La Seguridad de la Información como base para la gestión del *Compliance*

Pablo Sotres Cruz
Product Developer IT & Compliance
Bureau Veritas

Madrid, 16 noviembre 2017

Move Forward with Confidence

La Seguridad de la Información y Compliance Penal (UNE 19601)

La gestión del compliance es **mucho más** que solo cumplir con los requisitos de la legislación y normativa aplicables.

Sin embargo **se puede centrar la gestión de compliance** al ámbito penal y así dar cobertura al marco jurídico español e internacional.

Se requiere guiar a todas las **partes implicadas** en la forma de implantar y preparar respuestas eficaces ante los incidentes.

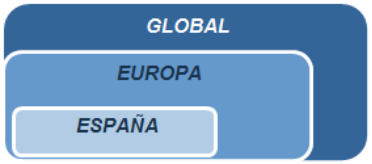
Debe tener como base la **gestión del riesgo** (ISO 31000)

Es fundamental que se **fusione en todas las actividades realizadas** por la organización, de forma transversal y apoyándose en una **sólida cultura del cumplimiento**.

Se cuenta con diferentes normas con enfoque en la **gestión global del cumplimiento** (**UNE 19601, ISO 37001 o ISO 19600**) y **específicos** (ISO 9001, ISO 27001, ISO 14001, etc.)

La Seguridad de la Información y Compliance Penal (UNE 19601)

Algunas fuentes de requisitos de cumplimiento (Compliance) que debe tener en cuenta una empresa:



Procedimientos internos operacionales

ISO 27001

Normativa y códigos sectoriales

ISO 14001

Controles internos de seguridad

Políticas corporativas de la sede central

Código Penal

Normativa fiscal y contable

Ley de Propiedad Intelectual

Ley Orgánica de Protección de Datos / Reglamento Europeo de Protección de Datos

Acuerdos con socios en UTE

Legislación Mercantil

Convenio con Universidad

Legislación Laboral

Estatuto de asociación empresarial asociada

Código ético interno

Requisitos de contratos con clientes

SLAs

ISO 9001

PCI-DSS

COSO

ENS y ENI

Normativa antifraude

LSSI

Requisitos del producto software desarrollado

Firma Electrónica

Ley Protección Infraestructuras Críticas

La Seguridad de la Información y Compliance Penal (UNE 19601)

LA CLAVE: GESTIÓN DEL RIESGO PENAL

PROCESO DE GESTIÓN DE RIESGOS PENALES

Identificación, análisis y evaluación de los riesgos penales

Análisis con respecto a cada UNO de los elementos del contexto

CÓDIGO PENAL

- Trata de seres humanos
- Tráfico / trasplante ilegal de órganos humanos
- Delitos relativos a la prostitución y la corrupción de menores
- Descubrimiento y revelación de secretos
- Estafa
- Insolvencias punibles
- **Daños informáticos**
- Delitos contra la propiedad intelectual e industrial, al mercado y a los consumidores
- Blanqueo de capitales
- Delitos contra la Hacienda Pública y contra la Seguridad Social
- Tráfico ilegal /inmigración clandestina de personas

- Delitos contra la ordenación del territorio
- Delitos contra los recursos naturales y el medio ambiente
- Establecimiento de depósitos o vertederos tóxicos
- Delitos relativos a la energía nuclear y a las radiaciones ionizantes
- Delitos de riesgo provocados por explosivos
- Delitos contra la salud pública :tráfico de drogas
- Falsificación : tarjetas de crédito y débito y cheques de viaje
- Cohecho
- Tráfico de influencias
- Corrupción en las transacciones comerciales internacionales
- Financiamiento del terrorismo
- Contrabando

Probabilidad de incumplimiento y consecuencias

RIESGO

CONSECUENCIAS: DAÑO PERSONAL Y AMBIENTAL, PÉRDIDAS ECONÓMICAS, DAÑO REPUTACIONAL Y RESPONSABILIDADES ADMINISTRATIVAS Y/O PENALES

