Secure&IT

www.secureit.es

# Acerca de Secure&IT


Francisco Valencia

Director General
Secure&IT
francisco.valencia@secureit.es
911 196 995

Secure&IT

www.secureit.es

# ¿Falsa sensación de seguridad?

# Los pilares de la Seguridad de la Información


**CUMPLIMIENTO NORMATIVO**

**Satisface la demanda que le es exigida a la organización.**

- & Exigencias **Legales** (Privacidad…)
- & Normas **Sectoriales** (PCI-DSS, ENS…)
- & **Estándares** (ISO 27001 / 20000 / 22301)
- & Medidas dispuestas por **Clientes**

**PROCESOS CORPORATIVOS**

**Permite dotar al CEO de un "cuadro de mando" de la gestión de su seguridad.**

- & Identificación y valoración de **Activos**
- & Análisis de **Riesgos**
- & Roles y **Responsabilidades**
- & **Medidas** aplicadas y sus **Resultados**

**SEGURIDAD INFORMÁTICA**

**Protege las vulnerabilidades propias de los sistemas informáticos:**

- & Sistemas anti **malware**
- & Protección contra **hackers**
- & **Copias** de seguridad
- & **Criptografía**

**VIGILANCIA DE LA SEGURIDAD**

**Permite la rápida detección, respuesta y mitigación de impactos de seguridad**

- & Aplica tanto a **IT** como a **procesos**
- & Reduce la incertidumbre. Existen **IRPs**
- & Control **gráfico**
- & Informes y **cuadros de mando**

# Acerca de Secure&IT

Empresa 100% española creada en 2009 por Abogados expertos en Derecho de las TIC, Ingenieros y Expertos en Seguridad de la Información.

Misión: Ayudar a las empresas a disminuir los riesgos a que se exponen a causa de la gestión de su información.

Líderes en auditoría e implantación de modelos avanzados de gestión de la ciberseguridad y el cumplimiento normativo

Equipo altamente cualificado, gran parte de la inversión destinada a formación.

Seguridad 360º para la información de su empresa:

Procesos Corporativos
Seguridad Informática
Cumplimiento Normativo

Secure&View©. SOC-CERT de control y supervisión de seguridad, redes y sistemas 24x7x365 ISO 27001.

# Nuestros Servicios. Seguridad 360º


- & Protección de Datos
- & Propiedad Intelectual
- & Comercio Electrónico
- & Telecomunicaciones
- & Firma Electrónica
- & Contratos TIC
- & Arbitraje y Mediación
- & Prevención del Delito
- & PCI-DSS
- & Esquema Nacional ENS
- & Peritajes Judiciales

- & Auditoría de Seguridad
- & Hacking Ético
- & Consultoría Seguridad
- & Planes Directores
- & Procesos corporativos
- & Análisis de Riesgos
- & Planes de Continuidad
- & Formación
- & ISO 27001 / SGSI
- & ISO 22301 / SGCN
- & ISO 20000 / SGSTI

- & SOC-CERT
- & 24 X 7 X 365
- & Monitorización
- & SIEM – Alertas
- & Respuesta rápida
- & Operación ISO 27001
- & Control de Políticas
- & Copias de Seguridad
- & Seguridad CLOUD
- & Sandboxing

- & Redes y Comunicaciones
- & Granjas de servidores
- & Firewalls UTM/NGFW
- & DNS Firewall
- & Anti DDOS
- & Web Firewall, WAF
- & Seguridad de Puesto/MDM
- & Seguridad Correo
- & Seguridad Bases de Datos
- & NAC
- & PKI, Identidad Digital
- & DLP/IRM

Secure & IT

www.secureit.es

PYME INNOVADORA

Válido hasta el 31 de diciembre de 2018

Seguridad Certificada

ISO/IEC 27001:2013
Certificate Nº:48038

# Novedades introducidas por el Reglamento General de Protección de Datos

# ¿Y este cambio a qué se debe?

- Normativa en privacidad obsoleta (La actual es de 1995, cuando las Tecnologías de la información no estaban desarrolladas)
- En España, el Real Decreto se actualiza en 2007 (hace 10 años)
- ¿Qué capacidad técnica tiene el legislador? → "La Ley va por detrás de la tecnología"
- Normas divergentes, incluso dentro del marco de la UE
- Nueva realidad y derechos de las personas (Derecho al olvido, Derecho a la portabilidad de datos, etc.)

# ¿A quién aplica?

- A empresas con domicilio en la UE.
- Aplicable a los datos de personas físicas, independientemente de su nacionalidad o residencia.
- La LOPD excluía datos profesionales de empleados, autónomos o apoderados.
- GDPR no hace esta exclusión.

# ¿Qué cambia legalmente?

- & Queda derogada la anterior Directiva Europea 95/46/CE
- & Queda derogada la Ley Orgánica 15/99 de Protección de Datos
- & Queda derogado el Real Decreto 1720/2007
- & Entra en vigor el Reglamento General de Protección de Datos UE 2016/679
- & La Agencia de Protección de Datos establece que podrá publicarse una norma de desarrollo en mayo de 2018
- & No es necesario transponer → Será igual en todos los países de la UE.

