GESTIÓN DE LA INSEGURIDAD: UNA VISIÓN DEL MODELO DE ANÁLISIS DE RIESGOS.

Introducción

Me gustaría comenzar esta comunicación con un breve chiste dirigido a los lectores. Es un chascarrillo muy viejo en los entornos de seguridad, el cual ya muchos conocerán:

"Pues se trata de unos amigos íntimos que han compartido los momentos más importantes de sus vidas, además de coincidir profesionalmente. De hecho son técnicos, expertos y responsables de valiosos sistemas de información es sus respectivas organizaciones.

Estos colegas se disponen a pasar unos días haciendo acampada libre, su pasión fuera del trabajo, la verdad, no es la primera vez y ya tienen bastante experiencia; son capaces de hacer las cosas de forma mecánica y no se molestan mucho en estudiar el terreno, en seguir las indicaciones o alguna guía de campo. De todas formas siempre se escuchan muchas tonterías sobre amenazas y riesgos ...

En definitiva, se lanzan a la aventura. Todo discurre como siempre, sin ningún sobresalto, hasta que una tarde..., mientras reposan una apetitosa comida que ha inundando de aromas el bosque (desoyendo las recomendaciones y todas las prohibiciones), oyen un terrible rugido. Salen sobresaltados y, a lo lejos, distinguen una figura peluda y enorme dirigiéndose hacia ellos: se trata de un gigantesco y hambriento oso.

En sus memorias se abre paso lo oído sobre esos peligros. Al unísono se lanzan a correr alocadamente. Tras unos minutos, uno de ellos, en medio de la carrera y con el oso cada vez más cerca, mira a los demás y casi sin resuello dice entre jadeos y ahogos:

- Es imposible,... no podemos... correr más.... que un oso... rabioso durante... mucho tiempo... "

Dejemos a nuestros expertos en T.I hasta el final de la comunicación, deseándoles buena suerte y comencemos por extraer algunas enseñanzas interesantes de la historieta. Sigamos en clave metafórica:

1. Los osos (riesgos, amenazas, vulnerabilidades) existen; aunque se quiera negar su realidad por la simple ignorancia.
2. Los osos normalmente, corren más que los excursionistas. Es difícil huir de ellos.
3. Las "guías de campon" (recomendaciones y buenas prácticas) tienen una razón de ser, normalmente se derivan, como lecturas positivas, de experiencias negativas de otros.

Abandonando el tono distendido, antes de plantear cualquier nueva alternativa, podría ser interesante bucear en la propia génesis del problema a tratar.

Sería muy fácil, pero no es nuestra intención, hacer una reflexión catártica sobre el panorama de la seguridad y elaborar una larga letanía de agravios, penas y dolencias.

Por el contrario, pretendemos sólo esbozar un paisaje a grandes pinceladas para plantear una posible estrategia.

Así, es factible identificar sencillamente algunas de las fisuras que determinan las debilidades y aquí hemos de establecer una necesaria dicotomía: las deficiencias con un origen meramente técnico y las organizativas. Veámoslas separadamente:

Debilidades Técnicas:

Síndrome del "**choque de futuro" y "rotación de conocimiento excesiva**". Se

manifiestan en la incapacidad de asumir los cambios tecnológicos en el sector, dada su excesiva celeridad. Son más rápidos que la posibilidad de absorción y asimilación del sustrato humano, y puede que se impongan tecnologías de producción inadecuadas sobre las que no es posible ejecutar convenientemente las labores de aseguramiento.

Se debería practicar una sana y controlada lentitud en la evolución de los medios y servicios posibilitantes de la Administración Electrónica. Un detalle, en las administraciones públicas ésto se agrava dada la rotación inevitable, hoy por hoy, existente en cuanto al personal funcionario.

La otra cara de la moneda es la "**fosilización de sistemas y hábitos**". Al contrario que el caso anterior, es también muy habitual mantener en producción aplicativos y servicios los cuales son imprescindibles pero se encuentra totalmente obsoletos, la vieja máxima de "Si funciona no lo toques" suele ser bastante acertada pero contiene en sí misma la semilla del desastre si no se sopesan sus implicaciones.

