ISACA®
Trust in, and value from, information systems
Barcelona Chapter

Oportunidades, ventajas y retos que ofrece el nuevo Reglamento General de Protección de Datos (GDPR)

Rosa Ortuño y Victoria Tabar
OptimumTIC para ISACA

7 de noviembre de 2017, Barcelona

OptimumTIC
OPTIMIZACIÓN DE PROCESOS Y SISTEMAS

OptimumTIC

OptimumTIC se crea a finales del 2009 ofreciendo servicios y productos del ámbito de la **seguridad de la Información, Auditorias de Sistemas y Planes de Adaptación en la Protección de datos, especializándonos en Ciberseguridad (prevención y mitigación de riesgos)**.

Desde nuestros inicios, trabajamos a partir de la revisión de procesos, optimizándolos y aportando mejora continua, y aplicamos **herramientas tecnológicas** que facilitan la salvaguarda y la integridad de los datos. **Adaptamos toda la parte documental y organizativa, en base a la identificación,** a tales medidas de seguridad con el objetivo de garantizar la confidencialidad, integridad y seguridad global de los activos de información de la empresa o la organización.

Además, nos aplicamos como **expertos para las compañías en soporte y en conocimiento**, ofreciendo **revisión y asesoramiento contractual**, tanto en negociaciones y procesos de negocio como en la implantación de herramientas (softwares, etc.), partiendo siempre del cumplimiento LOPD/RGPD y de la seguridad de la información (SGSI- ISO 27002).

Nuestro equipo propio, está especialmente preparado para todos los escenarios de cualquier organización, ya sea de carácter técnico, legislativo, forense o documental.

Nuestro objetivo en todos los proyectos que realizamos es **aportar valor y soluciones efectivas a nuestros clientes**, adaptándonos a su organización y trabajando siempre desde los más altos estándares de metodología, calidad, compromiso y seguridad en todos los ámbitos.

Equipo OptimumTIC

En OptimumTIC contamos con un equipo multidisciplinar propio, preparado y con experiencia en diferentes escenarios, niveles y ámbitos de actuación y de negocio, y con el objetivo de trabajar siempre desde la seguridad, la adaptabilidad y la calidad.

ESPECIALISTA SENIOR EN ESTRATEGIA Y SEGURIDAD DE LA INFORMACION

- Auditora de sistemas de Información y activos de la información, especializada en Gestión de Seguridad (SGSI- ISO 27001), Dirección y realización de Plan Director y Estrategia de los Departamentos de la Información, Organización y Tecnologías. Responsable de Seguridad en distintos Negocios y sectores.

ABOGADOS/AS ESPECIALISTAS EN DERECHO INTERNACIONAL

- Abogados/as con conocimientos y experiencia en Derecho Internacional, Tecnologías de la Información y la Comunicación y Protección de datos de Carácter Personal.
- Abogados/as especialistas en revisión y gestión contractual y elaboración de Marco Normativo de Protección de datos conforme estándares ISO 27001, RGPD y otras normativas aplicables.

TÉCNICOS/AS DE SEGURIDAD

- Técnicos/as de seguridad especializados en herramientas de seguridad, tratamiento, comunicación y seguridad de la información informatizada de última generación
- Técnicos/as de seguridad especializados en la implementación de herramientas de organización y optimización empresarial.
- Técnicos de la información especializados en Sistemas de Gestión de la Seguridad y su implementación (SGSI – ISO 27001)

CRIMINÓLOGOS/AS ESPECIALISTAS EN CIBERSEGURIDAD

- Criminólogos/as especializados en delitos informáticos, Ciberseguridad y Protección de datos de Carácter Personal.
- Criminólogos/as especializados en elaboración de Marco Normativo en Protección de datos y análisis de procedimientos en este ámbito conforme estándares ISO 27001

Nuevo contexto tecnológico

Los delitos en la red suponen *1 billón de euros al año a nivel mundial*

Los gastos en seguridad digital *70.000 millones*

CIBERDELINCUENCIA
La transformación digital traslada los delitos a la red

ORGANIZATIVA

LEGAL

TÉCNICA

CIBERSEGURIDAD
Garantizar la seguridad de la información en el ciber entorno

- BREAKING NEWS -

El spam, un vehículo clave para la ciberdelincuencia

El exploit detrás de WannaCry ahora está siendo usado para robar datos a través de redes WiFi de hoteles en Europa

PETYA: EL ATAQUE DE UN VIRUS AÚN MÁS LETAL QUE WANNACRY

5% DEL PIB MUNDIAL

El robo de los secretos comerciales causa pérdidas de 3 billones de euros

La sustracción de información valiosa se dispara un 60% en un año

El 90% de los ciberataques más graves en España procede de otros Gobiernos

La UE aprueba la ley de protección de datos, bloqueada desde 2013

Se buscan 350.000 expertos en ciberseguridad

El ciberataque con el virus WannaCry se extiende a nivel mundial

Los ciberataques han aumentado un 130% en el 2016

USOS DOMÉSTICOS

APLICACIONES LABORALES E INDUSTRIALES

Internet Of Things

ELECTRODOMÉSTICOS INTELIGENTES

EDIFICIOS Y CIUDADES CONECTADAS

SALUD Y BIENESTAR

CIBERSEGURIDAD

La firma Equifax reconoce un ciberataque que afecta a 143 millones de personas

La empresa estadounidense de información sobre solvencia crediticia admite también que los piratas cibernéticos accedieron a números de tarjetas de crédito de cerca de 209.000 consumidores

http://www.lavanguardia.com/internacional/20170908/431126253240/equifax-reconoce-ciberataque-afecta-143-millones-personas.html