TICs: *Tecnologías de la Información y las Comunicaciones*

I+D+i

INDUSTRIA

INFORMÁTICA Y TELECOMUNICACIONES

Aunque no seamos plenamente conscientes…

…las TICs son <u>críticas</u> para el funcionamiento de la economía mundial…

…y la Sociedad <u>exige</u>:

- **Cumplimiento**
- **Integridad**
- **Confidencialidad**
- **Disponibilidad**

TRANSPORTE

SALUD

FINANZAS

Marco regulatorio principal

- *Código Penal (reforma marzo 2015)*
- *Reglamento Europeo Protección Datos (abril 2016)*
- *Esquema Nacional Seguridad*
- *Plan Nacional de Protección de Infraestructuras Críticas*

La Seguridad de la Información y Compliance Penal (UNE 19601)

Contexto actual

Las organizaciones son cada vez más dependientes de los **riesgos** asociados a **sistemas de información complejos**.

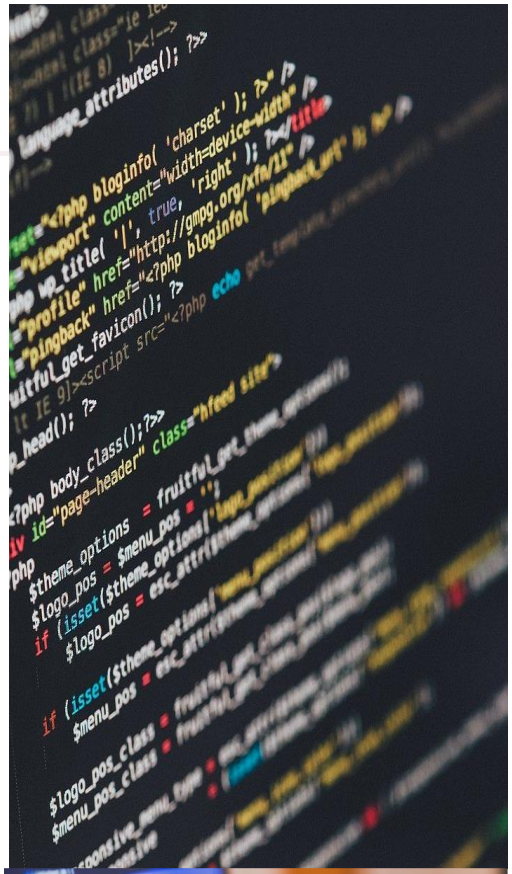
Los **requisitos de cumplimiento** (reforma del Código Penal) **nueva legislación** (Reglamento Europeo de Protección de Datos) y el aumento del número e impacto de las fallos de seguridad han hecho que las organizaciones sean más conscientes de la necesidad de tener un enfoque estructurado para la protección de la información.

La información de los usuarios (internos y externos) demanda el aseguramiento de su **disponibilidad y no repudio**.

El número de incidentes que amenazan la **fiabilidad en las operaciones** está aumentando (virus WannaCry 12/05/2017)

Un simple fallo de seguridad podría:

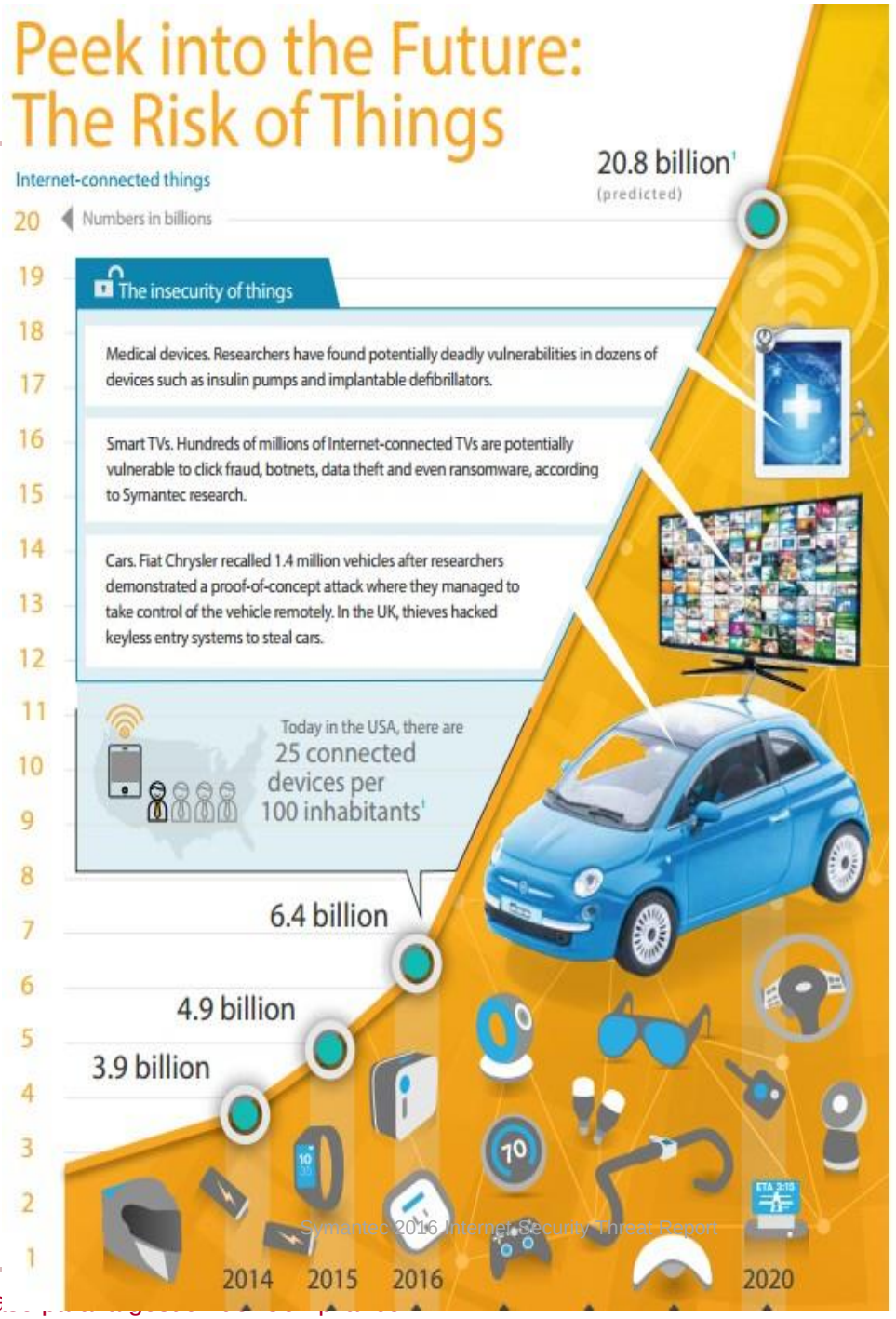
- ❑ Destruir la imagen de la compañía
- ❑ Disminuir el valor del negocio.
- ❑ Erosionar la cuenta de resultados; y
- ❑ Comprometer futuras ganancias



La Seguridad de la Información y Compliance Penal (UNE 19601)

El futuro cercano será más dependiente de los servicios on-line en internet y sin fronteras nacionales

- BIG DATA
- INTERNET DE LAS COSAS
- TRANSFORMACIÓN DIGITAL
- INDUSTRIA 4.0
- SMART CITIES



Fuente: SYMANTEC y gartner.com/newsroom/id/3165317

RIESGO PENAL Y SEGURIDAD DE LA INFORMACIÓN - *EJEMPLOS*

Artículo 264.

1. El que por c
deteriorase, alteras
informáticos o docu
será castigado con l
2. Se impondrá
impacto significativo al r

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro

¿QUÉ SOLUCIONES EXISTEN?