Pero esta petrificación puede detectarse aún más en el ámbtio de la Gestión del Servicio (soporte y provisión). Organizaciónes que todavía no han alcanzado una madurez suficiente para contar con una separación entre los diferentes elementos de gestión (incidentes, problemas, configuración, cambios, entrega) y que no siguen ningún patrón de buenas prácticas, son muy abundantes.

La ambigüedad en las funciones realizadas por los servicios de TI; no se corresponde, en muchos casos, con una adecuación de infraestructuras. Nos encontramos con CPD/CTI que dan servicio a una Lan de usuarios de micro y producción, y además, hacen publicación de aplicaciones. Evidentemente un error en cualquiera de los ámbitos puede comprometer el otro. En el perfil humano vemos técnicos en situaciones similares.

Debilidades de las Organizaciones:

Esnobismo tecnológico. Es innegable, aunque en este caso también puede no querer reconocerse, que la selección de soluciones tecnológicas, en muchos ocasiones no es resultado de un proceso serio, supervisado y dirigido por técnicos, pueden existir presiones y correcciones de rumbo sugeridas por proveedores, socios tecnológicos y otras fuentes incluso patrocinadas desde la cúspide de la pirámide organizativa. En definitiva, disponer de un Plan de Sistemas moderno, adecuado a la realidad tecnológica es importante, seguirlo vital.

La seguridad es una asignatura pendiente en el proceso de "alfabetización digital a ultranza" de los últimos años. Incluir esta entrada puede parecer un error pero debemos reflexionar acerca de como impacta acometer el aseguramiento "pese" a los usuarios, a los que se ha alfabetizado digitalmente a marchas forzadas sin ninguna educación en seguridad, o incluso a algunos técnicos que lo consideran un obstáculo. Obviamente, imponer medidas en este campo tiene la necesidad de conseguir su interiorización.

El "resultismo" a ultranza. El trabajo de los responsables y los técnicos en las administración públicas se encuentra mediatizado por cumplimientos de plazos y el obligado servicio al ciudadano. Todo ésto fuerza a poner en producción aplicativos no suficientemente maduros, no asegurados o que no han cumplido mínimamente el ciclo Desarrollo-Preproducción-Producción, ni han sido convenientemente auditados; todo ello cuando posiblemente el retraso proviene en la mayoría de los casos de áreas no técnicas.

De todo lo anterior se colige que la inseguridad es la punta del iceberg de un modelo tecnológico-organizativo erróneo. Gran parte nace de las situaciones preexistentes o sobrevenidas, además de mala praxis y de un crecimiento no sostenible.

Modelos de Aseguramiento (Tabla 1).

Una vez enunciadas algunas de las causas de este fenómeno, vamos a analizar la propia inoperancia de varios de los esquemas de aseguramiento actuales, para ello es necesario saber en qué contexto se encuentran inmersos, cuál es el ecosistema tecnológico extremo en el que se insertan.

La afirmación comúnmente admitida entre los expertos en este campo de que nos encontramos ante un nuevo horizonte es totalmente falsa. No existe un solo panorama sino una realidad poliédrica y mutante. Que el cibercrimen, el cibervandalismo y terrorismo electrónico están creciendo, es evidente y alarmante ; que esta amenaza "ciberpunk" supone un gran peligro externo también y por supuesto uno de los retos en ciernes del siglo XXI contra los estados y su modernización digital. Pero hay que tener algo muy claro, en organizaciones tan amplias y complejas como las nuestras hay que contemplar distintas fuentes de riesgo como las arriba enunciadas u otras como la permeabilidad que suponen los nuevos servicios y los dispositivos hipermóviles.

Pero nuestros escenarios de quiebras, no tienen por que ser tan "mediáticos" - aunque algunos lo han sido - pero si tener, incluso, mayor impacto real sobre el ciudadano. No olvidemos ésto, la Administración Electrónica y en general cualquier servicio digital que las distintas instituciones presten al público son, en la mayoría de las ocurrencias la materialización de derechos y deberes. Si entendemos la seguridad como la expresión de sus diversas dimensiones (disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad) y su ruptura, el decaimiento de cualquiera de ellas, una denegación de servicio en sistemas tan complejos puede provenir de simples errores de configuración o mal dimensionamiento de recursos; la revelación de información crítica, de cambios realizados sin tener en cuenta sus componentes de protección, la pérdida de trazabilidad fruto de la eliminación de alguna función no convenientemente documentada o cualquiera de ellos originarse por una crisis de seguridad interna.