# ¿Qué cambia conceptualmente?

## LOPD

- Consentimiento tácito
- 3 niveles: alto, medio y básico
- Inscripción pública de ficheros
- Regulación externa
- Medidas de seguridad establecidas en RD
- Seguridad reactiva
- 4 derechos: ARCO

## GDPR

- Consentimiento expreso
- 2 niveles: especiales y no especiales
- Registro interno de actividades de tratamiento
- Autorregulación
- Medidas de seguridad definidas por la empresa
- Seguridad proactiva: Vigilancia
- 6 Derechos: ARCO + olvido + portabilidad

Secure & IT

www.secureit.es

PYME INNOVADORA

Válido hasta el 31 de diciembre de 2018

Seguridad Certificada

ISO/IEC 27001:2013
Certificate Nº:48038

# RESPONSABILIDAD LEGAL DE LAS EMPRESAS ANTE EL NUEVO REGLAMENTO EUROPEO

# Infracciones y sanciones

| 10.000.000 € | 2% volumen negocio total anual del ejercicio financiero anterior |
|---|---|

- Falta de obtención del consentimiento paterno en caso de menores
- Falta de implementación de medidas de seguridad apropiadas.
- No realización de una evaluación de impacto
- No designar un Delegado de Protección de Datos.
- Falta de cooperación con la Autoridad de Control.
- Incumplimiento de las obligaciones por parte del encargado del tratamiento.
- Incumplimiento de las obligaciones como corresponsables.
- No cumplir con las obligaciones impuestas a los organismos de certificación
- No notificar las violaciones de seguridad

# Infracciones y sanciones

| 20.000.000 € | 4% volumen negocio total anual del ejercicio financiero anterior |
|---|---|

- Falta de cumplimiento de los principios básicos del tratamiento
- No atender o no facilitar el ejercicio de los derechos ARCOPO de los interesados:
- Incumplimiento de las normas del Estado Miembro.
- No permitir acceso a la Autoridad de Control a datos personales y/o locales
- No cumplir una orden de la Autoridad de Control.
- Incumplimiento de los requisitos para transferencias internacionales
- No informar a los interesados en el momento en el que se obtengan su datos.
- No contar con el consentimiento explícito del interesado.
- Incumplimiento del deber de secreto.

Secure & IT

www.secureit.es

PYME INNOVADORA

Válido hasta el 31 de diciembre de 2018

Seguridad Certificada

ISO/IEC 27001:2013

Certificate Nº:48038

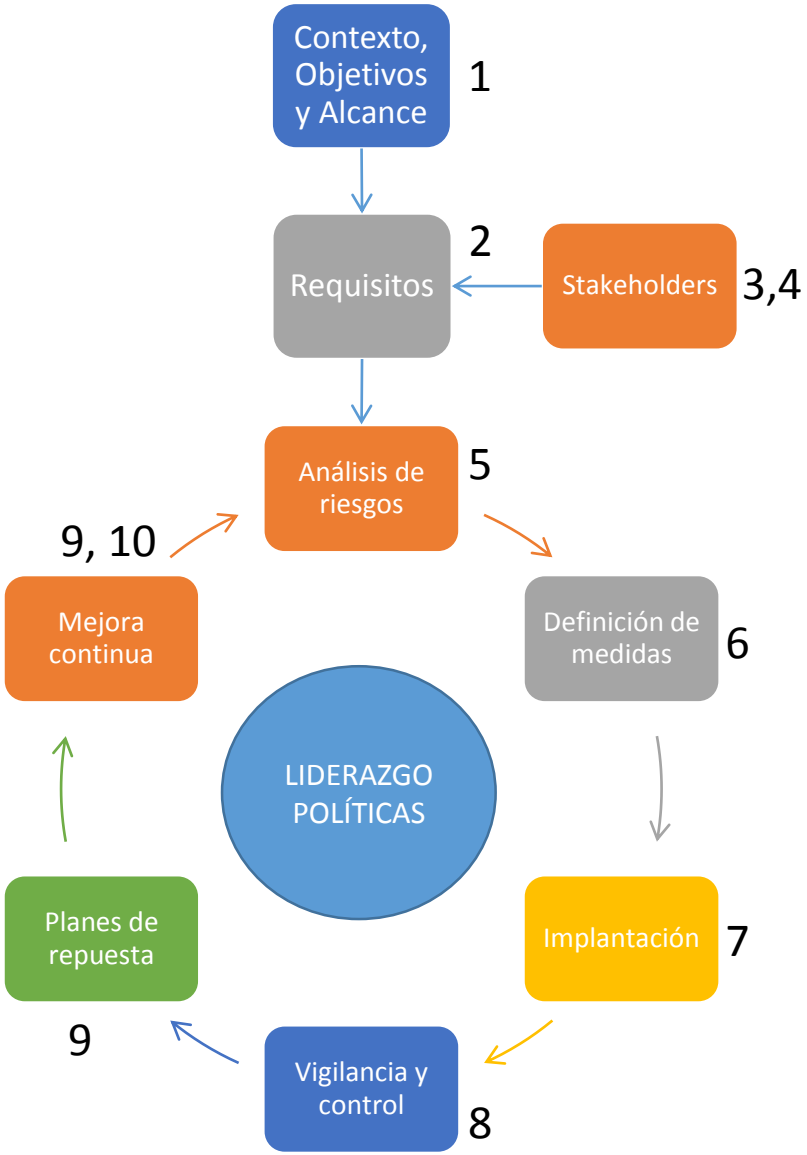
# Medidas organizativas y técnicas para el cumplimiento GDPR

