que garantice la recuperación ante incidente de seguridad
4. Verificar la capacidad y estado de los soportes de información, a través de pruebas de recuperación de información periódica
5. Implantar un sistema adecuado de protección antimalware que minimice el nivel de riesgo de infecciones con especial atención a los puestos de usuario) móviles, tablets, portátiles puestos fijos… (
6. Reducir el nivel de riesgo a ser atacado , revisando de forma continua las vulnerabilidades de los sistemas
7. **Segmentar adecuadamente las redes** y establecer y **revisar periódicamente las configuraciones aplicadas en los cortafuegos**, permitiendo únicamente el tráfico de datos necesario.
8. Establecer programas de **concienciación en buenas practicas de Seguridad** para todos los empleados. La Ingeniería Social es el principal vector de difusión de un ataque!
9. **Monitorizar y registrar las alertas y avisos que puedan facilitar los sistemas** TIC para detectar potenciales amenazas y actuar con la máxima celeridad en su remediación.
10. Establecer un **plan de continuidad de Negocio**. Cualquier empresa está expuesta a sufrir un incidente grave de Seguridad.

Ayudas aplicables al Cuaderno Digital de Campo

artica

ideas • ingeniería • innovación

Programa Kit Digital

- **Subvención**: Alcance; Bono digital de hasta 12.000 €.

- Requisitos a cumplir por la empresa:

- Ser una pequeña empresa, microempresa o autónomo.
- Cumplir los límites financieros y efectivos que definen las categorías de empresas.
- Estar en situación de alta y tener la antigüedad mínima que se establece por convocatoria.
- No tener consideración de empresa en crisis.
- Estar al corriente de las obligaciones tributarias y frente a la Seguridad Social.
- No estar sujeta a una orden de recuperación pendiente de la Comisión Europea que haya declarado una ayuda ilegal e incompatible con el mercado común.
- No incurrir en ninguna de las prohibiciones previstas en el artículo 13.2 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.
- No superar el límite de ayudas *minimis* (de pequeña cuantía).

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
KIT DIGITAL
Financiado por la Unión Europea NextGenerationEU

Programa Kit Digital

CATEGORIAS SOLUCIONES DE DIGITALIZACION

Un bono digital con una cuantía económica para que la administres escogiendo una o varias soluciones digitales de las ofrecidas por los agentes digitalizadores que desarrollen los servicios del catálogo:

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
KIT DIGITAL
Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

artica

ACTIVA FINANCIACIÓN

Esta actuación persigue el apoyo a proyectos que promuevan la transformación digital de las empresas industriales al mismo tiempo que contribuyen a la mejora de su sostenibilidad ambiental como consecuencia de dicha digitalización.

- Instrumentos y características de la ayuda: los apoyos se configurar en formato mixto de préstamo y subvención con 2 líneas de actuación diferenciadas

  ACTIVA-pyme:

  ACTIVA-Grandes implementaciones

ACTIVA FINANCIACIÓN

ACTIVA-pyme: sólo para PYMEs. La ayuda se retornan en 5 años (2 años de carencia).
Recomendación UE nº 651/2014 de la Comisión (menos de 250 empleados y facturación inferior a 50 M€ anuales)

Aplica a proyectos de investigación industrial, desarrollo experimental, proyectos de innovación en materia de organización, proyectos de innovación en materia de procesos y proyectos de validación experimenta .

- Gastos Financiables :
  - Aparatos, equipos e infraestructura.
  - Colaboraciones externas.
  - Amortización del instrumental y equipos y alquiler de equipamiento para validación preliminar.

ACTIVA-Grandes implementaciones: para todas las empresas, con un periodo de retorno de 10 años (3 años de carencia)

Aplica a proyectos de investigación industrial, desarrollo experimental, proyectos de innovación en materia de organización (con restricciones) y proyectos de innovación en materia de procesos (con restricciones)

- Gastos financiables:
  - Costes de personal.
  - Instrumental y material inventariable.
  - Costes de investigación contractual, conocimientos técnicos y patentes.