Los distintos modelos a continuación descritos son ideales y en el mundo real encontramos situaciones híbridas; y más que valorar la taxonomía o el despliegue técnico, intentamos identificar el nivel de madurez colectiva de todos los agentes respecto al papel jugado por los procesos de aseguramiento.

Primero. "Ciudad amurallada / ametódico"

Se disponen defensas perimetrales adecuadamente trazadas y reconocibles, sobre las que se deposita, casi místicamente, toda la confianza de la organización. Suele desestimarse el análisis de riesgos de elementos internos. Normalmente no existe ningún método a la hora de acometer las tareas y la seguridad se concibe más como un obstáculo que como un coadyuvante..

Afortunadamente, hoy se encuentran en franca desaparición, no obstante se mantienen restos muy vivos. Un botón de muestra: No se parchean servidores ni servicios pues supone una necesidad de reinicio y una incertidumbre a la hora de retomar el trabajo o se mantiene la identificación de usuarios de administración sin cambios de claves por idénticos motivos, se suspende el uso de antivirus en determinados usuarios, pues los penaliza en sus quehaceres. Muchas organizaciones dedican todos sus esfuerzos en los Cortafuegos, IDS, Appliances... y no mantienen una visión global. Se profesionaliza la gestión de estos "Glacis" defensivos, pero, por su propia naturaleza, nunca pueden llegar a ser elementos vertebradores en el gobierno de T.I .

Segundo. "Ciudad patrullada".

Se trata de un modelo más moderno, suele existir una rudimentaria gestión de riesgos .

Este tipo anuncia formas más completas, pero aún carece de un concepto de "totalidad" pues no llega a constituirse la seguridad bajo la premisa de "Por Defecto" y en el seno de la organización no se ha alcanzado la madurez que permite reconocer en estos procesos el camino conductor hacia casos de éxito.

En muchas ocasiones, puede provenir de algún mal acontecimiento de gran resonancia (real o en los medios de comunicación) padecido por la institución y suele acabar con la asfixia sobre los usuarios finales.

Tercero. "Análisis de riesgo".

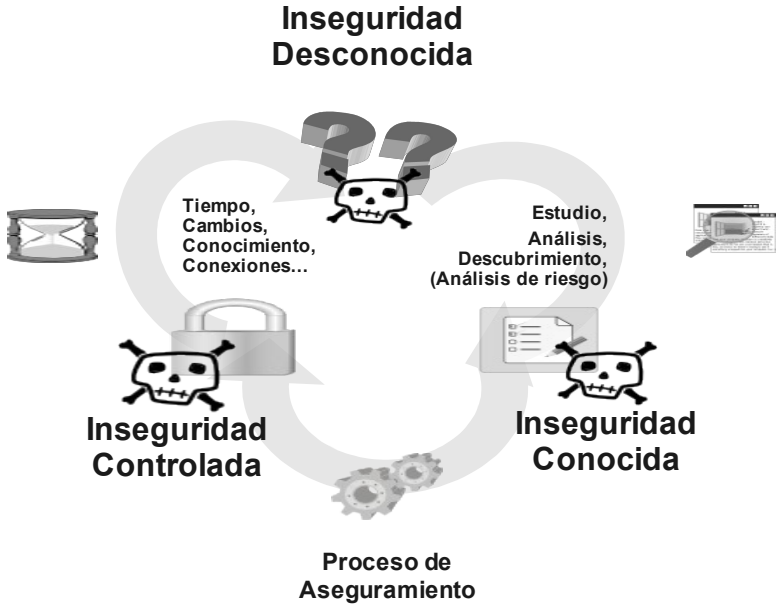
Es él más actual y moderno. Su núcleo es el mismo concepto de riesgo, su estudio y valoración. A partir de aquí se aplican todas las medidas. Existe todo un corpus teórico-práctico en forma de estándares internacionales y Buenas Prácticas aceptadas. Es inviable si no existe una implicación de la dirección

Es un modelo de éxito. Su talón de Aquiles radica en la excesiva "aceptación formal" que puede derivar en la sobrevaloración exclusiva de las "certificaciones" como mecanismo de seguridad. Lamentablemente se suele seguir considerando un lastre, incluso por sectores técnicos, las actuaciones de aseguramiento; en lugar de un principio rector.

