FREMM
Federación Regional de Empresarios del Metal Murcia

legitec
LEGISLACIÓN & TECNOLOGÍA

ACTIVA CIBERSEGURIDAD

Toma de contacto y Presentación del proyecto

legitec

CIBERSEGURIDAD

- Consultoría
- Legitec Backup Cloud
- Concienciación
- Teletrabajo
- Productividad
- Auditoría de Ciberseguridad
- Vigilancia Activa
- Vulnerabilidades en Apps

Activa Ciberseguridad

PROTECCIÓN DE DATOS

- Consultoría RGPD
- Delegado de protección de datos DPD/DPO
- Auditoría LOPD

DERECHO DIGITAL

- Aspectos legales de apps móviles y negocios digitales
- Aspectos legales del comercio electrónico
- LSSI – Política de Cookies

CUMPLIMIENTO/COMPLIANCE

- Cumplimiento Normativo
- Prevención de Blanqueo de Capitales
- Planes de igualdad

SISTEMAS DE GESTIÓN

- ISO 9001
- ISO 27001
- ISO 14001
- ENS-INES

Financiado por la Unión Europea
NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

EOI Escuela de organización industrial

legitec

WHOAMI

- Director Técnico de Legitec Ciberseguridad
- Perito informático por el colegio oficial y asociación de ingeniería informática de la región de Murcia
- Grado en Ingeniería Informática especializado en tecnologías de las comunicaciones
- Certified Ethical Hacking (CEHv12) – ECC Council
- Cisco CCNA: Cyber Ops
- Ransomware: Identify, Protect, Detect, Recover por (ISC)²
- Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013 por Bureau Veritas
- Top 10 nacional (I y II edición) en la NATIONAL CYBERLEAGUE de la guardia civil.
- Ganador del concurso Defensa y yo por la embajada de Estados Unidos
- Integrador de soluciones de fortinet (NSE4)

La UE realiza un simulacro de ciberataqu
prueba su capac

Europa Press Internaciona

Aumenta l

HISCOX
SEGUROS ESPECIALIZADOS

27 Mayo 2022

- El coste m
  euros
- El 43% de l
- El 28% de l

En los últim
hecho, el cos
euros, frente
las empresas
concluye en

El 60% de las pymes que

CCN-CERT
centro criptológico nacional

DEFENSA DAVANT DE LES CIBERAMENACES

CCN-CERT | Gestió d'incidents | Red Nacional de SOC | Formació | Guies | Informes | Solucions | ENS | Seguretat al dia | Comunicació | Registre

DARRERA HORA 07/02/2023 10:24

Actualizada la guía CCN-STIC 1614 sobre procedimiento de empleo seguro Fortinet FortiMail 6.2

Inici > Gestión de Incidentes > LUCIA > Noticias de actualidad

500.000 euros, coste medio de un ciberataque para las empresas

- Estadísticas e informes

Alrededor de 500.000 euros es el coste medio que deben afrontar las grandes empresas tras ser víctimas de un ciberataque, según recogen los datos de la Encuesta Global sobre seguridad TI corporativa – 2013 de B2B Internacional y Kaspersky Lab.

Los expertos de B2B Internacional han calculado los daños derivados de los ciberataques, basándose sólo los incidentes ocurridos en los últimos 12 meses y evaluando la información de las pérdidas sufridas como resultado directo de los incidentes de seguridad. Uno de los componentes principales son los daños causados por el incidente en sí, como pérdidas derivadas de la fuga de datos críticos, continuidad de negocio y los costes asociados con la participación de especialistas para solventar el incidente; y que suponen la mayor parte de las pérdidas (alrededor de 431.000 euros). Por otro lado están los costes no planificados para prevenir ataques similares en el futuro, como el personal de contratación/formación, el hardware, el software y otros cambios de infraestructura (unos 69.000 euros) Los daños dependen de la zona geográfica en la que se ubique la empresa, los mayores se han asociado con incidentes sufridos en compañías que operan en América del Norte, con un promedio de 624.000 euros; seguidos de América del Sur, con 620.000 euros. En Europa Occidental se registró una media más baja, pero aún considerable, de las pérdidas derivadas de ciberataques, llegando a 478.000 euros.