“Tu cara es Big Data”: El fotógrafo ruso utiliza el reconocimiento facial para encontrar a la gente que ha fotografiado en el metro

http://blog.consultaeducation.com/2016/12/13/cara-big-data-fotografo-ruso-utiliza-reconocimiento-facial-encontrar-la-gente-ha-fotografiado-metro/

Con ‘V’ de Big Data

Para definir la nueva deidad informática, los expertos emplean las llamadas “tres Vs”: volumen, velocidad y variedad

Los bancos han empezado a utilizar datos sociales para decidir a quién ofrecen o conceden un crédito

CIBERSEGURIDAD Y NORMATIVA

ISO 27001

Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande.

ISO 27001

Adaptar la compañía al marco ISO 27001, a partir de la aplicación de sus controles, contribuye a:

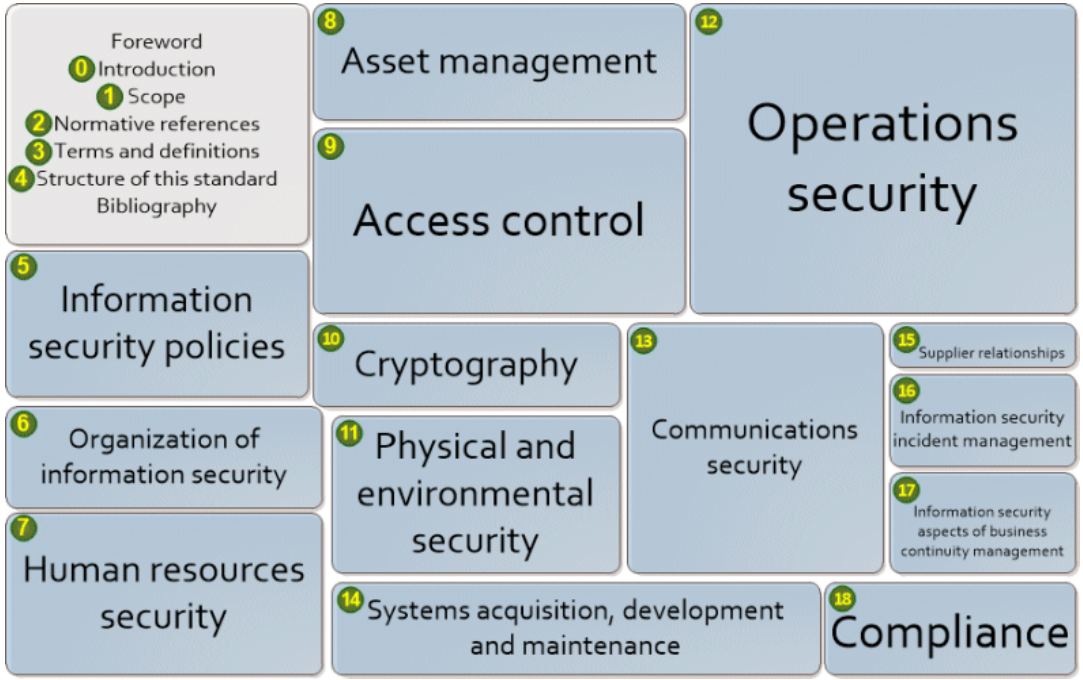
- Abarcar un espectro más amplio de la seguridad
- Adoptar medidas de seguridad estándar
- Elaborar medidas y procedimientos de seguridad transversales a la organización
- Acercarse un paso más al Compliance

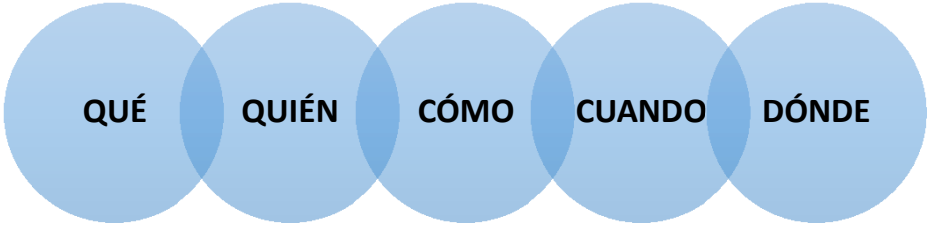
Clasificación	Título del Documento
A - Política de Seguridad	Política Corporativa de Seguridad de la Información
B - Gestión de la Seguridad de la Información	Norma de Roles y Responsabilidades de Seguridad de la Información
	Norma del Sistema de Gestión de la Seguridad de la Información
	Norma de Auditoría de los Sistemas de Información
	Norma de Gestión de Registros de los Sistemas de Información
	Norma de Informática Forense
	Norma de Análisis y Gestión de Riesgos
	Norma de Gestión de los Planes de Recuperación de Desastres
	Norma de Gestión de No Conformidades
C - Clasificación y Control de activos	Norma de Clasificación y Gestión de la Información
	Norma de Inventario de Activos
D - Seguridad ligada a las personas	Normativa de Gestión del Personal Interno
	Norma de Gestión de Prestadores de Servicios Externos
E - Seguridad Física y del Entorno	Norma de Protección Física y del Entorno
F - Seguridad Operativa	Norma de Uso de los Sistemas de Información
	Norma de Identificación, Autenticación y Control de Accesos
	Norma de Gestión de Incidentes
	Norma de Gestión de Cambios
	Norma de Desarrollos Seguros
	Norma de Gestión de Dispositivos Portátiles
	Norma de Gestión de Copias de Respaldo
	Norma de Protección contra código malicioso y correo no deseado
	Norma de Seguridad en el Correo Electrónico
	Norma de Seguridad en Redes y Comunicaciones
G - Conformidad y Cumplimiento	Norma de Requisitos Legales y Otros Requerimientos TIC
H - Mapeo con ISO 27001	Declaración de Aplicabilidad