# MODELO GENERAL DE CUMPLIMIENTO. CHECKLIST

1. • Identificar y registrar el tratamiento de datos pretendido
   • Realizar análisis de impacto. -> Con ciertos supuestos, consulta previa
2. • Nombrar un Delegado de Protección de Datos interno o externo
   • Identificar código de conducta sectorial
3. • Presentar información y pedir consentimiento al interesado. Ojo a la finalidad
4. • Realizar acuerdos contractuales con terceros encargados del tratamiento
5. • Realizar análisis de riegos PARA EL INTERESADO de la pérdida de confidencialidad, integridad o disponibilidad de sus datos (Magerit, ISO 31000, etc…)
6. • Selección de controles adecuados. Comparar con un marco de controles (ISO27002, ISO27018, COBIT, etc.)
7. • Implantación las medidas técnicas y organizativas resultantes del análisis de riesgos.
   • Política, RRHH, Control de accesos, Criptografía, Física, TI, Comunicaciones, Continuidad de Negocio, etc..
8. • Monitorización, vigilancia continua del sistema
   • Respuesta ante incidentes
9. • Auditoría del sistema
   • Toma de decisiones para la mejora
10. • Certificación del Sistema de Gestión de Privacidad (Voluntario pero recomendable)

# SISTEMA DE GESTIÓN DE LA PRIVACIODAD

1. •Identificar y registrar el tratamiento de datos pretendido
   •Realizar análisis de impacto. -> Con ciertos supuestos, consulta previa
2. •Nombrar un Delegado de Protección de Datos interno o externo
   •Identificar código de conducta sectorial
3. •Presentar información y pedir consentimiento al interesado. Ojo a la finalidad
4. •Realizar acuerdos contractuales con terceros encargados del tratamiento
5. •Realizar análisis de riegos PARA EL INTERESADO de la pérdida de confidencialidad, integridad o disponibilidad de sus datos (Magerit, ISO 31000, etc…)
6. •Selección de controles adecuados. Comparar con un marco de controles (ISO27002, ISO27018, COBIT, etc.)
7. •Implantación las medidas técnicas y organizativas resultantes del análisis de riesgos.
   •Política, RRHH, Control de accesos, Criptografía, Física, TI, Comunicaciones, Continuidad de Negocio, etc..
8. •Monitorización, vigilancia continua del sistema
   •Respuesta ante incidentes
9. •Auditoría del sistema
   •Toma de decisiones para la mejora
10. •Certificación del Sistema de Gestión de Privacidad (Voluntario pero recomendable)