Pymes

Los costes de un ataque en las pequeñas y medianas empresas es mucho más bajo que en las grandes compañías.La pérdida media de los incidentes de seguridad TI es de aproximadamente 38.000 euros. Alrededor de 28.000 euros derivados del incidente en sí, mientras que los restantes 10.000 provienen de otros gastos asociados.

Las mayores pérdidas generadas por ciberataques entre pequeñas y medianas empresas se registraron en compañías de Asia-Pacífico (73.000 euros). En segundo lugar fue en empresas de América del Norte, con unas pérdidas de 62.000 y las más bajas se detectaron en Rusia, con 16.000 euros de media. Según el estudio los ciberataques más destructivos y costosos podrían haberse evitado, ya que explotan agujeros de seguridad que las empresas podrían haber tapado antes de tener problemas.

Computerworld (03/07/2013)

Más información

Los ciberataques globales aumentaron un 38% en 2022

ueños y ágiles, mientras
resarial. Las
ciberdelincuentes.

obre las tendencias de

De

Esta

La ciberseguridad es el asunto que más preocupa a las empresas españolas

Más de la mitad de las empresas españolas ha sido víctima de un ciberataque (51%), con una media de 84 ataques a cada una de ellas. Esta realidad ha llevado a las empresas a colocar la ciberseguridad como el asunto que más les preocupa, con un 48% que le

LEV DOLGACHOV (EL PERIÓDICO)

PARA SUSCRIPTORES

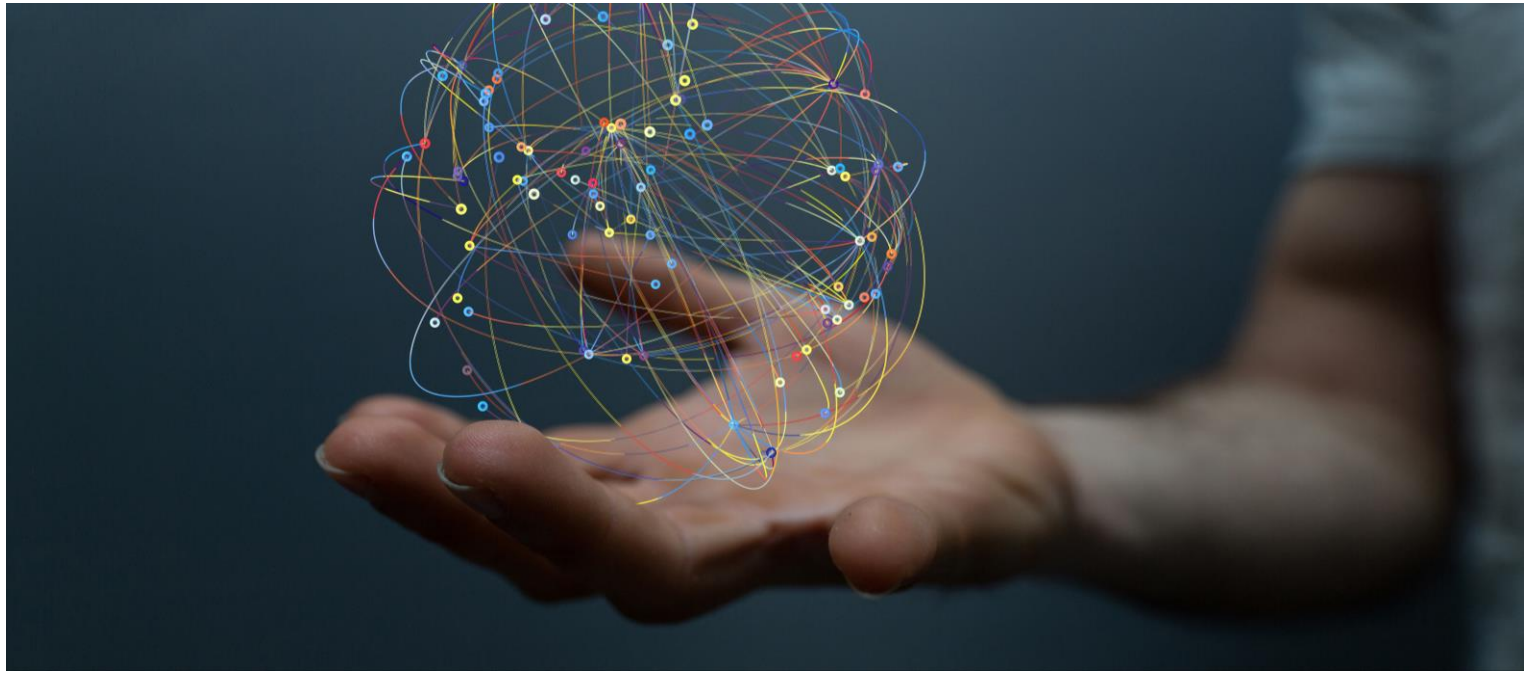
Impacto de la ciberseguridad para la sociedad y la economía