ISO 27001

El marco ISO 27001 proporciona una referencia para la seguridad de la información en general,

Y en ella se integra la PROTECCIÓN DE DATOS PERSONALES.





ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/Controles/ISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
- **5.1 Política de seguridad de la información.**
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- **6.1 Organización interna.**
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- **6.2 Terceros.**
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- **7.1 Responsabilidad sobre los activos.**
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- **7.2 Clasificación de la información.**
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- **8.1 Antes del empleo.**
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- **8.2 Durante el empleo.**
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- **8.3 Cese del empleo o cambio de puesto de trabajo.**
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- **9.1 Áreas seguras.**
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- **9.2 Seguridad de los equipos.**
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- **10.1 Responsabilidades y procedimientos de operación.**
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- **10.2 Gestión de la provisión de servicios por terceros.**
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- **10.3 Planificación y aceptación del sistema.**
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- **10.4 Protección contra el código malicioso y descargable.**
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- **10.5 Copias de seguridad.**
  - 10.5.1 Copias de seguridad de la información.
- **10.6 Gestión de la seguridad de las redes.**
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- **10.7 Manipulación de los soportes.**
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- **10.8 Intercambio de información.**
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- **10.9 Servicios de comercio electrónico.**
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- **10.10 Supervisión.**
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- **11.1 Requisitos de negocio para el control de acceso.**
  - 11.1.1 Política de control de acceso.
- **11.2 Gestión de acceso de usuario.**
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- **11.3 Responsabilidades de usuario.**
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- **11.4 Control de acceso a la red.**
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- **11.5 Control de acceso al sistema operativo.**
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- **11.6 Control de acceso a las aplicaciones y a la información.**
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- **11.7 Ordenadores portátiles y teletrabajo.**
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- **12.1 Requisitos de seguridad de los sistemas de información.**
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- **12.2 Tratamiento correcto de las aplicaciones.**
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- **12.3 Controles criptográficos.**
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- **12.4 Seguridad de los archivos de sistema.**
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- **12.5 Seguridad en los procesos de desarrollo y soporte.**
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- **12.6 Gestión de la vulnerabilidad técnica.**
  - 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- **13.1 Notificación de eventos y puntos débiles de seguridad de la información.**
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- **13.2 Gestión de incidentes y mejoras de seguridad de la información.**
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- **14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- **15.1 Cumplimiento de los requisitos legales.**
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- **15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- **15.3 Consideraciones sobre las auditorías de los sistem. de información.**
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

www.iso27002.es

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

Definir Plan de Seguridad

Para empezar, debemos identificar qué tipo de datos trata la empresa y qué tratamientos necesita:

- ¿Trata algún dato relativo a la salud, la ideología, rasgos psicológicos u otra categoría que requiera un nivel medio o sensible?
- ¿Trata datos de clientes? ¿Y de empleados?
- ¿Realiza transferencias de datos con otras empresas u organizaciones?
- ¿Dónde almacena los datos? ¿Servicio externo o servidor propio?
- ¿Qué medidas de seguridad hay para proteger las bases de datos? ¿Antivirus, Firewall, etc.?
- ¿Dispone de algún sistema que permita crear roles de usuario y accesos personalizados?

Todas estas preguntas, junto con otra, relativas al ámbito legal, organizativo y técnico, nos ayudarán a crear un mapa de la situación actual de la organización en relación al cumplimiento de la protección de datos, y se podrá configurar un plan de enfoque y actuación sobre la prevención y seguridad, qué importancia y recursos vamos a otorgarle, y como va a gestionarse.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Nueva legislación a **nivel europeo** que reúne y unifica las distintas medidas y normativas europeas en el tratamiento de datos.

MAYO 2016: publicación oficial de la normativa GDPR.

MAYO 2018: obligado cumplimiento

El GDPR **no deroga la LOPD** sino que la obliga a renovarse y/o a modificar aquellos puntos no compatibles con el GDPR

- **todos los países miembro** de la Comunidad Europea,
- **empresas instaladas en países miembro** con sedes fuera de la Comunidad Europea y
- empresas instaladas fuera de la Comunidad Europea que traten **datos personales de ciudadanos residentes** en ella.