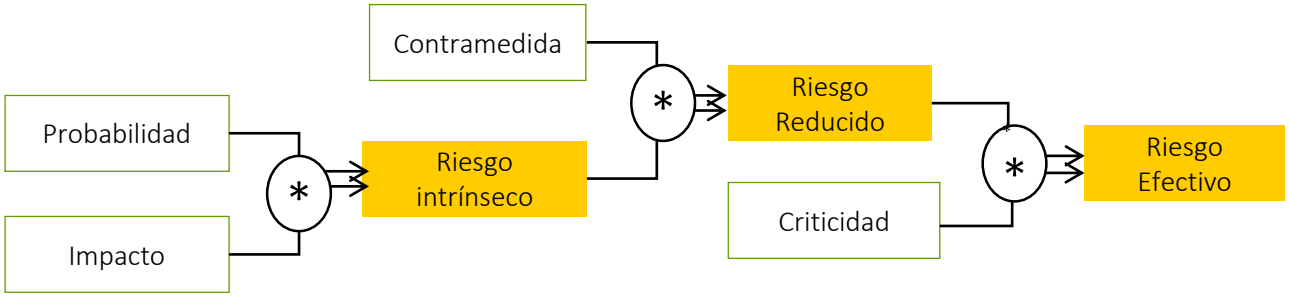


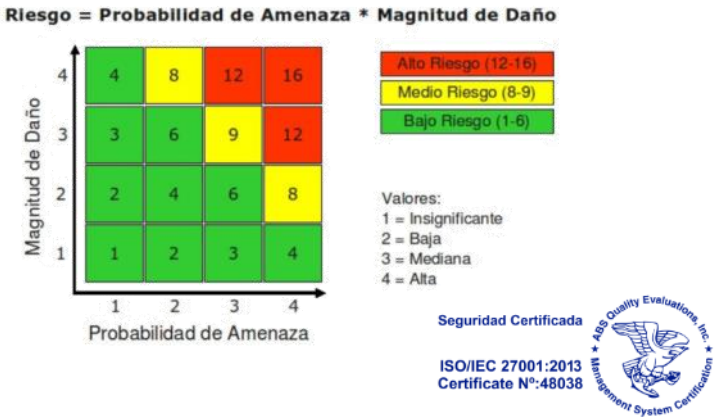
# CONTEXTO, OBJETIVOS, TITULARES

- ¿Qué queremos hacer con los datos?
  - Finalidad buscada
  - Cuestiones externas e internas
  - Contexto regulatorio, social y cultural
  - ¿Datos especiales?
- ¿Identificamos un IMPACTO elevado en caso de pérdida de confidencialidad, integridad o disponibilidad? ¿Estamos en alguno de los casos que la AEPD dictará? Entonces debo pedir permiso
- ¿Para que nos ha autorizado el titular disponer de estos datos? ¿Coincide su expectativa con la nuestra?
- Para garantizar SUS derechos, nombraré un Delegado de Protección
  - Interno o externo
  - Independiente
  - Vela por los titulares, no por la empresa
- Si existe un código de conducta aplicable, estudiar la adhesión al mismo
- Garantizar que nuestros proveedores cumplen las medidas de seguridad que se deciden -> Encargados del tratamiento

# ANÁLISIS DE RIESGOS

- & Responde a: ¿Cómo afecta a los usuarios la pérdida de confidencialidad, integridad y disponibilidad de sus datos?
- & Analizar ESCENARIOS DE RIESGO en base a la probabilidad y al IMPACTO de que se materialicen.
- & Ej: Robo de datos, deslealtad, malware, fallos informáticos, incidentes, cibercrimen, espionaje, etc…
- & Ideal: Emplear una metodología conocida (ISO31000, MAGERIT, etc)





Secure&IT
www.secureit.es

# PROCESOS CORPORATIVOS …

- & ESTABLECIMIENTO DE POLÍTICAS
- & ROLES Y RESPONSABILIDADES (DPO, OTROS ROLES Y AUTORIDADES, COMPATIBILIDADES)
- & PROCESO DE AUTORIZACIÓN DE ACCESO
- & REVISIÓN Y METODOLOGÍA DEL ANÁLISIS DE RIESGOS
- & CONCIENCIACIÓN Y FORMACIÓN
- & PROCESO DE ALTA Y BAJA EN LA EMPRESA
- & SEGURIDAD FÍSICA Y AMBIENTAL
- & MANTENIMIENTO DE SISTEMAS
- & PROCESO DE DESTRUCCIÓN DE INFORMACIÓN
- & TELETRABAJO
- & GESTIÓN DE EVENTOS, INCIDENCIAS Y CAMBIOS
- & PLAN DE CONTINUIDAD DE NEGOCIO
- & AUDITORÍA

# … Y MEDIDAS DE SEGURIDAD TI

- & SEGURIDAD PERIMETRAL Y EN REDES DE COMUNICACIONES
- & CONTROL DE PUESTO DE TRABAJO Y SERVIDORES
- & SERVICIOS WEB
- & COPIAS DE SEGURIDAD
- & USO DE LOS SISTEMAS DE TI
- & ANTIMALWARE
- & SEGURIDAD EN BASES DE DATOS
- & CRIPTOGRAFÍA
- & SEGURIDAD EN DISPOSITIVOS MÓVILES
- & PREVENCIÓN DE FUGA DE INFORMACIÓN
- & MONITORIZACIÓN Y VIGILANCIA
- & ANÁLISIS DE VULNERABILIDADES TÉCNICAS

# APLICABILIDAD DE CONTROLES

## DOMINIOS ISO 27002

## SE DESARROLLAN EN 114 CONTROLES

- POLÍTICA DE SEGURIDAD
- ASPECTOS ORGANIZATIVOS DE LA SI
- SEG. LIGADA A RRHH
- GESTIÓN DE ACTIVOS
- CONTROL DE ACCESOS
- CIFRADO
- SEG. FÍSICA Y AMBIENTAL
- SEG. EN LA OPERATIVA
- SEG. EN LAS TELECOMUNICACIONES
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN
- RELACIONES CON SUMINISTRADORES
- GESTIÓN DE INCIDENTES EN LA SI
- ASPECTOS DE SI EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO
- CUMPLIMIENTO

# Muchas medidas… ¿Cómo se coordinan todas?

¿


?