CERTIFICACIÓN ISO 27001

CERTIFICACIÓN RGPD

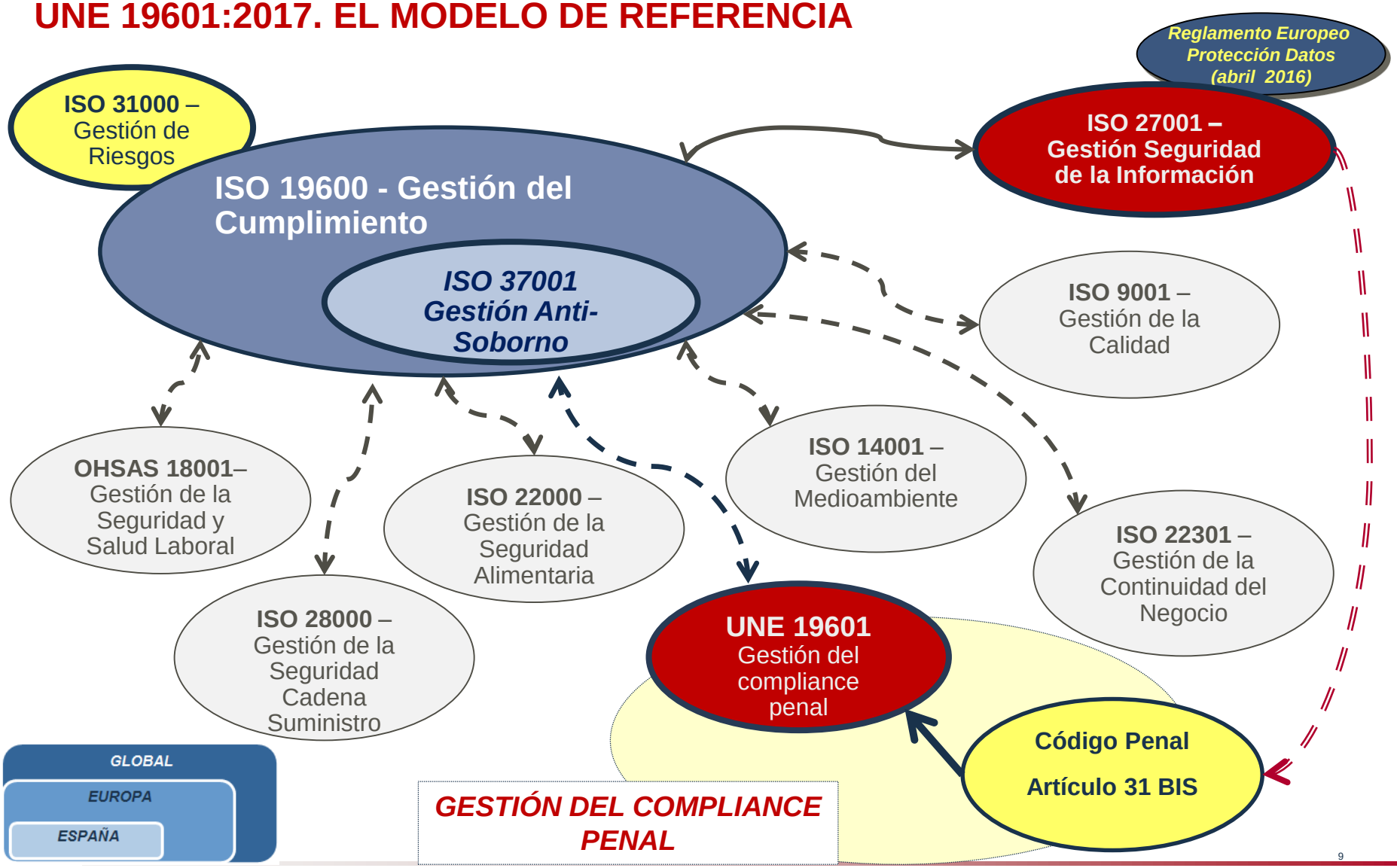
b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

