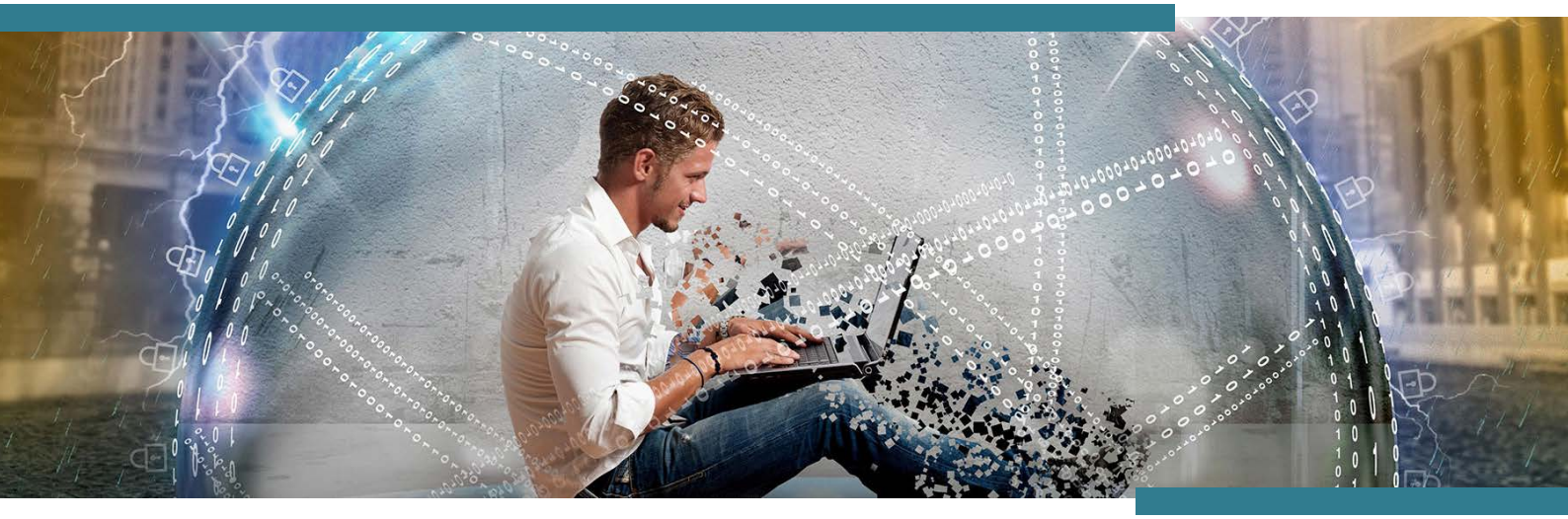
ESTRATEGIA DE CIBERSEGURIDAD 360º



"Hay únicamente dos tipos de compañías: aquellas que ya han sufrido ciberataques y aquellas que los sufrirán. Incluso esa división está fusionándose en una sola categoría: aquellas compañías que ya han sido 'hackeadas' y que volverán a serlo". Robert Mueller III. 6º Director del FBI (2001 - 2013)

¿Está preparado para lo inevitable?

Hoy ya no es realista preguntarse si su compañía sufrirá o no un incidente de ciberseguridad. La pregunta es cuándo y cómo ocurrirá.

La forma en que su compañía enfrente ese incidente tan transcendental para su cuenta de resultados, patrimonio, reputación y, en definitiva, su futuro, dependerá enteramente de hasta qué punto haya implantado un programa de prevención de incidentes de ciberseguridad apropiado y completo, es decir, un **plan de prevención integral** o de **360º**.

3 condiciones para una ciberseguridad total

Un enfoque de la ciberseguridad desde la perspectiva del daño y el riesgo, permite apreciar tres facetas o, si se quiere, **tres condiciones que deben darse para que una compañía pueda considerarse que está realmente "cibersegura":**

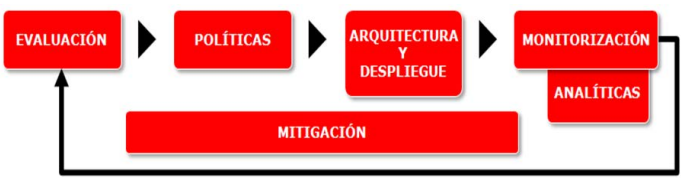
1. La **condición técnica:** la empresa debe asegurarse de que sus infraestructuras IT críticas, es decir, aquellas que gestionan los principales activos de información de la empresa, cuentan con elementos técnicos que impiden accesos no autorizados, pérdidas de información o caídas del servicio.

2. La **condición legal:** es necesario que la empresa se asegure también de que el marco jurídico y contractual que rige tales infraestructuras IT críticas, establece mecanismos legales para prevenir el incidente de ciberseguridad y mitigar, o en su caso eliminar, el daño que la empresa puede sufrir en caso de que un incidente ocurra, bien provenga tal daño de responsabilidades contractuales, sanciones, perjuicio en la reputación,...

3. La **condición de cobertura:** la empresa debe contar con una adecuada política de transferencia del riesgo asociado al incidente de ciberseguridad y con pólizas de seguro correctamente diseñadas para dar cobertura a este tipo de siniestros tan particulares.