# PROGRAMA GOLD SECURITY

& **Secure&IT**, como empresa especializada en **ciberseguridad** y **cumplimiento**, ha desarrollado un servicio de acompañamiento que ayuda a las organizaciones a establecer un Sistema de Gestión de Seguridad de la Información y el cumplimiento considerando:

- & **Protección de Datos**
- & **Cumplimiento normativo**
- & **Prevención del Delito Tecnológico**
- & **Procesos Corporativos de Seguridad**
- & **Seguridad de la Información**
- & **Tecnología y vigilancia**

& Este programa de acompañamiento es **reconocido** y **certificado**. Un programa que certifica un estricto cumplimiento de controles de seguridad que han sido seleccionados por **Secure&IT** de entre los presentes en los mejores estándares y normativas de gestión de la Seguridad.

& Gracias a este servicio, su empresa contará con un **COMITÉ DE SEGURIDAD**, formada por personal propio y por expertos, que le ayudarán a medir y reducir sus riesgos, y demostrar a terceros esta capacidad.


Secure&IT
www.secureit.es

Certifica que la compañía

EMPRESA EJEMPLO, S.L.

Ha satisfecho los requerimientos de seguridad **2015** correspondientes al nivel **GOLD SECURITY,** y reconoce su excelente labor en la gestión de la Seguridad de la Información en las lineas de trabajo de:

**Protección de Datos y Cumplimiento Normativo**
**Procesos Corporativos de Gestión de la Seguridad**
**Sistemas de Seguridad Informática**

Madrid, a 28 de Febrero de 2015
Firma y sello:


Secure&IT
www.secureit.es

Seguridad Certificada
ISO/IEC 27001:2013
Certificate Nº:48038

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
AUTHORIZED TO USE CERT

# PROGRAMA GOLD SECURITY

& Se establece un periodo de trabajo de 3 años, en los cuales:

- & Se establece un **Comité de Seguridad y cumplimiento** con seguimiento mensual
- & Se realizan **auditorías** bienales de Protección de Datos, Seguridad Informática y Procesos
- & Se establece un **Plan Director de Seguridad y cumplimiento**, con indicación de los proyectos a ejecutar en los tres años
- & Se asegura el **cumplimiento** de la organización en la normativa que le es de aplicación
- & Se establecen **procesos corporativos** de gestión de la seguridad
- & Se certifica a la organización conforme la norma **ISO/IEC 27001:2013**
- & Se imparte **formación y concienciación** continuada (píldoras formativas semanales)
- & Se implantan las **medidas tecnológicas** necesarias para el cumplimiento
- & Se integran los sistemas de TI de la organización en el **SOC-CERT** de **Secure&IT**

& Y todo ello bajo una única cuota mensual. Sin inversiones ni más gastos

# MONITORIZACIÓN Y VIGILANCIA

**CUMPLIMIENTO**

**Satisfacer la demanda que le es exigida a la organización.**

& Exigencias **Legales** (Privacidad…)
& Normas **Sectoriales** (PCI-DSS, ENS…)
& **Estándares** (ISO 27001 / 22301….)
& Medidas dispuestas por **Clientes**

**PROCESOS**

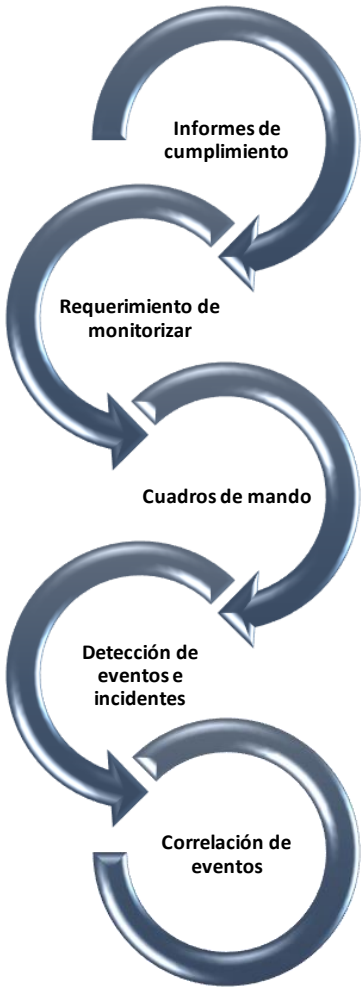
**Permiten dotar al CEO de un "cuadro de mando" de la gestión de su seguridad.**

& Identificación y valoración de **Activos**
& Análisis de **Riesgos**
& Roles y **Responsabilidades**
& **Medidas** aplicadas y sus **Resultados**
& **Procedimientos de prevención**

**SEGURIDAD TI**

**Protegen las vulnerabilidades propias de los sistemas informáticos:**

& Sistemas anti **malware**
& Protección contra **hackers**
& **Copias** de seguridad
& **Criptografía**