La Seguridad de la Información y Compliance Penal (UNE 19601)

UNE 19601:2017. EL MODELO DE REFERENCIA



La Seguridad de la Información y Compliance Penal (UNE 19601)

► Sistema de Gestión de la Seguridad de la Información (SGSI) – ISO 27001:2013

- ❑ La parte del sistema de gestión de la organización, basada en un enfoque del riesgo empresarial, para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información
- ❑ Es un proceso de ***Gestión*** y no un proceso tecnológico
- ❑ Decisión estratégica de la organización para:
  - Diseñar e implantar…
    - Necesidades y objetivos
    - Requistos de seguridad (internos y externos)
    - Procesos y recursos empleados
  - Ajustado según “necesidades”

>33.000
certificados en todo el mundo (*)

(*) Fuente: ISO Survey (2016)

La Seguridad de la Información y Compliance Penal (UNE 19601)

- **ISO/IEC 27001:2013**
  - Sistema de Gestión de Seguridad de la Información: Certificación de los sistemas de información que dan **soporte** a los **procesos del negocio**, minimizando los **riesgos** y asegurando su **continuidad** frente a imprevistos o desastres.
  - Norma preventiva basada en la valoración y tratamiento sistemático de los riesgos en materia de seguridad de la información. Asume los principios de **ISO 31000.**
  - Integrable con **ISO 9001, ISO 20000-1, UNE 19601 e ISO 22301, entre otras**.
  - Se caracteriza por preservar, al menos: Confidencialidad, Integridad y Disponibilidad.
  - Propone un catálogo mínimo de 114 controles, detallados en ISO 27002.

(Técnicos, organizativos y legales)

La Seguridad de la Información y Compliance Penal (UNE 19601)

Un nuevo reglamento aplicable a todas las empresas que traten datos de ciudadanos de la UE

- El RGPD entró en vigor el 24 de mayo de 2016 y se aplicará a partir del **25 de mayo de 2018**.
- Afecta a **todas las empresas que procesen datos personales de ciudadanos de la UE**, independientemente de su ubicación.

Derechos y libertades de las personas físicas

- Derecho al **olvido**,
- Derecho a la **portabilidad**
- **Consentimiento explícito** de los interesados y mejora de la información facilitada a estos
- Confirmación de las **obligaciones de protección y confidencialidad** en el caso de **transferencias de datos fuera de la UE**

Nuevas obligaciones para las empresas (incluidos sus subcontratistas)

- Principio de **responsabilidad proactiva**: las empresas deberán demostrar que cumplen lo dispuesto en el RGPD (con un registro de las actividades de tratamiento de datos, políticas de protección y evaluaciones de impacto relativas a la protección de datos sensibles, así como mediante la adhesión a un código de conducta o a un mecanismo de certificación).
- Principios de «**protección de datos desde el diseño**» y «**protección de datos por defecto**» para todos los servicios
- **Notificación de las violaciones de la seguridad** de los datos a la **autoridad de protección de datos** + notificación directa a los clientes y usuarios finales + reparación de violaciones
- Nueva función de cumplimiento: **Delegado de protección de datos**

Incrementan las multas administrativas por infracciones:

- Máximo 20M€ o un 4 % del volumen de negocios total
- **Se pueden reducir en caso de certificación**

La Seguridad de la Información y Compliance Penal (UNE 19601)

Tratamiento de datos personales de interesados que se residen en la Unión Europea cuando las actividades de tratamiento estén relacionadas con