Condición técnica con SOGETI

Cuando los riesgos no pueden ser asumidos ni transferidos, es preciso controlarlos y mitigarlos. El ciclo de la seguridad que propone **Sogeti** entra dentro de un modelo sistémico de ciberseguridad que permite una mejora continua tanto en el control y mitigación de los riesgos como en el avance de la seguridad en los procesos de negocio.



En este contexto, **Sogeti**:

1. **Evalúa** el estado de la protección de los activos mediante técnicas como auditorías de seguridad y pruebas de penetración.

2. Propone aquellas modificaciones en las **políticas** de protección de seguridad de la compañía que sean precisas a la luz de los resultados de la evaluación.

3. Implanta las mejoras en la **arquitectura** que puedan ser requeridas para un mejor gobierno y un mayor control y capacidad de actuar frente a cualquier incremento de riesgo.

4. **Monitoriza**, a través de su Centro de Operaciones de Seguridad (SOC), el estado de las circunstancias de las que depende el riesgo y extrae **analíticas** que muestran la eficacia de las medidas tomadas frente a los ataques a los que la organización está expuesta. Finalmente, **mitiga** los riesgos descubiertos mediante acciones que precisan una nueva evaluación.

Junto a ello, **Sogeti** realiza planes de **formación y concienciación** a directivos y empleados, y acciones de **continuidad del negocio** que cierran el círculo de la ciberseguridad.

Condición legal con Hogan Lovells

Los abogados de **Hogan Lovells** especialistas en ciberseguridad, le ayudan a construir su "escudodefensivo" mediante el análisis del marco regulador que rige a sus infraestructuras IT y la identificacion y solución de vulnerabilidades legales que expongan a su empresa a daños y responsabilidades. Ello se logra a través de una metodología probada que se basa en las siguientes **etapas**:

1. Identificación de **activos intangibles estratégicos** (datos de clientes, diseños, programas, invenciones, etc.) e **infraestructuras TIC críticas** (servidores, proveedores, redes de comunicación, etc.) de la compañía.

2. Determinación del **marco regulador** (contratos con clientes, proveedores y empleados, leyes, códigos de autorregulación, políticas internas) de las infraestructuras TIC críticas.

3. Identificación de **vulnerabilidades** respecto del marco regulador de las infraestructuras TIC críticas (obligaciones indeterminadas, responsabilidad poco clara o insuficiente, posibles incumplimientos legales, etc.) y plan de acciones.

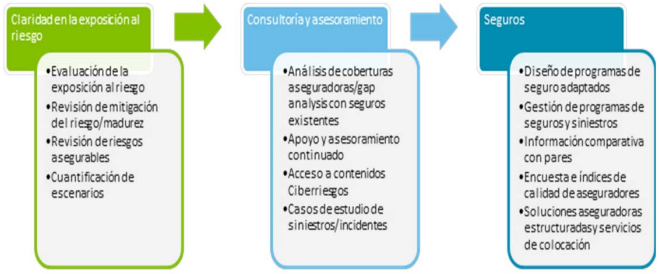
4. Solución de vulnerabilidades y ejecución del **plan de acciones** que cree un **"escudo defensivo"** (renegociación de contrato, desarrollo de políticas, planes de formación, etc.).

Hogan Lovells está también preparado para enfrentar los aspectos legales de cualquier incidente legal que se materialice, tales como inspecciones, acciones legales, etc.

Condición de cobertura con AON Empower Results®

Las organizaciones no pueden prescindir de aplicar los avances tecnológicos a su negocio y necesitan, por tanto, comenzar a integrar los nuevos escenarios de riesgos dentro de sus políticas de gestión. Una herramienta fundamental dentro de la gestión de riesgos es su transferencia a través de soluciones aseguradoras. Sin embargo, cada empresa es única en su enfoque frente al riesgo y las soluciones aseguradoras deben estar ajustadas a esta realidad. No vale la misma póliza de seguros para todas las empresas.

Mediante la propuesta **Cyber Clarity Process**, **Aon** puede ayudarle a identificar y cuantificar los riesgos derivados de sistemas y de la información, y poner en marcha las medidas de mitigación más efectiva, mediante una metodología de gestión integral de riesgo que abarca:



1. El **análisis** en cuanto a qué amenazas tienen mayor probabilidad de materializarse, cuál puede ser el impacto económico en caso de materialización.

2. La determinación de la **política de transferencia de estos riesgos.**

3. Mediante la **selección y diseño del producto asegurador** que se ajuste a las necesidades de cobertura de su organización.

Durante el proceso de transferencia, **Aon** puede ayudarles a distinguir entre los productos de cada aseguradora y a diseñar el seguro más adecuado a sus necesidades, además de apoyarles durante la vida del seguro y la gestión de siniestros.

Juan Carlos Pascual
Security Lead- Sogeti
jc.pascual@sogeti.com
Tlf. +34 91 308 44 33
www.sogeti.es

Gonzalo F. Gállego Higueras
Socio - IPMT - Hogan Lovells
gonzalo.gallego@hoganlovells.com
Tlf. +34 91 3498200
www.hoganlovells.com

Claudia Gómez
Director de Ciberriesgos - Aon Risk
claudiabeatriz.gomez@aon.es
Tlf +34 91 340 46 45
www.aon.com/spain