# REQUERIMIENTOS DE CUMPLIMIENTO …

## EXIGENCIA DE REGISTRO

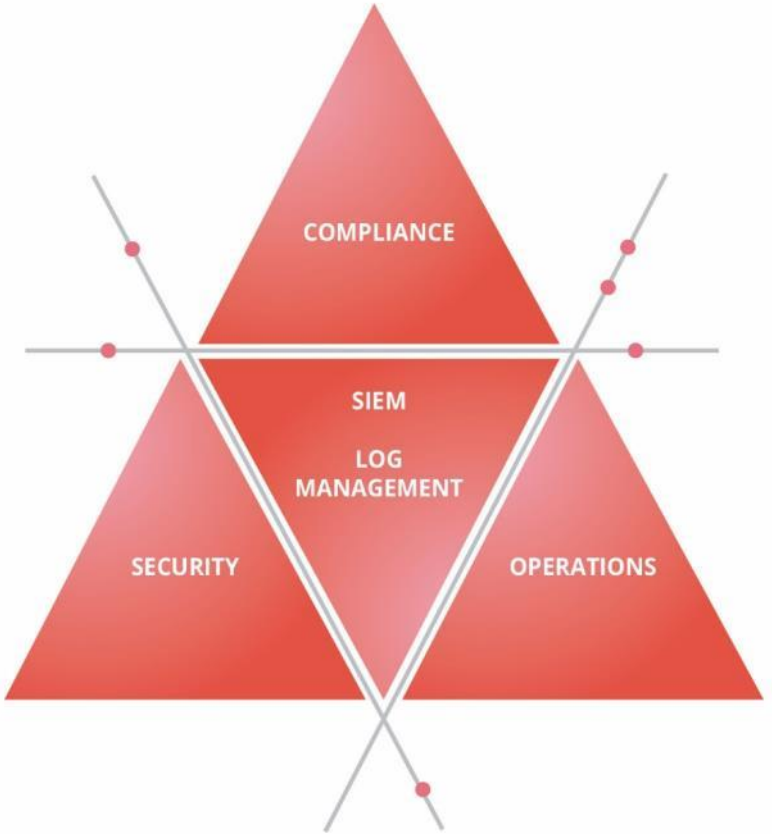
- & LEY 34/02 SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y EL COMERCIO ELECTRONICO (ART. 27)
- & 59/03 FIRMA ELECTRÓNICA (ART. 17)
- & RD 1720/07 PROTECCIÓN DE DATOS (ART. 102)
- & RD 03/10 ESQUEMA NACIONAL DE SEGURIDAD (ART. 24)
- & LEY 10/10 BLANQUEO DE CAPITALES (ART. 25)
- & RD 304/14 BLANQUEO DE CAPITALES (ART. 18)
- & LEY 25/07 CONSERVACIÓN DE DATOS RELATIVOS A COMUNICACIONES ELECTRÓNICAS (ART. 3, ART. 5)
- & PCI-DSS V3.2 (REQ 3.1, REQ 3.6, REQ 8)
- & LEY 26/06 MEDIACIÓN DE SEGUROS (ART. 8)
- & RD 764/10 MEDIACION DE SEGUROS (CAP I, ART. 1)
- & LEY 41/02 AUTONOMIA DEL PACIENTE (ART. 2)
- & FOOD AND DRUGS ADMINISTRATION (ART. 4)