PRINCIPIOS Y BASES DEL RGPD

Principio de responsabilidad proactiva

Art. 5

Protección de datos *by design* & *by default*

Art. 25

Principio de transparencia

Art. 5

Delegado de Protección de Datos

Art. 37

Avaluaciones de Impacto en la Privacidad (PIA)

Art. 35

Comunicar incidencias seguridad

Art. 33

Aumento de las sanciones

Art. 84

Nuevos derechos para los usuarios

Art. 17, 20

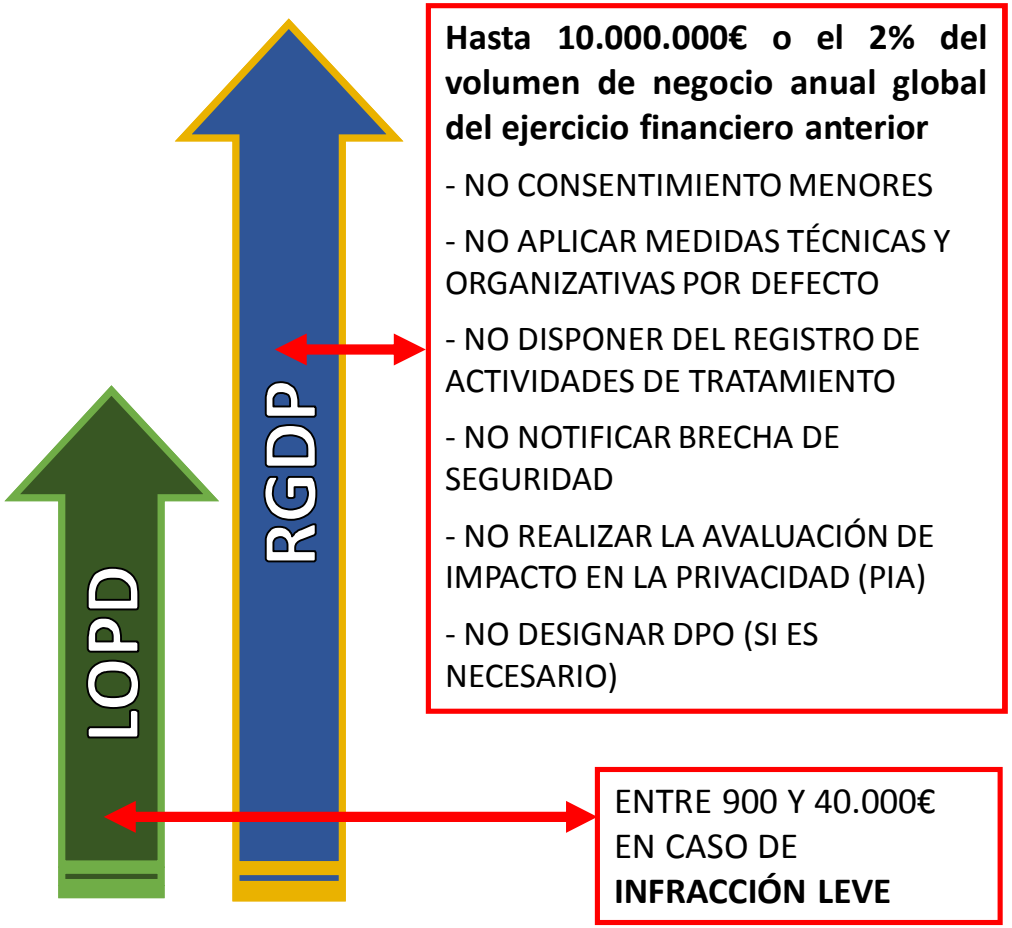
Regulación consentimiento recogida y tratamiento