- **ENTORNO TOTALMENTE DIGITALIZADO**
  - Dependencia de los sistemas en el tejido empresarial. Todos conocemos los beneficios de la digitalización, pero no analizamos con detenimiento los riesgos de aplicarlo en nuestros negocios.

- **AUMENTO DE DIGITALIZACIÓN, SIN ADECUACIÓN EN LAS MEDIDAS DE CIBERSEGURIDAD**
  - Mientras la digitalización ha calado en el tejido empresarial, no han aumentado la ciberseguridad de forma equivalente.
- **AUMENTO DE LOS CIBERATAQUES EN MÁS DE UN 125% EN LOS ÚLTIMOS AÑOS**
  - 7/10 ciberataques son dirigidos a la pequeña y mediana empresa. 6/10 empresas atacadas cierran en los 6 meses posteriores a un ataque (INCIBE).

- **“La ciberseguridad no es una opción, es una necesidad crítica para la supervivencia empresarial.” Alejandro Cano 2024.**

El cibercrimen ha venido para quedarse



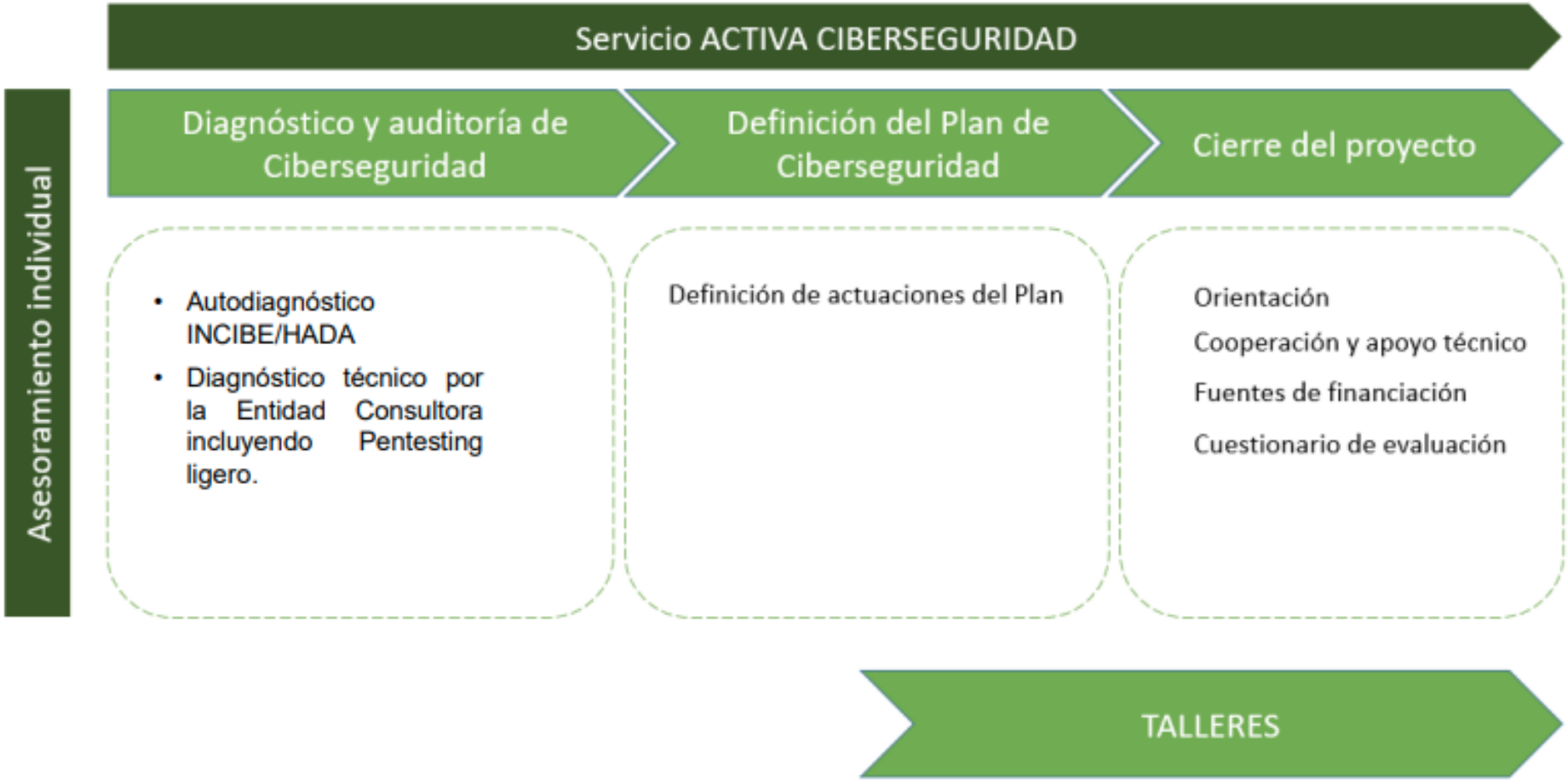
¿Por qué la Ciberseguridad es crucial para tu Empresa?

