La Ley 11... ¿J? (Junio de 2007)

EL CAMINO CON EL QUE ESPAÑA OBTENDRÍA UN "SOBRESALIENTE", ES EL DE ENROLAR TODA LA IMPLANTACIÓN DE LA LEY 11 A TRAVÉS DE UN PROCESO CONTINUO DE CERTIFICACIONES RECONOCIDAS INTERNACIONALMENTE

Alejandro Corletti

DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA

NCS

Os ruego de todo corazón que no mal interpretéis este título, pero también apelo al sentido común de todas las AAPP españolas, pues sinceramente, si no hacemos las cosas bien, estamos jugando con fuego.

No quiero ser tremendista, pero tampoco minimizar las cosas.

No deseo asustar, pero tampoco me gusta seguir viendo como avanzan algunos temas y que sus responsables sigan durmiendo tranquilos.

No quiero decir que la Ley no esté bien, sino todo lo contrario. Y justamente por ello es que deseo resaltar muchos aspectos que tal vez no se estén leyendo con el detalle que merecen.

En resumen no quiero que lo más importante de esta Ley (y que lo refleja con toda claridad), sea dejado en segundo término, en pos de "llegar a tiempo". **Lo más importante de esta Ley es y seguirá siendo la Seguridad** y, como veremos más adelante, lo dice a todas luces. Si no se interpreta así puede desencadenar en algún momento algo GRAVE, y tal vez mucho más grave de lo que en estos momentos o en estas líneas podemos presentar, y este sí es el verdadero mensaje.

Como militar que fui (cosa que uno lo lleva para toda la vida), no puedo dejar de plantearme todo proyecto

> En el caso de la seguridad informática se basa en muchísimos casos en tácticas y estrategias militares

con parámetros muy similares a los que llevé adelante la mitad de mi vida. En el caso de la seguridad informática, la verdad es que es muy fácil, pues tiene gran analogía y se basa en muchísimos casos en tácticas y estrategias militares. Es más, cuando iniciamos nuestra primera amistad con Internet y un grupo de gente, en el ámbito militar de mi País, cada paso dado fue planteado a través de lo que se llama "Secuencia de pasos para la toma de decisiones", que no es otra cosa que la experiencia militar de miles de años volcado a las operaciones bélicas. Esta secuencia, probada con amplia experiencia, no es nada menos que analizar y asesorar, por parte de la Plana Mayor, la cantidad de posibilidades que pueden ocurrir antes que el Comandante adopte su decisión sobre el "Curso de acción elegido". Todo este conjunto de tareas y acciones, se analizan desde el punto de vista de la propia tropa y del enemigo, y para ello existe el oficial (o grupo) de Operaciones y el de Inteligencia respectivamente, cada uno de ellos presenta sus puntos de vista de uno y otro lado del problema, es decir propio y enemigo. Como se puede esperar, no era tarea sencilla "abrir" las redes y sistemas militares al resto del mundo (para ese entonces era Jefe de Redes del Ejército Argentino). Con sus más y sus menos, el desafío se fue llevando a cabo. Lo importante y que deseo resaltar en este texto, **es que SIEMPRE se partió desde el punto de vista de la seguridad, para LUEGO de ver el cómo, seguir avanzando**.

Hasta aquí todo suena muy natural, pues cualquiera dirá que es

lógico que sea así en un ámbito militar, pues sus sistemas de información tienen datos estratégicos nacionales, de inteligencia, de seguridad de estado, de...

Hasta aquí cualquiera lo vería bien, pues se supone que los planes y acciones militares, desembocan en guerras, batallas, violencia...

Hasta aquí es lógico que un militar vele por la seguridad ante todo...

Hasta aquí es muy coherente que un militar no pueda ceder la información de sus sistemas, comunicaciones, redes, armamento... ¿personas?

Y si hasta ahora todo esto lo vemos de forma tan natural, ¿**por qué no es así con el 100 % de la información de la totalidad de los ciudadanos de una País? ¿No es acaso mucho más importante**?

La única explicación que le encuentro (y lo digo con toda sinceridad), es que se piense que el enemigo externo de un país guarda exclusiva relación con el ámbito militar. En este caso puntual, podría ser el "Ciberenemigo". Por esta razón es que quise plantear este "TÍTULO FUERTE", o es que acaso el Ciberterrorismo no es algo a tener en cuenta. Y ojo que no me refiero exclusivamente a países, ideologías, o fundamentalismos. Me refiero al peor de todos los enemigos actuales:

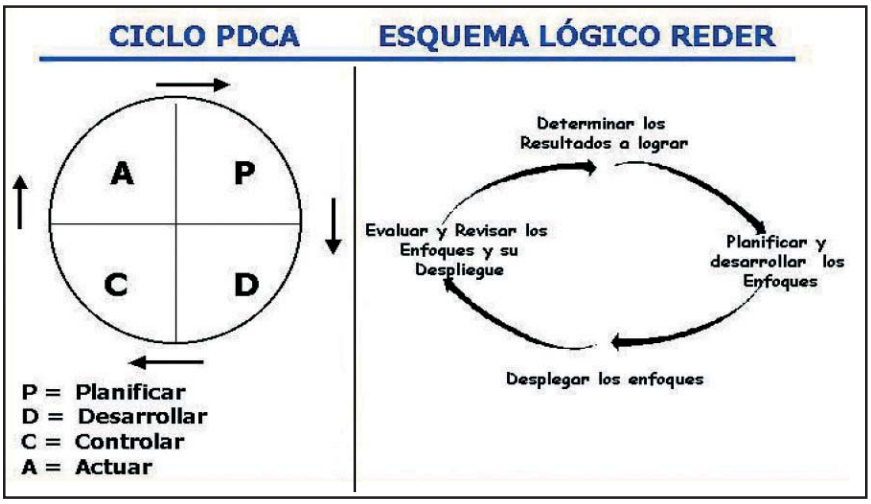
"Al ansia de dinero"

¿Alguien puede dudar que la información que contendrá dentro de unos años este proyecto de la "Ley 11", **valdrá tanto como para "quebrar un Estado"**? Nos encontraremos ante la mayor fuente de información que contendrá España. Nos encontraremos ante las bases de datos más "jugosas" de este País, nos encontramos con sistemas de información que "centralizarán", todos los datos necesarios como para poder derrocar al mejor aparato político que se pueda imaginar, para desautorizar a todo un Estado, para dejarlo fuera de la Unión Europea o la NATO. Si es "casi" inimaginable el poder que daría contar con el listado de usuarios de tarjetas VISA, o del banco "X", nos

> No deseo asustar, pero tampoco me gusta seguir viendo como avanzan algunos temas y que sus responsables sigan durmiendo tranquilos

podemos imaginar lo que reportaría obtener los del DNI electrónico, o de la Seguridad Social, exámenes médicos, o de propiedad de inmuebles, o rentas, o familiares (¿de mis hijos?), a fotos, planos catastrales, etc., etc., etc. ¿Cuánto dinero valdría esta información? Quiero dejar aquí latente la idea que ya no sólo es una patente cuestión de Ciberterrorismo, cosa que tal vez escribamos en otro momento pues aunque parezca de cuento, al igual que las brujas haberlas, haylas, y se tienen datos muy ciertos al respecto. Es eso y mucho más aún, es el blanco preferido de todo "malintencionado" de Internet (para el lado o bando que más se os ocurra), es el más perverso de los enemigos actuales "El ansia de dinero" (parezco Cruz y Raya... el anssiiiiiaaaaa).

¿Nos podemos imaginar el impacto que ocasionaría, **una vez que todo español haya confiado en el sistema**, que el mismo caiga en manos "indeseables"? ¿Cómo se recupera España de un hecho así? ¿Existe recuperación, o no tiene retorno? Tal vez el retorno pueda ser tan, pero tan costoso, que no se esté en condiciones de recuperación. El éxito más grande de una operación militar, es dejar al enemigo "Sin capacidad de reacción". Una acción de este tipo, hoy en día, sería mucha más exitosa que una operación bélica, que un atentado, y aquí es donde no podemos ser tan ilusos de no tenerla en cuenta. No se puede dejar de presentar un proyecto de esta envergadura como algo de "Seguridad Nacional", tanto o más importante que



el desarrollo de cualquier arma o acuerdo militar, y aquí es donde me atreví a remarcar este título **"Ley 11"... ¿J?** Junio está justo al medio de marzo y septiembre. Mil disculpas, pero quiero seguir destacando la importancia de esta Ley, no quiero que se sigan tomando medidas y acciones presupuestarias para "Llegar a término" como estoy viendo a diario, sin tener presente la SEGURIDAD en toda su extensión, tal cual lo menciona la ley en cada una de sus hojas. **Insisto, la seguridad es la base de esta Ley**, y tal vez, si los que podemos saber algo sobre este tema, no despertamos la atención de cada responsable de su implantación, estaremos siendo en parte responsables de esta omisión.

Si analizamos alguno de sus párrafos:

Comienza en la Exposición de motivos diciendo:

"Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. ***Depende de la confianza y seguridad que genere en los ciudadanos..."***

"El hecho de reconocer el derecho de los ciudadanos a comunicarse electrónicamente con la Administración plantea, en primer lugar, la necesidad de definir claramente la «sede» administrativa electrónica con la que se establecen las relaciones, promoviendo un ***régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad"***.

¿Alguien puede dudar que la información que contendrá dentro de unos años este proyecto de la "Ley 11", valdrá tanto como para "quebrar un Estado"?

El artículo 1. Objeto de la Ley, en el punto 2 sigue:

"Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, ***asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias"***.

Artículo 3. Finalidades de la Ley, en el punto 3 continúa.

"Crear las condiciones de confianza en el uso de los medios electrónicos, ***estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos"***.

Podríamos seguir así a lo largo de todo el texto, pues la Ley no deja de hacer mención a este tema. Por esta razón es que apoyo totalmente el contenido de esta Ley, y siendo tan rotunda en este tema, me cuesta entender, desde qué modelo se están iniciando muchas acciones al respecto.