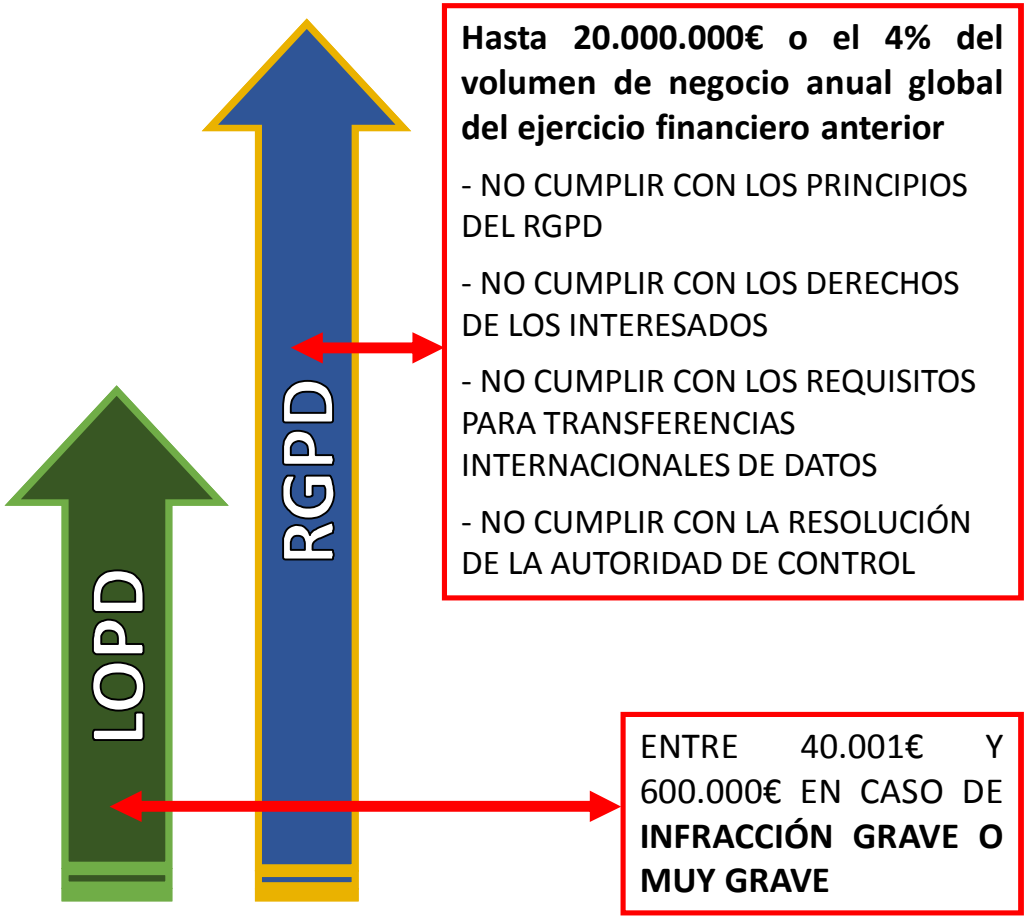
Art. 6,7

Garantías transferencias internacionales

Considerando 110 RGPD

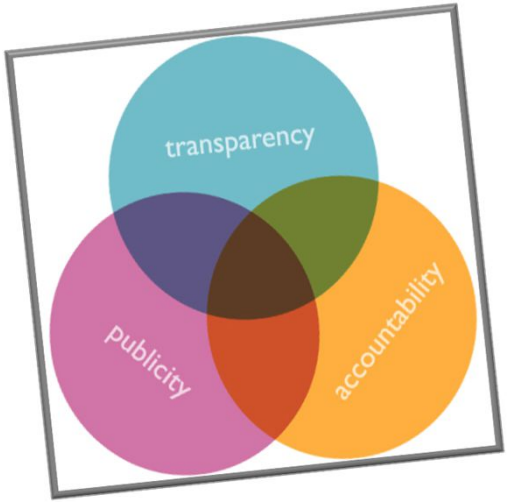
INFRACCIONES Y SANCIONES

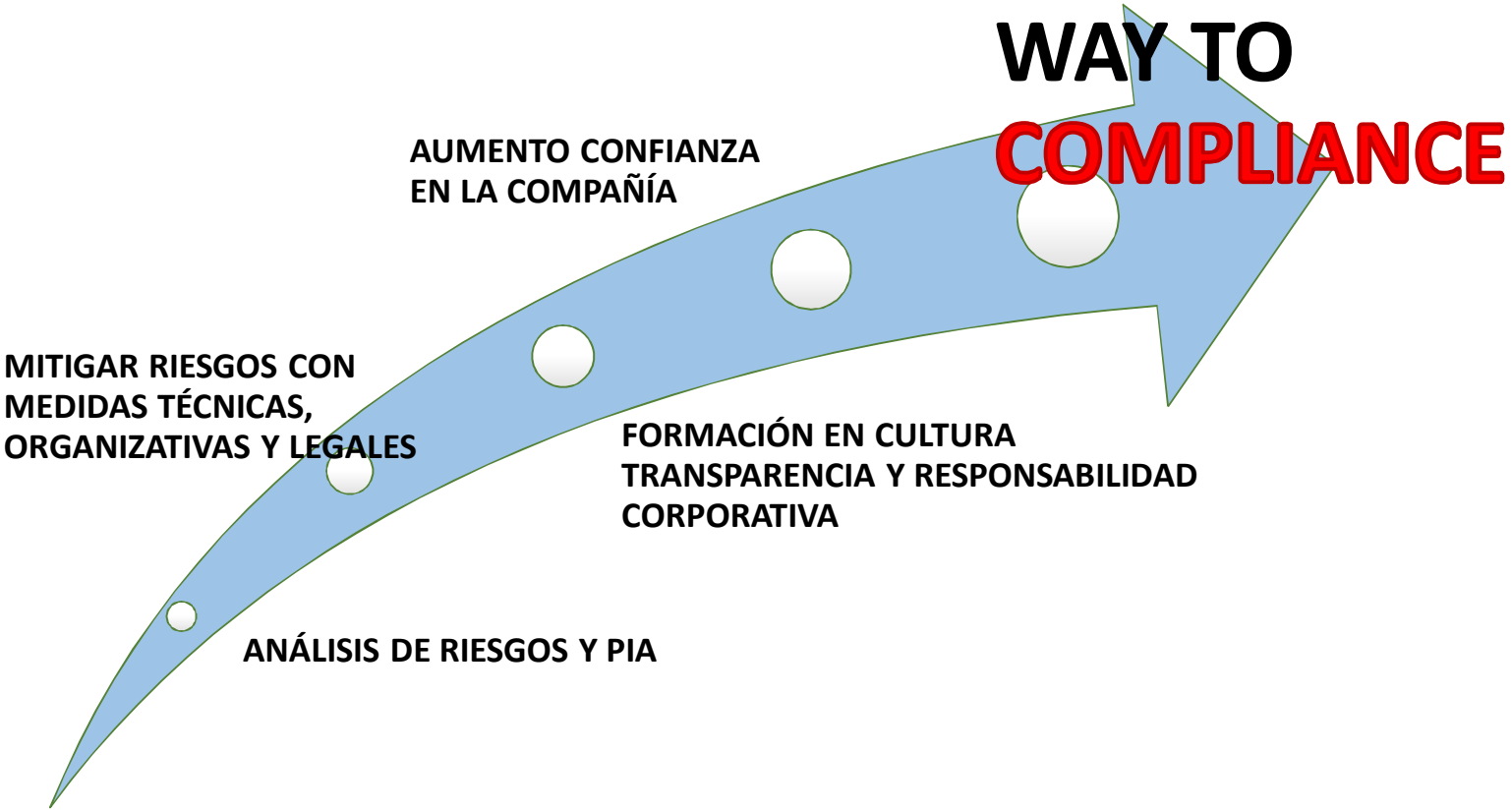




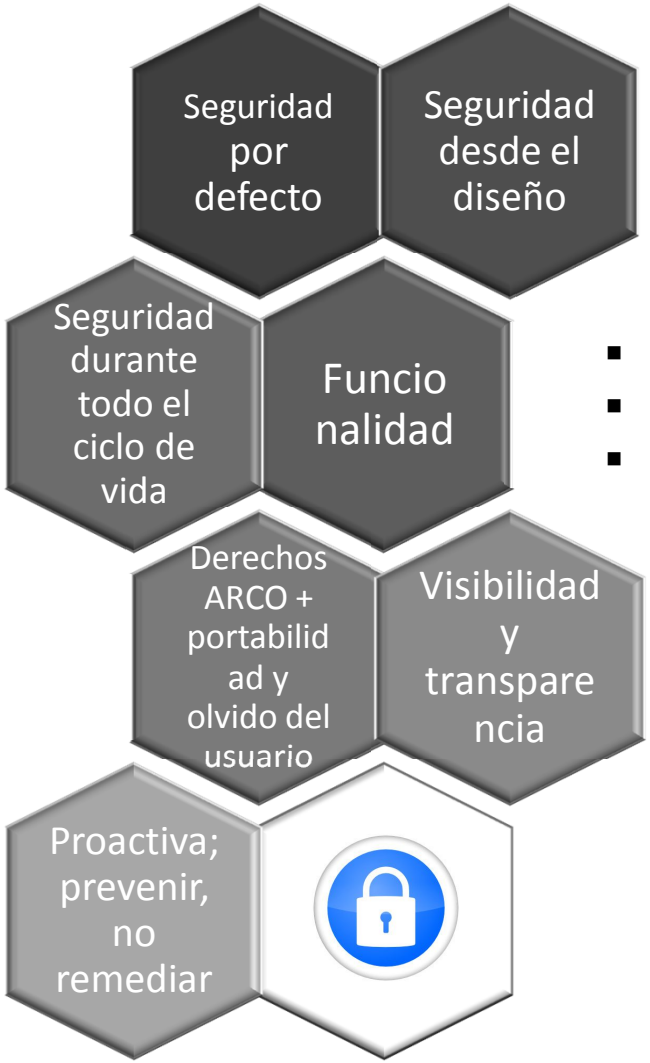
RESPONSABILIDAD PROACTIVA

Accountability o responsabilidad proactiva: responsabilidad de las organizaciones en la implantación de medidas de prevención, garantía y cumplimiento de las obligaciones y principios en protección de datos.





PRIVACY BY DESIGN & BY DEFAULT



VISIÓN **REACTIVA** DE LA SEGURIDAD

VISIÓN **PROACTIVA** DE LA SEGURIDAD

- Reducción y mitigación riesgos y costes
- Automatización y optimización de procesos
- Nuevas homologaciones y certificaciones