Cuatro. "Gestión de la Inseguridad"

Ahora nos atrevemos a proponer un enfoque particular sobre el modelo que nos parece más válido, "Análisis del Riesgo", que llamaremos "Gestión de la Inseguridad y su conocimiento". Que parta del reconocimiento de los problemas como causados, en muchas ocasiones, por debilidades estructurales-organizativas, persiga transformar la seguridad en un principio rector y se fundamente en las métricas del binoimio inseguridad / seguridad, sus controles y el conocimiento de los sistemas y especialmente sus debilidades.

Sería interesante examinar el ciclo en que se basa esta perspectiva. Con una naturaleza recursiva, se inicia en un estado de "Inseguridad No Conocida", aplicándole un proceso de análisis e investigación se eleva a otro estado de "Inseguridad Conocida" que permitirá mediante las tareas de aseguramiento alcanzar otro de "Inseguridad Controlada", evidentemente los cambios en el propio sistema con el paso del tiempo, la evolución del conocimiento del mismo o las interconexiones acarrean, de nuevo, el retorno al momento inicial del ciclo.



Ciclo de Gestión de la Inseguridad

Tabla 1: Tipología de Modelos de Aseguramiento

CARACTERÍSTICAS / **MODELO**	**Ametódico\Amurallado**	**Patrullado**	**Análisis del Riesgo**	**Gestión de la Inseguridad**
Las soluciones de seguridad aplicadas son , básicamente, desatendidas.	x	x		
Es un objetivo fundamental del proceso asegurador el obtener una certificación.			x	
La seguridad llega a entenderse como un elemento vertebrador y principal, no un obstáculo.				x
Se utiliza algún método recursivo a la hora de acometer las tareas de aseguramiento.			x	x
Existe compromiso activo y no solo formal por parte de la Dirección.			x	x
Existe un entorno multicapa para la segurida interior.		x	x	x
Existen defensas perimetrales.	x	x	x	x
Existe análisis y Gestión de Riesgos.			x	x
Existe una dedicación de recursos suficiente.			x	x
Las soluciones de seguridad se fudamentan sobre un equipo humano y profesional .			x	x
Se planifica el trabajo a acometer en los diversos niveles: Operacional, Táctico, Estratégico y de Control.			x	x
La seguridad se entiende como un proceso, no como un producto.			x	x
Existe un principio de "Reevaluación Periódica" plasmado en una formula espiral de trabajo a la hora de construir un SGSI.			x	x
Existe una Evaluación de Seguridad en las adquisiciones de Software y Hardware.			x	x
Existen esquemas, protocolos y organismos para respuesta a incidentes de seguridad. Se practican, comprueban y realizan simulacros al respecto.			x	x
Se opta por una adecuada combinación entre software propietario y de código abierto, por pincipio				x
Se contemplan dinámicamente nuevos posibles "Nichos de Inseguridad" para la organización (nuevos dispositivos móviles p.e.)				x
Se entiende la implantación de aseguramiento como la superación de un modelo tecnológico-organizativo erróneo.				x
Se establece la seguridad como una función diferenciada y no comprometida con otras áreas.				x
Se contempla seguridad "en Origen".				x
Existe un principio de cooperación coordinada entre todos los elementos de la organización a la que el organismo pertenece.				x
Existen modelos de trabajo y buenas prácticas que garantizan la concentración de esfuerzos y no su dispersión en materia de seguridad.				x
Se entiende que el principal esfuerzo es la formación y concienciación y cualquier actuación, tanto técnica como organizativa, debe contemplar este aspecto y redundar en ese sentido.				x
Se cuenta con métricas del nivel de inseguridad para conocer la situación y dirigir los esfuerzos con efectividad y además mecanismos de seguimiento de los trabajos y su cumplimiento.				x

Características de la vista "Gestión de la Inseguridad".

Las principales características añadidas en esta vista son:

Enriquecimiento mediante herramientas y procedimientos de gestión, **del principio de seguridad en origen**. Aseguramiento desde la idea y uso de marcos de desarrollo seguros. Basta con repasar la larga serie de sitios de Internet infectados o con graves vulnerabilidades de diseño o implementación técnica, más aún cuando suele tratarse de "errores de libro" ampliamente estudiados, y solucionados.