- **Protege tu negocio**: Resguarda tus datos, propiedades intelectuales, información de clientes…
- **Cumple con las regulaciones**: Evita sanciones legales y facilita contrataciones a los requisitos de administraciones públicas o clientes.
- **Reduce riesgos financieros**: Evita el coste de recuperarse de un incidente de ciberseguridad (mucho más voluminoso que invertir en defenderte).
- **Reduce daños reputacionales de tu organización**
- **Ventaja competitiva**: Valor diferencial frente la competencia, más oportunidades de mercado, acceso a clientes de mayor envergadura.

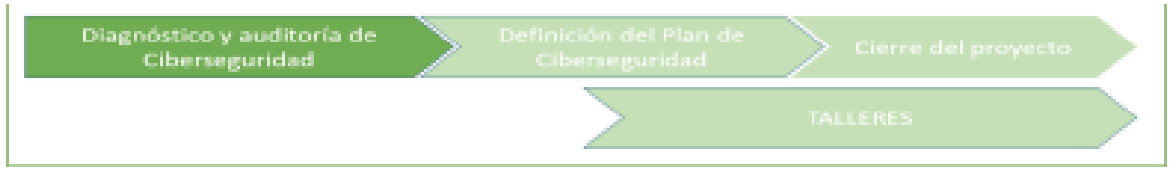
Una oportunidad única: Auditoría de ciberseguridad sin coste para tu negocio

- Asesoramiento personalizado para empresas con capacidad de mejora en acciones de ciberseguridad del cualquier sector de actividad
- OBJETIVO: Ofrecer un **análisis de la situación actual de la empresa en materia de Ciberseguridad** y elaboración de un **Plan de Ciberseguridad** específico para la misma con un diseño personalizado de acciones de mejora de ciberseguridad.
- Se trata de un programa impulsado por la SG de Industria y de la Pyme con la colaboración de EOI. Se realizará con la metodología desarrollada por la SGIPYME.
- **Diagnóstico e identificación de oportunidades de mejora**.
- Aprox. 20 horas dedicación a vuestro proyecto:
    - Un mínimo de dos reuniones, una de ellas será visita presencial.
    - Se podrán realizar otras reuniones si se considera oportuno.
    - Elaboración de informes y seguimiento en remoto
    - Taller grupal
- Programa gratuito para las PYMES beneficiarias.