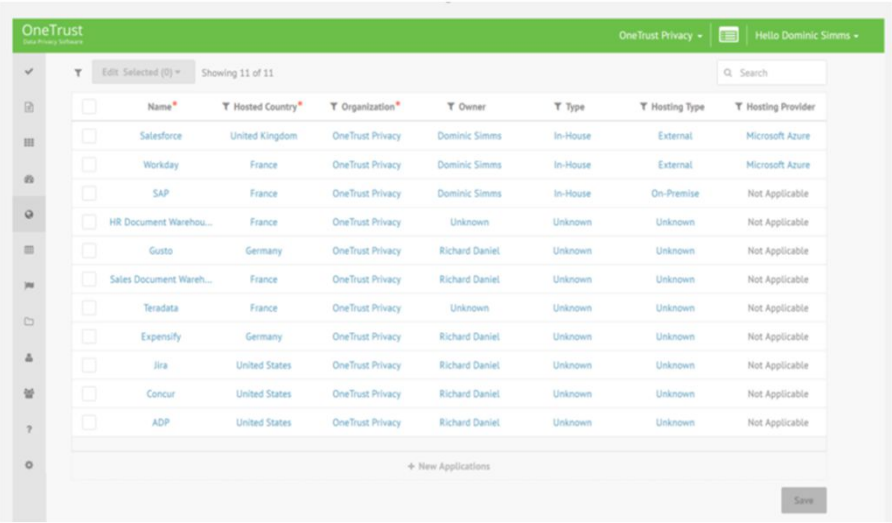
La Audiencia multa a Òmnium y ANC por abuso de datos ideológicos

El órgano judicial fija sanciones ya ejecutables por vía de apremio de 440.000 euros

Protección de Datos multa a Google con 900.000 euros por infracciones graves

Los hackers de Ashley Madison publican los datos de sus más de 32 millones de usuarios

REGISTRO DE ACTIVIDADES DE TRATAMIENTO Y TRANSFERENCIAS INTERNACIONALES DE DATOS

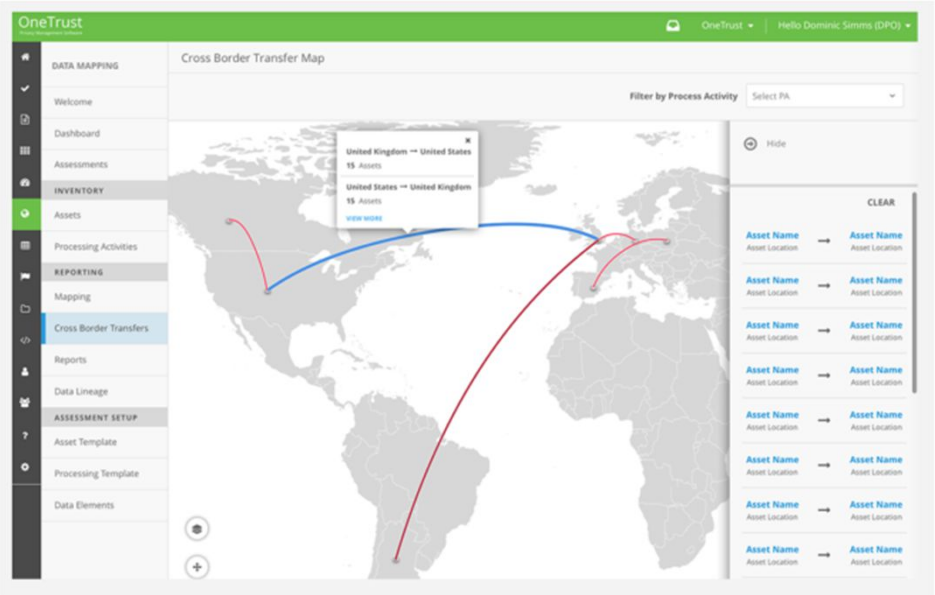


Para optimizar los procesos que establece el RGPD, y mantener unificada y actualizada toda la documentación, es recomendable utilizar una herramienta que gestione toda esta información.

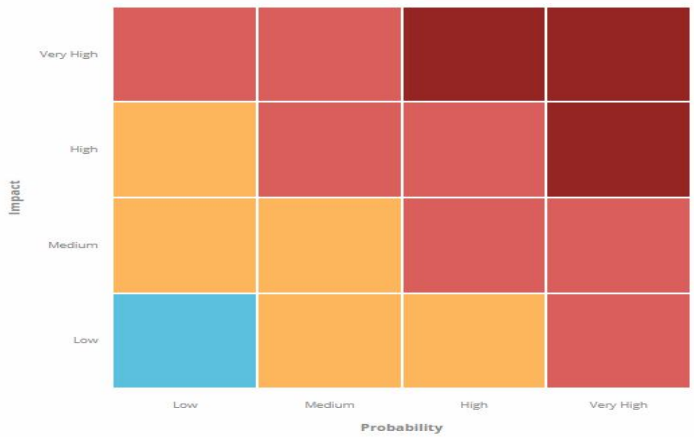
Aunque actualmente se ofrecen muchas y variadas herramientas de cumplimiento RGPD, es importante recordar que las medidas de seguridad deben ser TÉNICAS, ORGANIZATIVAS y LEGALES, y que ninguna herramienta puede abarcar todas las medidas transversales.

Registro de tratamiento: desaparece la obligación de inscribir los ficheros en la AEPD, pero se establece la obligación de elaborar y mantener actualizado el registro de tratamiento.

