CSTIC 2018

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

El Seguro de Ciber Riesgos

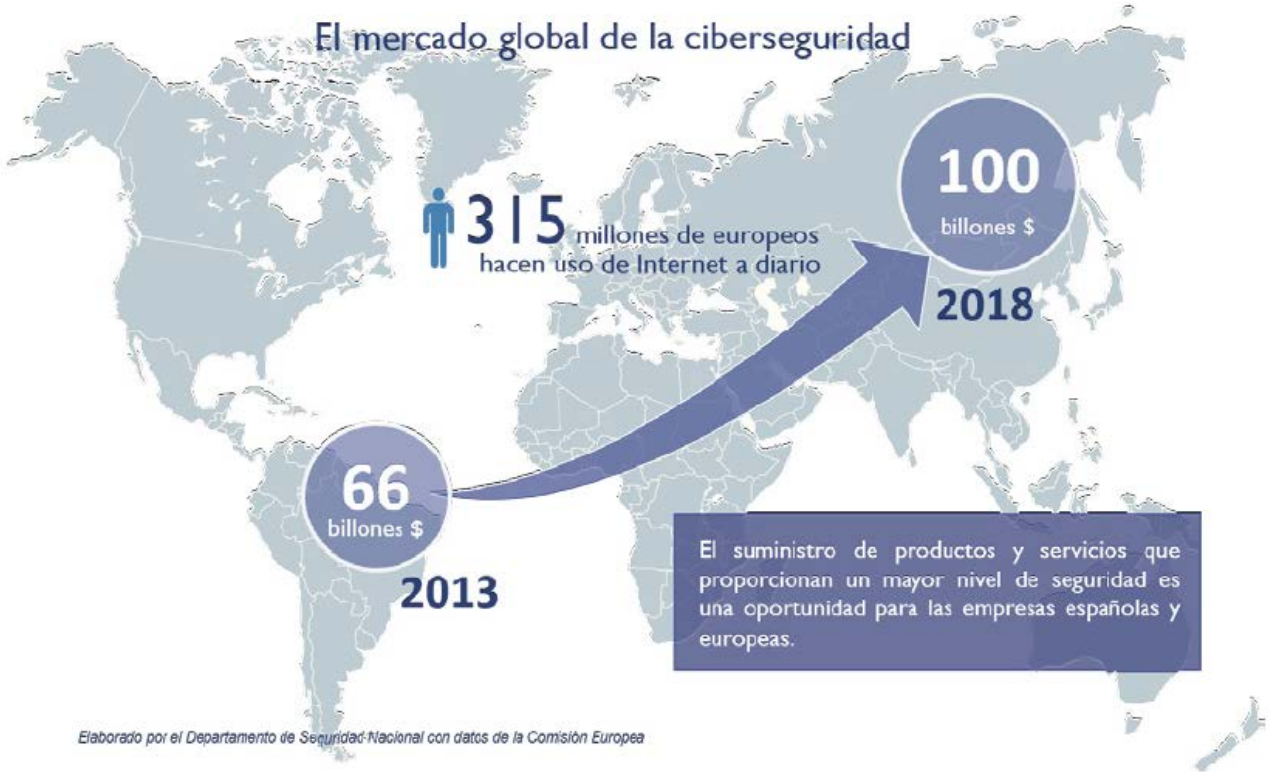
Las personas ya no sólo piensan en proteger objetos, sino también el estilo de vida

Manuel Huerta, CEO

Lazarus

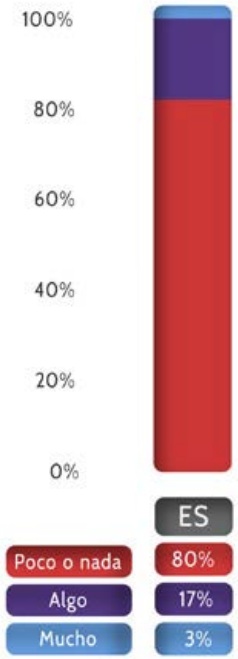
Lazarus Technology

El ADN de Lazarus es la tecnología, nuestro I+D se basa en el estudio en profundidad del entorno tecnológico de las personas, los negocios y la sociedad, el análisis de los riesgos, la prevención de los mismos y la remediación en caso de incidente.


El mercado global de la ciberseguridad
315 millones de europeos hacen uso de Internet a diario
100 billones $
2018
66 billones $
2013
El suministro de productos y servicios que proporcionan un mayor nivel de seguridad es una oportunidad para las empresas españolas y europeas.
Elaborado por el Departamento de Seguridad Nacional con datos de la Comisión Europea

Ciber Riesgos

Grado de Concienciación de las empresas



Fuente: CCN CERT

Hoy en día ya no es una cuestión de si las Ciber amenazas pueden o no afectar a una empresa con independencia de su tamaño, sector o ubicación, la pregunta a realizarse es simplemente, ¿cuándo sucederá? y si la organización contará con los mecanismos adecuados para afrontar el incidente.