Oferta de bienes o servicios a interesados en la Unión Europea

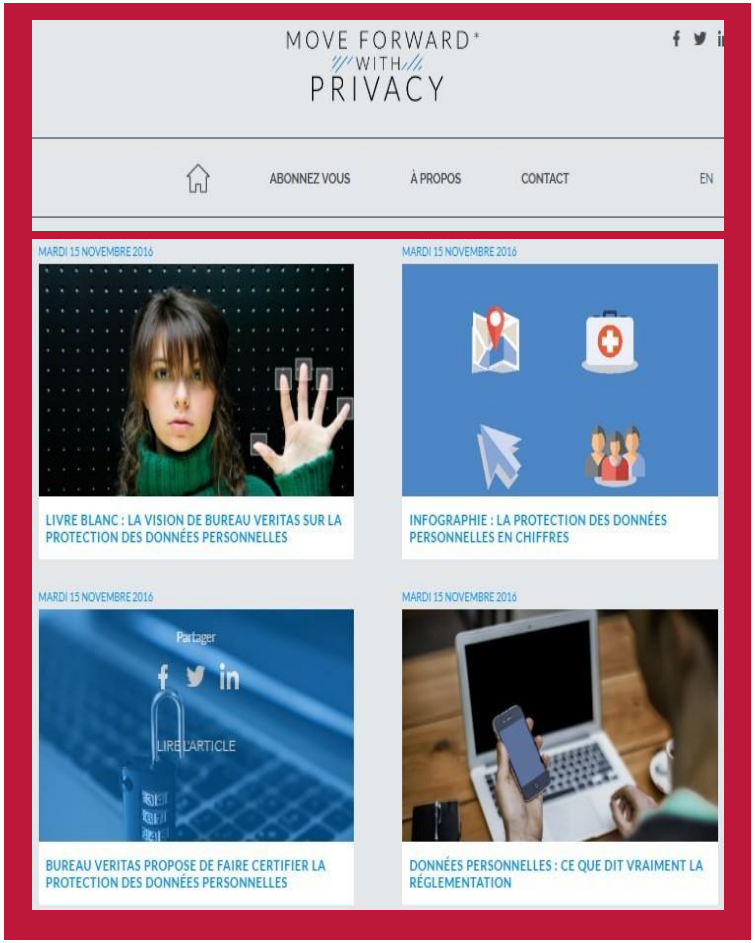
y/o

el control de su comportamiento

La certificación de protección de datos demostrará la existencia y adopción de garantías adecuadas

Art. 42 del RGPD

BV se posiciona proactivamente en la privacidad y el compliance



Creando primero una imagen de marca corporativa BV basada en la privacidad
Libro blanco y sitio web
http://www.move-forward-with-privacy.bureauveritas.com/en/

Proponiendo un mecanismo de certificación

- Una **certificación internacional** independiente de requisitos de cumplimiento locales.
- Se centra en el **sistema de gestión de datos personales.**
- Crea un **proceso de mejora continua** para la protección de datos personales.
- Se puede adaptar al modelo de responsabilidad social corporativa (RSC) y toda la cadena de suministro.
- Se aplica a **todo tipo de empresas**.

Ofreciendo cursos y seminarios virtuales sobre el RGPD

Proponiendo un plan relacionado con la certificación de delegados de protección de datos

La Seguridad de la Información y Compliance Penal (UNE 19601)

El artículo 42 del Reglamento establece expresamente una certificación independiente

Certificación

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

La **primera norma técnica mundial** de certificación **RGPD**

- Directrices emitidas por WG G29
- RGPD
- ISO 27001 (seguridad de TI/SI)
- ISO 9001 (sistema de gestión)
- ISO 29100 e ISO 29101 (privacidad y arquitectura)

Sistemas de gestión

Organización y estructura

- Gestión de datos personales y de interesados - Evaluación de impacto relativa a la protección (PIA)
- Comunicación, incluida la gestión de crisis
- Diseño y desarrollo de productos y servicios
- Tratamiento
- Subcontratación y prestación de servicios

Funciones de apoyo

TI/SI | RR. HH. | Márketing | Equipo Jurídico

Interesado/persona física

Gracias por su atención.

Para cualquier duda pueden contactar con:

Pablo Sotres Cruz
Product Developer Information Technology & Compliance
pablo.sotres@es.bureauveritas.com

© - Copyright Bureau Veritas