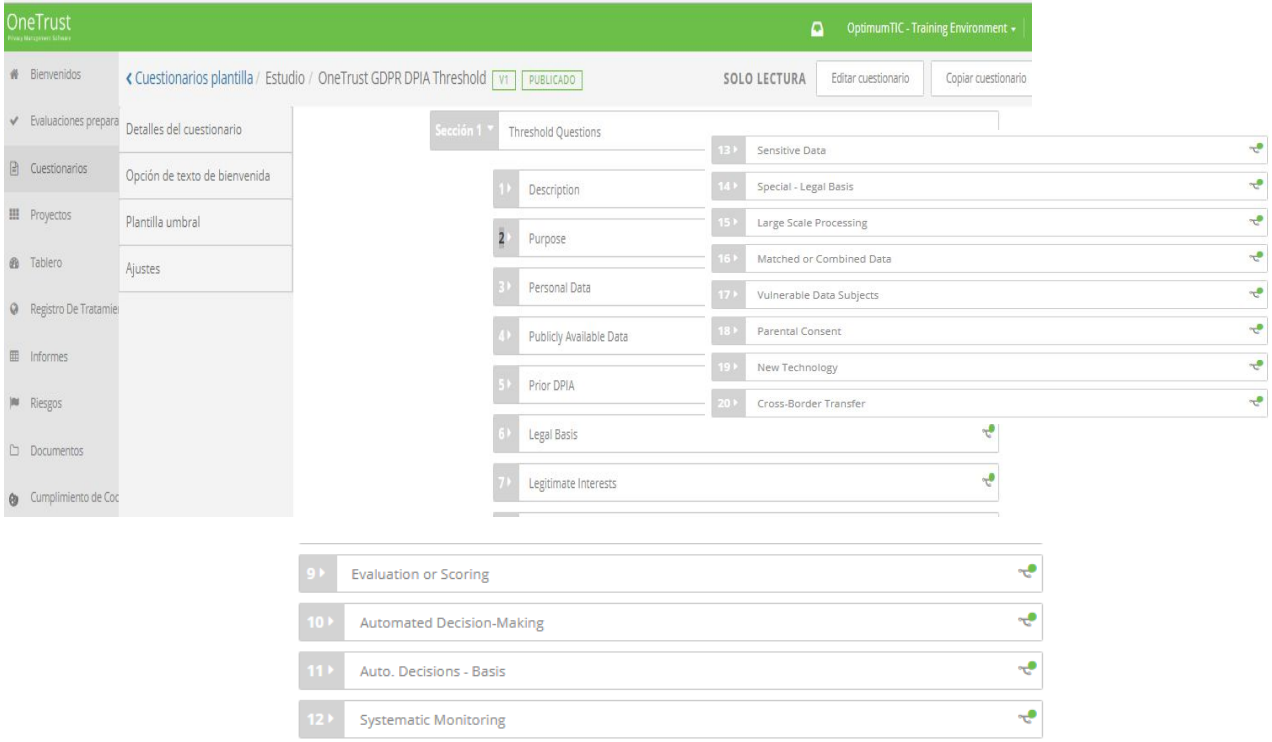
Transferencias internacionales: sólo se podrán transmitir datos a aquellos países, territorios, sectores u organismos internacionales que disponen de un nivel adecuado de protección o aportan garantías suficientes según la Comisión Europea.



ANÁLISIS DE RIESGO Y DATA PROTECTION IMPACT ASSESSMENT (DPIA)



El GDPR exige realizar análisis de riesgos para determinar y configurar medidas preventivas y seguridad para cada tratamiento.



Análisis de los riesgos que un producto o servicio puede entrañar para la protección de datos de los afectados y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

DATA PROTECTION OFFICER
Delegado de Protección de Datos

- Interno o externo, pero **independiente**
- Informar y asesorar al **responsable** de tratamiento sobre las obligaciones LOPD/GDPR
- Supervisar la aplicación de la normativa por el **encargado** de tratamiento (responsabilidades, formación y auditorías)
- Supervisar notificaciones **brechas de seguridad**
- Establecer contacto y relación con **autoridades de control** de protección de datos
- Trabajo conjunto y **coordinación con otras figuras independientes** relativas a la Seguridad en la organización: CISO y/o Responsable de Seguridad, Auditor Interno, Compliance Officer.

¿Cuándo es necesario un DPO?

1. El tratamiento lo lleve a cabo una **autoridad u organismo público**, excepto los tribunales que actúen en ejercicio de su función judicial.
2. Las actividades principales consistan en **tratamientos que, por naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala**.
3. Las actividades principales consistan en el **tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas e infracciones penales**.

DE RETO A OPORTUNIDAD

Problemas de presupuesto y cambios superficiales.	• Oportunidad de cambios estratégicos
Mentalidad de silos	• Procedimientos y medidas transversales
Inconsistencias en la homogeneización de formatos	• Homogeneización internacional
Obstáculos de adaptación y creación de nuevos protocolos	• Bases para alcanzar sistemas de Compliance

ISACA®
Trust in, and value from, information systems
Barcelona Chapter

Muchas Gracias

Oportunidades, ventajas y retos que ofrece el nuevo Reglamento General de Protección de Datos (GDPR)

OptimumTIC S.L.
Edifici Macià
Plaça Francesc Macià, Nº7. Planta 9, Oficina 9
C.P: 08029 - Barcelona
Tlf. +93 252 74 67
Info@optimumtic.com
www.optimumtic.com

OptimumTIC
OPTIMIZACIÓN DE PROCESOS Y SISTEMAS