Es importante introducir aquí alguna reflexión más a cerca de procesos de desarrollo actuales, los cuales insisto, obvian cualquier trabajo de aseguramiento por una supuesta carga económica e ineficiencia. Creemos necesaria un directiva básica para las administraciones pública.

En este mismo ámbito, una pequeña reseña más, se hace muy necesario incrementar la agilidad para atender cualquier incidencias / sugerencia sobre seguridad proveniente de la comunidad de usuarios de los servicios públicos, episodios de bugs, agujeros y debilidades manifiestas reportados a la administración y no corregidas, son lamentablemente muy usuales.

Reconocimiento de la gestión humana como valor añadido y escapar de la panacea de "Seguridad Enlatada". Este parece un corolario bastante obvio tras lo dicho hasta ahora y ha de ser una de las columnas sustentadoras de toda la administración del proceso.

La profesionalización estricta, acompañada de una formación que, por supuesto, debe ser complementaria a la titulación académica (certificaciones serias de fabricantes, especialización y actualización continua...), con soporte sobre un correcto tratamiento del conocimiento y la documentación.

Desde luego es imprescindible usar y explotar la "inteligencia enlatada" en cualquiera de las vertientes ofrecidas por la industria pero no perder una sana actitud de "duda metódica" acerca de los productos que se contratan y explotan, como por otra parte la experiencia y los últimos acontecimientos refrendan.

Cooperación a niveles internos y externos. Es posible ofrecer un frente suficientemente coherente para esta situación. Ejemplos recientes de cooperación dentro del seno de la propia industria (caso Kaminsky-DNS) son importantes. Iniciativas autoorganizadoras, por ejemplo, CNCC son un paso muy interesante.

Hemos de aceptar una máxima más: **el riesgo de uno es él de todos**. No podemos seguir entendiendo nuestros esfuerzos como aislados, debemos generar sinergias fruto de los mismos, considerarlos una malla para protegernos por igual y que propicie el intercambio de conocimiento y experiencia. Me gustaría hacer mención especial de la administración a la que pertenezco, la Junta de Andalucía que lleva varios años con proyectos en esta dirección y actualmente ultima un Plan Director de Seguridad de los Sistemas de Información y Telecomunicaciones.

Convertir en principio la "Gestión del Riesgo", y poner en marcha métricas de inseguridad.

La motivación para intentar medirla es evidente: a) Huir de lecturas positivas y triunfalistas enmascaradoras de problemáticas sustanciales. b) Generar documentación y estadísticas fácilmente escalables, explicables y que no induzcan a confusión. c) Poder adecuar los recursos disponibles y utilizar herramientas y métricas adecuadas. d) Obtener inmediatamente líneas de trabajo y de actuación para seguir. Es fundamental en este punto disponer de herramientas y medidas que nos proporcionen los datos necesarios. Contar, por

ejemplo, con una matriz de inseguridad (Tabla 3) donde se enumeren y se haga seguimiento de los principales ítem elegidos; estadísticas de cumplimiento de metas tales que controles seleccionados pertenecientes a la ISO27002 implantados o relación de aplicaciones aseguradas con diversos aspectos, por ejemplo, números de horas dedicadas a la auditoría, o cambios sustanciales que hacen necesario reexaminarlas; asociándoles una magnitud de riesgo (Tabla 2).