## ADEMAS: MONITORIZACIÓN Y DETECCIÓN DE INCIDENTES

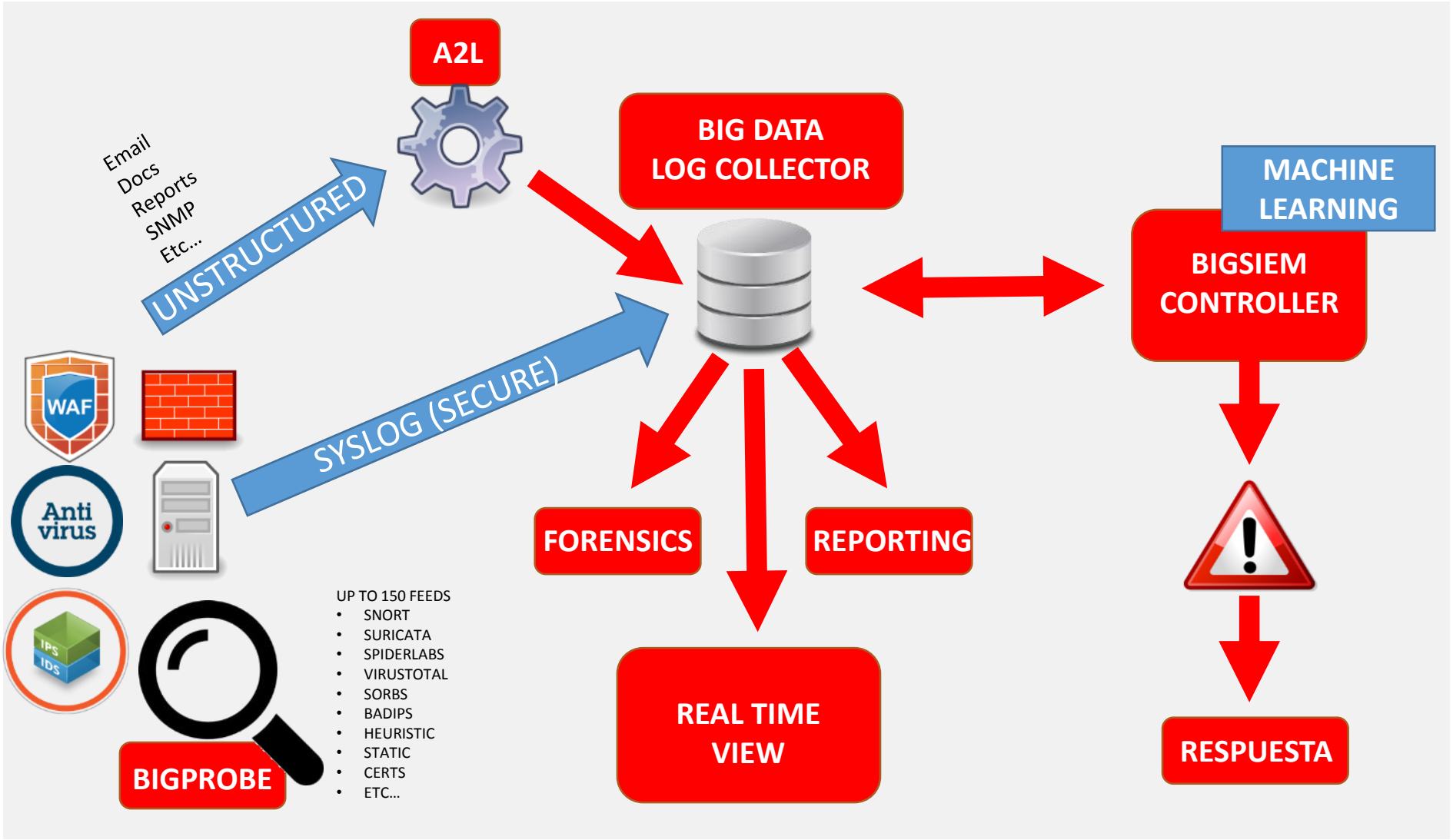
- & GENERAL DATA PROTECTION REGULATION - GDPR (ART 32, ART.33)
- & RD 03/10 ESQUEMA NACIONAL DE SEGURIDAD (ART. 23)
- & LEY ORGÁNICA 10/95 CÓDIGO PENAL (ART. 31BIS)
- & PCI-DSS V3.2 (REQ 5.1, REQ 10.5, REQ 11.1)
- & ISO 27001 (REQ A.12.4)
- & ISO 22301 (REQ 8.4)
- & ISO 20000-1 (REQ 6.6)
- & HIPAA (AP. 164.308)
- & SOX (SECC 404)

# SIEM
# (Security Information Event Management)

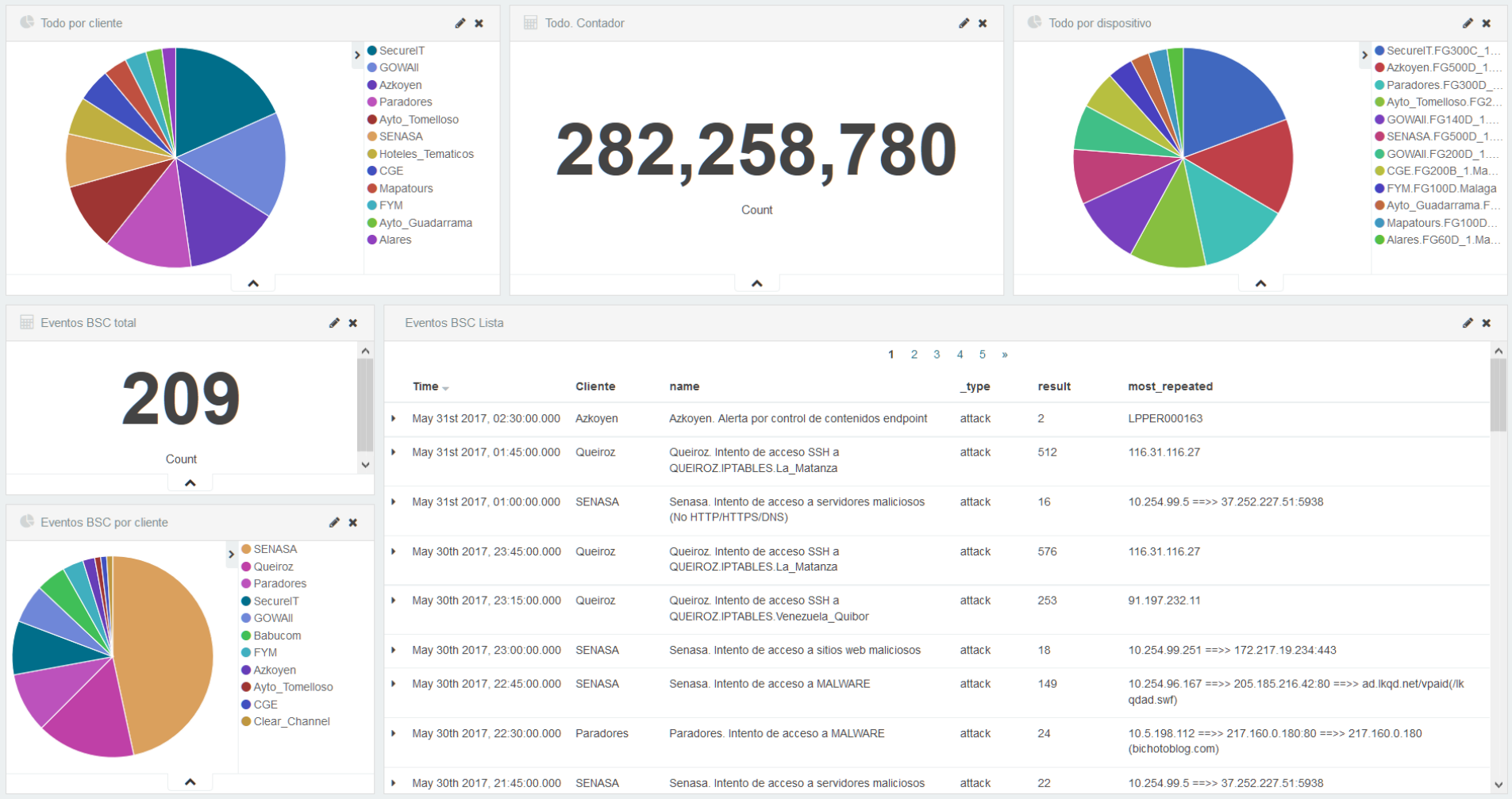
- & Análisis en tiempo real de eventos de seguridad
- & Almacenamiento y registro de los datos
- & Categorización y de los registros
- & Inteligencia de negocio
- & Alertas y notificaciones
- & Herramientas de visualización y control
- & Priorización de eventos
- & Reporting
- & Cumplimiento