Los dos únicos modelos a tener en cuenta deberían ser:

- Seguridad de los servicios de información
- Calidad de los servicios de información.

Para el primero de ellos, a esta altura del siglo ya no puede haber dudas que la referencia es ISO-27001, como lo venimos afirmando desde hace más de un año.

Para el segundo de ellos la metodología es CMMI o ITIL, que si se desea certificar, puede hacerse a través de ISO-20000, con lo cual se avanzaría de forma homogénea.

Cualquiera de estos modelos, propone resumidamente las siguientes piezas clave:

- Análisis de Riesgo
- Compromiso de todos los participantes
- Sistema de Gestión (que implica ciclo PDCA: Plan-Do-Check-Act)
- Controles y/o procesos
- Calidad.

Para ello también podría entrar en juego lo que hemos escrito en el artículo anterior, referido al Ministerio de Administraciones Públicas por

ISO-20000	ISO-27001	Modelo EFQM de Excelencia
6. Procesos para la provisión del servicio. **6.1.** Gestión del nivel del servicio **6.2.** Generación de informes de servicio **6.3.** Gestión de la continuidad y disponibilidad del servicio **6.4.** Elaboración de presupuesto y contabilidad de los servicios de TI **6.5.** Gestión de la capacidad **6.6.** Gestión de la Seguridad de la información **7.** Procesos de relaciones. **7.2.** Gestión relaciones con el negocio **7.3.** Gestión de suministradores **8.** Procesos de resolución. **8.2.** Gestión del incidente **8.3.** Gestión del problema **9.** Procesos de control. **9.1.** Gestión de configuración **9.2.** Gestión del cambio **10.** Proceso de entrega. **10.1.** Gestión de la entrega	**A.5** Política de seguridad **A.6** Organización de la información de seguridad **A.7** Administración de recursos **A.8** Seguridad de los RRHH **A.9** Seguridad física y del entorno **A.10** Administración de las comunicaciones y operaciones **A.11** Control de accesos **A.12** Adquisición de sistemas de información, desarrollo y mantenimiento **A.13** Administración de los incidentes de seguridad **A.14** Administración de la continuidad de negocio **A.15** Cumplimiento (legales, de estándares, técnicas y auditorías)	**Criterio 1.** Liderazgo **Criterio 2.** Política y Estrategia **Criterio 3.** Personas **Criterio 4.** Alianzas y Recursos **4a** Gestión de la información y del conocimiento **4b** Garantizar y mejorar la validez, integridad y seguridad de la información. **4c** Cultivar, desarrollar y proteger la propiedad **Criterio 5.** Procesos **5a** Diseño y gestión sistemática de los procesos Aplicar en la gestión de procesos estándares de sistemas **5.** La autoevaluación AAPP La autoevaluación debe formar parte del sistema de gestión de las organizaciones que la componen

medio de su **Agencia de Evaluación y Calidad** con sus Certificaciones del Nivel de Excelencia a través del "Modelo EFQM de Excelencia", el cual presenta el esquema lógico de REDER (Resultados-Enfoque-Despliegue-Evaluación y Revisión) como podemos apreciar en la imagen, tiene una analogía directa con el ciclo PDCA mencionado.

El camino con el que España obtendría un "**Sobresaliente**" y sería pionera en toda la UE, es el de enrolar toda la implantación de la Ley 11 a través de un proceso continuo de certificaciones **reconocidas internacionalmente**, que implica una inversión mínima respecto al gasto total. En resumen es lo que propone toda la legislación española y el MAP. En la actualidad todas las que proponemos poseen el nivel de madurez y consenso internacional como para que ofrezcan las mayores garantías.

> Tal vez el retorno pueda ser tan, pero tan costoso, que no se esté en condiciones de recuperación

A continuación se puede apreciar un cuadro resumen de tres métodos para abordar la "Ley 11", que son certificables y donde brevemente tratamos de presentar los aspectos comunes, relacionados a la seguridad en ambos extremos de la tabla (en rojo), que coinciden con los de la mayoría de los once grupos de control de ISO-27001 (al centro).

Desde esta visión fuertemente orientada hacia la seguridad que proponemos aquí, el punto de partida y los pasos a seguir para cada proceso a abarcar en el cumplimiento a la "Ley 11", debería ser: el Análisis de Riesgo, luego la elección de un curso de acción, el inicio de un SGSI (a través del ciclo PDCA), el avance paso a paso de cada subproceso, criterio y/o control, con lo cual una vez que empiece a estar maduro todo el desarrollo, se estaría en condiciones de presentarse para cualquiera de las tres certificaciones (ISO-27001, ISO-20000 y EFQM), con este panorama nos encontraríamos todos los ciudadanos españoles, **ante algo verdaderamente asombroso**, y de demostrada "Gestión de su Calidad" sustentada en una infraestructura Segura, donde finalmente las posibilidades de explotación indebidas quedarían mucho más acotadas de como vienen pintando en la actualidad.