Tabla 2: Ejemplo simple de cálculo de inseguridad en aplicaciones		
Nombre de la Aplicación: **Identificativo:** **Fecha de revisión:** **Magnitud de riesgo asociado:**		
Nº Item	**Item de aseguramiento**	**r (1/0)**
1	¿La aplicación respeta el Plan de Arquitectura ?	
2	Si no respecta no lo respeta, ¿Su implantación ha sido asegurada?	
3	¿La aplicación cumple el principio de "Aseguramiento en Origen"?	
4	¿Están asegurados individualmente, los diferentes activos que componen la cadena de producción del aplicativo?	
5	¿Ha sufrido un procedimiento de comprobación y aseguramiento documentado en el ciclo de Desarrollo-Preproducción-Produción ?	
6	¿Se ha auditado externamente en alguna ocasión?	
7	Si se cumple 6, ¿Se han dedicado más de 120 horas y un auditor técnico conocido y contrastado?	
8	Si se cumple 7 ¿Se ha realizado alguna otra auditoría del producto, interna o externa, en los últimos 18 meses ?	
9	¿Está sometido a un plan de análisis mediante herramientas automáticas?	
10	¿El acceso a la aplicación es mediante certificado digital ?	
11	¿Es exclusivamente interno a la organización su ámbito de uso?	
12	¿NO hay reportados incidentes graves de seguridad asociados a las tecnologías usadas?	
13	¿Podemos considerar como NO obsoletas las tecnologías que usa?	
14	¿Se han realizado y registrado convenientemente correcciones en los sistemas resultado de los items anteriores?	
15	¿ Se ha vuelto a comprobar, acto seguido, mediante auditoría; la solidez de las soluciones propuestas para las vulnerabilidades y debilidades encontradas ?	
16	¿Se ha informado, mediante reunión y acta posterior a los responsables técnicos, funcionales y a los órganos competentes de las deficiencias en seguridad y vulnerabilidades encontradas ?	
17	¿Existe algún tipo de análisis de riesgos asociado al aplicativo ?	
18	¿ La aplicación gestiona información de naturaleza **EXCLUSIVAMENTE NO crítica, NO confidencial, NO estratégica o NO protegida por la LOPD** ?	
19	¿La aplicación cuenta con las salvaguardias convenientes y un plan de puesta en marcha en caso de desastre si es requerido ?	
20	¿Se cuenta con información técnica suficiente sobre la misma ?	
Mi= Magnitud de Inseguridad (Mínima -1, Máxima -21)		**Σr**
Magnitud total de inseguridad identificada a la fecha:		**Mi =(Σr - 21)**

Tabla 3: Ejemplo simple Matriz de Inseguridad

MÉTRICA	Fecha 1	Fecha 2	Tendencia 1	Fecha 3	Fecha 4	Tendencia 2
Número de estaciones de trabajo SIN ANTIVIRUS o NO completamente operativo.						
Número de Servidores SIN ANTIVIRUS o NO completamente operativo.						
Número de servidores SIN PARCHEO actualizado.						
Número de aplicaciones a disposición del usuario externos SIN AUDITAR.						
Número de Estaciones de Trabajo SIN MECANISMO de parcheo.						
Número de portátiles SIN REVISIÓN periódica.						
Número de estaciones SIN USB almacenamiento desactivados.						
Número de usuarios SIN PROXY.						
Número de virus "in the wild" encontrados.						
Número de CORREOS INFECTADOS detectados.						
Número de INFECCIONES TOTALES ocurridos						
Número de CUALQUIER OTRO INCIDENTE de seguridad detectado distinto a los anteriores.						
Numero de HORAS DE TRABAJO dedicadas a situaciones de malware.						
Número de Reglas en el cortafuegos de "PASO FRANCO"						
Número de intentos deINTRUSIONES detectadas, verificadas y comprobadas (IDS).						
Número de Controles de la ISO 27002, seleccionados y no implementados.						
Número de PORTÁTILES EXTERNOS INGRESADOS en la red sin controlar						
Número de usuarios con CUENTAS EXTERNAS de correo.						
Número de Aplicativos de cara al Exterior que NO CUENTAN con un sistema que asegure la continuidad de la actividad en caso de crisis.						
Número de Sistemas con INFORMACIÓN CRÍTICA O SENSIBLE no asegurados.						
Número de Sistemas de Información de cara al exterior que NO CUENTAN CON gestión y análisis de riesgos INDEPENDIENTE.						
Número de Activos cuya MAGNITUD DE RIESGO no se han visto mitigada en la última iteración del SGSI.						
Número de PLANES DE ANÁLISIS DE VULNERABILIDADES Y AMENAZAS, consensuados que no se han realizado en el periodo indicado.						
Número de INTERCONEXIONES CON OTROS SISTEMAS DE INFORMACIÓN NO ASEGURADAS que existen.						