FASES DEL PROGRAMA



FASES DEL PROGRAMA. Diagnóstico y auditoría



Auto Diagnóstico INCIBE / HADA

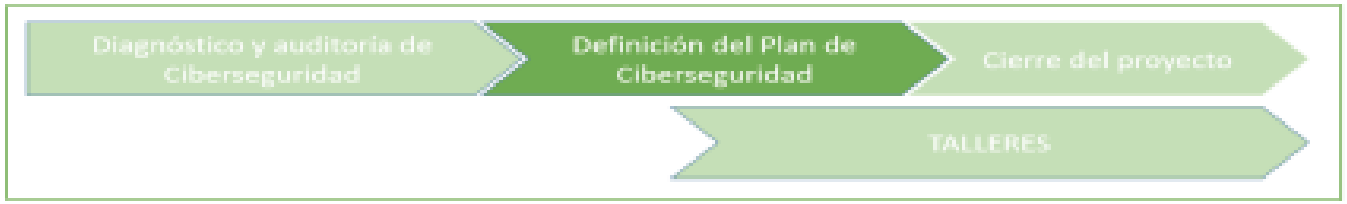
Primera aproximación de los riesgos a los que está sometida la organización, tomando conciencia del valor de sus activos de información, la importancia de tener controlados sus riesgos y la necesidad de iniciar un Plan de Ciberseguridad:

- Servicio de autodiagnóstico de INCIBE.
- Test de madurez digital de HADA (habilitador de ciberseguridad).

Diagnóstico (Consultor)

- Detección de las posibles vulnerabilidades y deficiencias de la organización en materia de ciberseguridad.
- Interpretación de los resultados del autodiagnóstico.
- Realización de un pentesting ligero de la web y los servicios públicos de la empresa.
- Propuesta de indicadores que sirvan para determinar las medidas que aseguren la protección de la información crítica de la empresa.

FASES DEL PROGRAMA. Definición del Plan de Ciberseguridad



Definición de actuaciones del Plan

- ✓ Elaboración de un plan que contemple, en forma de ficha, la relación de oportunidades y acciones detectadas con la siguiente información:
  - Información descriptiva
  - Información de evaluación y seguimiento
  - Información de impacto económico
- ✓ Presentación de las líneas generales del Plan de Ciberseguridad

FASES DEL PROGRAMA. Taller y Cierre del Servicio

Activa Ciberseguridad

Talleres demostrativos

- Taller grupal donde se expondrán de manera práctica las herramientas y soluciones que permitan impulsar y desarrollar mejoras en materia de Ciberseguridad.
- Los talleres se realizarán con las empresas asesoradas por la propia consultora en grupos de 25 a 50 empresas.
- Los talleres se realizarán en formato de videoconferencia online para garantizar la asistencia de empresas beneficiaras de distintos territorios.
- Los talleres deberán ser grabados para posteriores justificaciones.

Entregables en la Ejecución

Activa Ciberseguridad

Relación de los entregables que se generarán en la PLATAFORMA DE GESTIÓN durante la ejecución del proyecto. Deberán ser subidos a la plataforma y validados por la empresa beneficiaria en cada fase:

FASE METODOLÓGICA	NOMBRE ENTREGABLE	ENTREGA Y VALIDACIÓN POR PARTE DE LA EMPRESA
Fase de Diagnóstico	Informe de Diagnóstico	✓
Fase de definición del Plan de Ciberseguridad	Informe del Plan de Ciberseguridad	✓
Fase de Cierre del servicio	Informe de cierre	✓

Una vez finalizado el servicio la plataforma de gestión emitirá un Comprobante de las actividades desarrolladas, que deberá ser firmado por entidad consultora y empresa beneficiaria y deberá entregarse en la justificación de la ayuda.

Activa Ciberseguridad

Muchas Gracias

¿Alguna duda?

Contacto:
acano@legitec.com

legitec CIBERSEGURIDAD

Financiado por la Unión Europea NextGenerationEU

Plan de Recuperación, Transformación y Resiliencia

EOI Escuela de organización industrial