# BigSIEM: SIEM SaaS & Emergency Response



# BigSIEM: Capacidad de Análisis

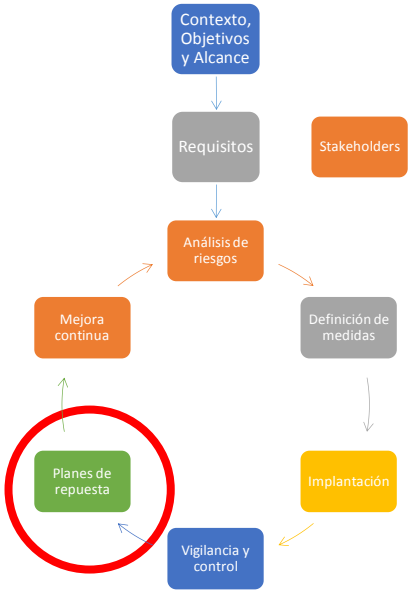


# Secure&View©. Capacidad de Respuesta

## SERVICIOS

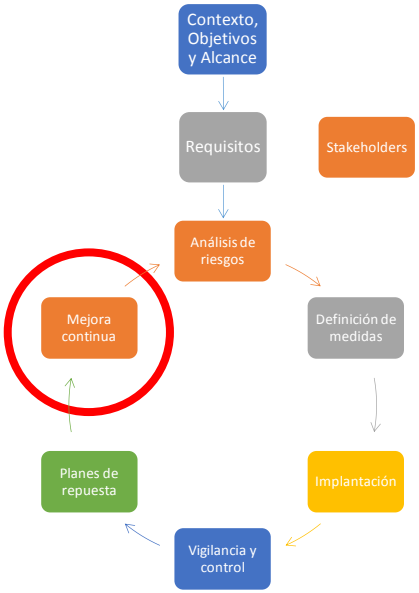
- Alertas de seguridad
- Avisos de vulnerabilidades
- Monitorización
- Gestión de incidencias
- Gestión de vulnerabilidades
- Auditorías
- Test de Intrusión
- Inteligencia y análisis
- Gestión de dispositivos
  - Firewalls
  - WAF
  - Antimalware
  - MDM/MDS
  - DNS Firewall
- Análisis de Riesgos
- Continuidad de Negocio
- Formación
- Consultoría
- Evaluación de productos
- Cumplimiento

- Servicio **24x7x365**
- Certificado **ISO27001:2013**
- Acreditado **CERT** (Community Emergency Response Team)



# MEDIDAS, MÉTRICAS Y AUDITORÍA

- & El análisis de riesgos da como resultado una selección de controles
- & Establecer grados de implantación y medida de eficacia para cada control
- & Establecer el peso relativo en la reducción del riesgo
- & Chequear la reducción efectiva del riesgo
- & Repetir este proceso de manera periódica o cuando haya cambios significativos en la valoración de riesgos
- & Toma decisiones correctoras
- & Involucración de alta dirección
- & Preferentemente auditoría por auditor externo
- & Posibilidad de certificar el sistema



Secure&IT

www.secureit.es

# ¡MUCHAS GRACIAS!

**Francisco Valencia**

**Director General**
**Secure&IT**
**francisco.valencia@secureit.es**
**911 196 995**