	Nº tendencias negatvias	Nº item alarmantes	Nº Crisis asociadas a algún item	Nº de Alertas decretadas	Nº de actuaciones (órdenes e incidencias) del área de seguridad.
Observaciones en la Tendencia 1					
Observaciones en la Tendencia 2					
Observaciones en la Tendencia n					

Se deben definir **modelos de trabajo**, o acogernos a algunos de los ya contrastados, para permitir la concentración y no disipación de los esfuerzos (utilizar para el plazo inmediato órdenes y cambios, a corto plazo -3 ó 4 meses- planes de actuación y a medio y largo, proyectos), y por añadido controlar la misma naturaleza de inducción entrópica de cualquier actuación de aseguramiento, aquí vuelve a hacer útil el uso de ITIL en cuanto a la gestión de cambio, configuración, incidentes y problemas.

Constituir el **conocimiento de los sistemas de información** y sobre todo los aspectos relacionados con su continuidad y defensa en verdadera piedra angular. Detectar y atender todos los posibles nichos de riesgos y peligros nuevos o preexistentes en la organización, por ejemplo, los elementos de ultramovilidad que pueden quebrar todas las medidas de aseguramiento existentes.

En este punto nos permitimos una breve referencia al **uso de software libre** para todas las herramientas utilizadas en este ambiente. En ningún momento estamos suponiendo que los productos de fuente abierta son más seguros, sí planteamos que ofrecen un nivel mayor de profundidad en cuando a su conocimiento y flexibilidad además de una posibilidad de ahorro en licencias que puede revertir en activos humanos.

Debe ser un objetivo perseguir el estado mental ya mencionado de **considerar los esfuerzos en aseguramiento, principios rectores**. Esto pasa, lógicamente, por dos líneas: formación y concienciación. Evidentemente estas actividades han de alcanzar a todos los estratos de la organización, incluso individualizadamente si es necesario, y principalmente deben ser los propios técnicos, expertos en T.I y altos responsables quienes han de dejar de considerar un calvario a su quehacer diario sólo por asumir las misiones de aseguramiento.

Insistamos en que cualquier tarea de formación debe estar imbricada completamente en todos los planes a materializar, técnicos y de cualquier tipo; en definitiva ser conscientes, como algunos expertos indican, de que la pila OSI no termina en el nivel 7, sino alcanza uno más, el 8, el técnico o usuario final.

Para finalizar, el primer paso para solucionar un problema es reconocerlo, y por ahí deberíamos de empezar todos. **Identificar la seguridad no sólo para cumplimiento de una legislación , si no llegar a entenderla y hacerla entender como nuevo hecho cultural para los que intervienen en T.I .**

Un buen ejemplo a seguir, sería la incipiente extensión del uso de "Buenas Prácticas" por los técnicos y gestores del sector que ha permitido en forma de casos de éxito la continuidad y supervivencia de muchos entornos TI, los cuales de otra forma, seguro, se hubieran colapsado.

Esquema Nacional de Seguridad

No quisiera terminar esta comunicación sin dedicarle algunas líneas al Esquema Nacional de Seguridad (El Real Decreto 3/2010, de 8 de enero -BOE de 29 de enero-). Brevemente; me parece un hito de una importancia histórica para la Administración Española.

El conseguir superar el cómodo estatus de "aconsejable marco de referencia" que suponen los estándares internacionales y alcanzar el de obligación legal, supone un antes y un después. A su favor sólo comentar la simplicidad y claridad propuesta para el cálculo de riesgos (amén de la obligatoriedad del mismo), la introducción del concepto de "Seguridad por Defecto" o la profesionalización e individualización de la función de aseguramiento en las organizaciones. Creo que supondrá para todos nosotros el impulso necesario para alcanzar los modelos más avanzados.

En resumen, me parece una gran "guía de campo" la cual les habría venido muy bien a nuestros amigos excursionista. Echemos un vistazo a ver que tal les ha ido a los intrépidos

aventureros:

"El oso, con sus fauces abiertas, se acerca cada vez más amenazante. Todos se miran de reojo y de repente se ven conscientes de lo que se les viene encima. No obstante sin parar de correr otro dice:

– No,... no puedo... correr más que... un oso rabioso... pero tengo... bastante con correr... más que el resto.... de vosotros."

Bueno, confiar que la inseguridad de los demás cubra y ampare las vulnerabilidades y debilidades propias, también es un modelo que hemos olvidado incluir arriba y nos parece que está muy extendido.