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

ACTIVA FINANCIACIÓN

La financiación total a conceder, de préstamo nominal más subvención, será como máximo el 80% sobre el presupuesto financiable.

Prioridades temáticas:

- Plataformas de interconexión de la cadena de valor de la empresa (software).
- Soluciones para el tratamiento avanzado de datos (software).
- Soluciones de inteligencia artificial (software).
- Proyectos de simulación industrial (gemelo digital, software).
- Diseño y fabricación aditiva (simulador 3D, I+D+i, nuevos procesos o nuevos materiales y tintas...).
- Proyectos de realidad aumentada, realidad virtual y visión artificial.
- Robótica colaborativa y cognitiva (al menos un robot físico).
- Sensórica.

Requisitos:

CNAE encuadrado en la sección C- Divisiones 10 a 3 y actividades complementarias, realizadas al menos durante un periodo de tres años contados hasta la fecha de fin de plazo de solicitud.

FEADER: Ayudas para inversiones materiales e inmateriales

Ayudas para inversiones en transformación y comercialización de productos agrarios cofinanciadas por el Fondo Europeo Agrícola de Desarrollo Rural (Feader)

Ayudas en forma de subvención que se convocan y tramitan por cada Comunidad Autónoma.

Requisitos: presupuesto elegible **menores a 100.000€.**

Gastos financiables:

- Construcción o mejora de bienes inmuebles.
- Adquisición de maquinaria, salvo excepciones a consultar.
- Costes de arquitectos, ingenieros y asesoramiento sobre la sostenibilidad económica y medioambiental del proyecto.
- Inversiones intangibles: **adquisición o desarrollo de programas informáticos, adquisiciones de patentes o licencias.**

Características:

- Intensidad de la ayuda variable dependiendo de la característica de la empresa, el tipo de inversión y la Comunidad Autónoma donde se realice la inversión, por norma general, entre el 15% y el 25% del gasto subvencionable, pudiendo ser mayor en determinados casos muy específicos.

- Concurrencia competitiva, los proyectos se valorarán siguiendo unos criterios de evaluación teniendo en cuenta las características de la empresa, las propias del proyecto y del lugar de la inversión.

- La ayuda se percibe a la **finalización y justificación** de la inversión

PASVE : Plan de Ayudas al Sector Vitivinícola Español 2023-2027

Requisitos: presupuesto elegible **igual o superior a 100.000€.**

Gastos subvencionables:

- Construcción, adquisición o mejora de bienes inmuebles.
- Compra de nueva maquinaria y equipo hasta el valor de mercado del producto.
- Gastos administrativos como honorarios de arquitectura, ingeniería y asesoría, así como estudios de viabilidad.
- **Adquisición o desarrollo de soportes lógicos de ordenador y adquisición de patentes, licencias, derechos de autor y el registro de marcas colectivas.**

Características:

- Intensidad de la ayuda variable dependiendo de la característica de la empresa, el tipo de inversión y la Comunidad Autónoma donde se realice la inversión, por norma general, entre el 25% y el 50% del gasto subvencionable, pudiendo ser mayor en determinados casos muy específicos.
- La ayuda se percibe a la finalización y justificación de la inversión

¡Muchas Gracias!

artica

ideas •ingeniería •innovación

Madrid (Central)

c/ Musgo, 2. Edificio Europa II. Bajo B. 28023 Madrid. España

tel. +34 913 570 798

Valencia

Avda. de Cataluña, 13. Entresuelo, Despacho F. 46020 Valencia. España

tel. +34 963 621 260

Santiago de Compostela

Edificio WITLAND. c/ Rúa Camiños da Vida S/N. 2ª Planta
15705 Santiago de Compostela. La Coruña. España

tel. +34 981 937 990

www.articai.es