El concepto Ciber Riesgo reúne una combinación de riesgos que pueden causar daños materiales, pérdidas, daños en intangibles (datos, información, sitios webs, propiedad intelectual, patentes, nombres de dominios,...) y daños a terceros en los que entra en juego la responsabilidad civil e incluso penal.

GDPR

El nuevo Reglamento General de Protección de Datos (GDPR, en inglés) plantea a las empresas de la UE una revisión de su política de procesamiento de datos.

Es un tema muy vinculado a la Ciberseguridad y a la definición de políticas de seguridad.

La puesta en marcha de GDPR supondrá entre otras operativas:

Auditar el estado de las redes para aumentar su protección
Detectar vulnerabilidades
Implantar o revisar soluciones de cifrado
Identificar y monitorizar dispositivos, aplicaciones y contenidos, tanto en entornos físicos, como de movilidad y en la Nube.

El objetivo es evitar ciberataques y proteger los datos personales además de evitar las penalizaciones que contempla la nueva regulación.

GDPR	Multas administrativas:	Si se trata de una empresa:
Sanción	10 millones €	2% del VNTAG *
Sanción Reincidencia	20 millones e	4% del VNTAG *

** VNTAG = Volumen de Negocio Total Anual Global*

CST

PYMES

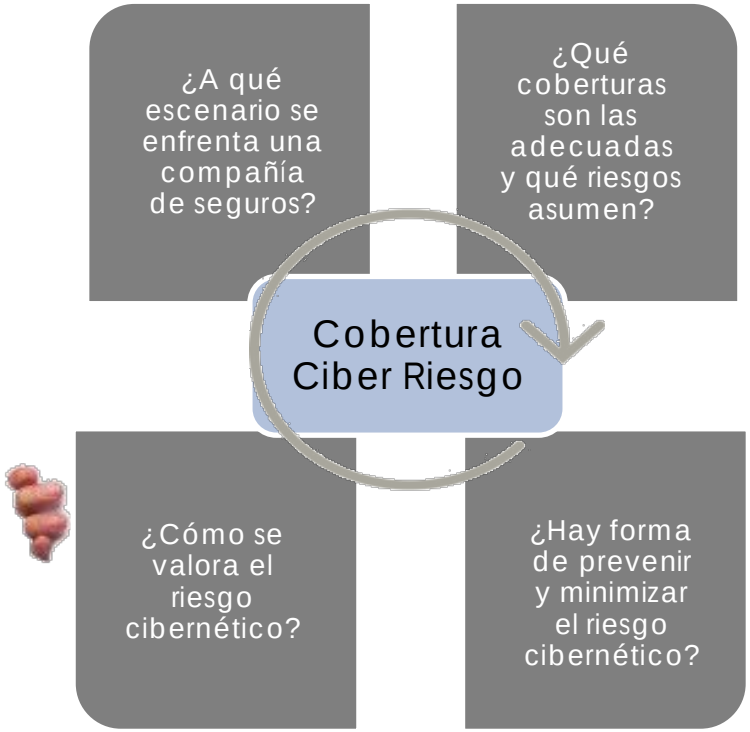
Porqué son susceptibles las PYMES de recibir ataque cibernéticos?

- Usan la tecnología en sus negocios
- Utilizan smartphones, portátiles... (BOYD)
- Aumenta el almacenamiento de datos (propio y nube)
- Comparten información con clientes y proveedores
- Tienen comercio electrónico
- Medios de pago
- Tiene empleados

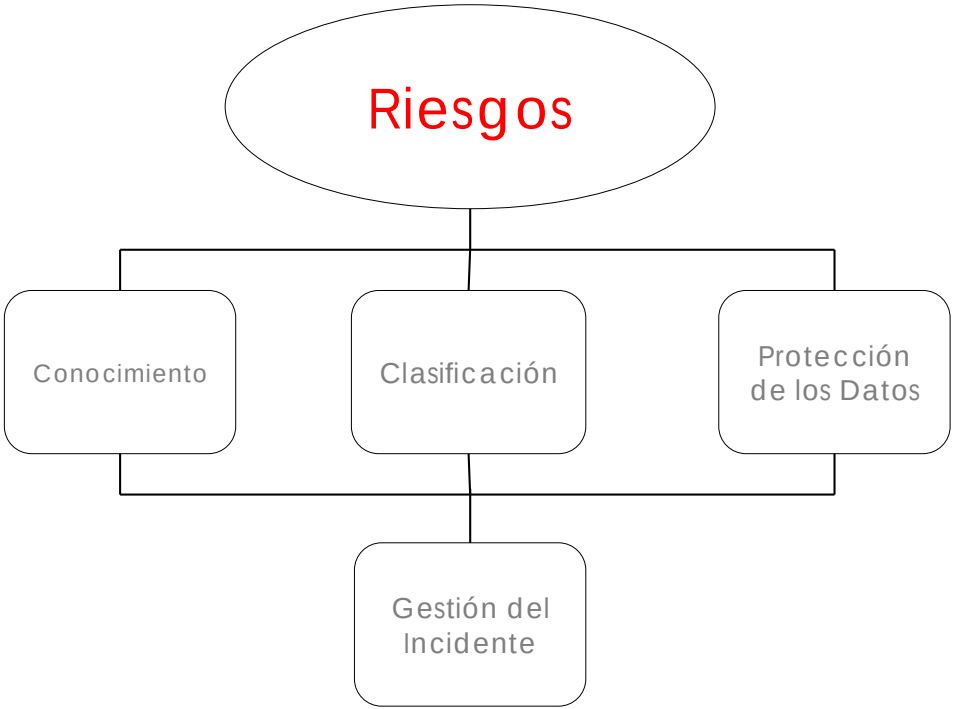
Porqué son más vulnerables?

- Desconocimiento de la amenazas
- Solo el 40% de las empresas disponen de infraestructuras digitales correctamente garantizadas.
- Acceso a grandes corporaciones
- Un 70% de los ataques se dirige contra compañías de menos de 100 empleados.

El escenario



El sector asegurador **necesita expertos** en la gestión del riesgo tecnológico



Minimización del impacto
Histórico
Cálculo Actuarial

Análisis e identificación del Siniestro

El siniestro cibernético es producido por un acto malintencionado, que afecta a la información y al funcionamiento de la empresa o a terceros.

Delimitar origen, causa, efecto y responsabilidad, es completamente inviable sin una investigación tecnológica.

Tipos de Daños

Lucro Cesante
Daños a la imagen
Perdida de competitividad
Sanciones
Reclamaciones de terceros
Responsabilidad civil
Responsabilidad penal

Buenas Prácticas

Una Cobertura Ciber Riesgos, debería cumplir con los requisitos necesarios para que una empresa pueda **proteger sus sistemas ante riesgos cibernéticos**.

Conocer el estado de sus sistemas y realizar un **análisis de las posibles vulnerabilidades** existentes.

Corregir las vulnerabilidades.

Dotarse de las herramientas específicas de detección y protección contra el Ransomware y otros tipos de malware.

Disponer de una política de buenas prácticas y Formar a su personal.

Además debe incluir un **conjunto de actuaciones dirigidas a la prevención y contención de los riesgos**, además de disponer de todos los procedimientos de actuación en caso de producirse algún incidente, tanto en la peritación como en la remediación y puesta en marcha.

Esquema
Solución
Aseguradora

Normalización del riesgo asegurado.

Herramienta Prevención Lazarus BestSafe

- Análisis Vulnerabilidades Externas/internas/web
- Check list Seguridad y Buenas Prácticas
- Política Back Up
- Evaluación y Cumplimiento
- Presencia en Internet

Incident Response

Análisis Vulnerabilidades — **Corrección y políticas** — **Lazarus BestSafe** — **Cesión de Riesgo** — **Incident response**

Servicios y Coberturas Ciber Seguro

SERVICIOS

- Gestión de Crisis
- Servicios Preventivos Normalización

COBERTURAS

- Incidentes Internos
- RC de Privacidad, Comunic. y Seguridad
- Pérdidas Económicas
- Gastos defensa Normativa y multas
- Cyber Extorsión
- Daños Reputacionales

Claves

Cualquier empresa puede ser atacada (no importa el tamaño).

La PYME es un objetivo como cualquier otro. Olvidarse del “a mi no me va a pasar”

Poner a disposición de la empresa elementos preventivos y aplicar buenas prácticas.

Obligación de cumplir con la normativa.

La industria aseguradora necesita expertos en riesgos cibernéticos.

Un buen producto asegurador debe garantizar la continuidad de los negocios en caso de incidente.

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

LazaRus
clínica de datos

C/ Teide 5, 3ª Planta
Edificio Milenio
San Sebastián de los Reyes,
28700 (Madrid)
España
+34 91 658 64 16
info@lazarus.es

bsi. ISO 9001 Gestión de la Calidad
bsi. ISO/IEC 27001 Seguridad de la Información

06/06/2018