Asociación Española de empresas de Seguridad

Dinamizando la Industria de la Seguridad

Boletín Informativo

Número 54 - Junio 2015

Espías vs Inteligencia

Security Forum 2015

Planes Compliance penal en la empresa

Adopta el Cloud en toda confianza

La Seguridad Privada celebra su Día Nacional

Espías vs Inteligencia

Antonio Ávila Chuliá

El que espía escucha lo que le desagrada.
Proverbio árabe.

Desde tiempos inmemoriales los humanos necesitaron subsistir seguros, la avaricia, codicia o envidia fueron la principal causa de fisgonear en vida ajena, husmeando para conocer los triunfos, fracasos e incluso las desgracias de los demás. El espionaje, aunque hoy se le acicale con el término "inteligencia", constituye parte importante en el devenir del ser humano, baste citar que el servicio secreto de Filipo fue muy eficaz y profesional, tanto como singular el ejército macedonio; Alejandro estaba al corriente de las cualidades de los sátrapas, sabía a quién podía nombrar administrador y a quien no. Su conocimiento de los persas, cartagineses y atenienses era lo bastante preciso como para poder nominar los hombres más apropiados para ofrecerles un soborno o algo similar.

En el supuesto de descender a la terrenal vida cotidiana, resulta sencillo percatarse cómo los vecinos colindantes de los campos en producción se curiosean entre sí, contemplan las plantaciones, las cosechas e incluso los métodos de cultivo para poder comparar con la propia; tres cuartos de lo mismo sucede en la mar, allí se repara en el barco que mayor número de capturas logra pues de ello depende el bienestar de las familias, de la tripulación y de los dueños de la embarcación; lo propio pasa en el mundo empresarial, todos nos vigilamos para aprender del genial triunfador en los duros mercados. Saber para vencer ha sido y es la máxima de cualquier gobernante, así como de los ejércitos de la totalidad de los pueblos de la tierra.

Los individuos, desde el origen de los tiempos pretenden consolidar el futuro de sus respectivos países para mejorar el de sus hogares, ante el miedo a lo incógnito, por ello no produce extrañeza en el común de las gentes que atesorar propiedades, riquezas al fin, se convierta en una obsesión compulsiva, por ser un modo de sobrevivir al futuro. Esta nociva concepción afecta por igual al conjunto de los sectores de la población, empresas, empresarios, instituciones, políticos, gobernantes, personalidades del mundo financiero, del deporte o la cultura. No debe sorprender que el espionaje sea o fuese parte importante del ser humano, pues estar al corriente de lo que hace y dice nuestro contrincante o amigo da una ventaja indiscutible así como cierta satisfacción a algún oscuro deseo.

Boletín Informativo de AES
Revista Trimestral - Junio 2015 - núm. 54

Edita:
Asociación Española de Empresas de Seguridad
C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225 - Fax 915 766 094
www.aesseguridad.es - aes@aesseguridad.es

Consejo de Redacción:
Antonio Escamilla Recio
Julio Pérez Carreño
Antonio Pérez Turró
Francisco Ramos Moreno
Javier Ruiz Gil
Manuel Sánchez Gómez-Merelo

Coordina:
Paloma Velasco Merino

Diseño, Maquetación y Realización:
ERRE comunicación
www.erre-comunicacion.es

Junta Directiva de AES

Presidente:	D. Antonio Pérez Turró	Fichet Industria
Vicepresidente:	D. Antonio Escamilla Recio	Bosch Security Systems
Presidente Honorífico:	D. Antonio Ávila	A. Consulting
Secretario:	D. Julio Pérez Carreño	Eulen Seguridad
Tesorero:	D. Francisco Ramos Moreno	Cersa Seguridad
Vocales:	D. Javier Ruiz Gil	Baussa
	D. Manuel Escandón	Securitas
	D. Miguel Gutiérrez	Segurcontrol
	D. Manuel Sánchez Gómez-Merelo	Estudios Técnicos
	D. Darío Vicario Ramírez	Gunnebo España
	D. Luis Miguel Salinas	Honeywell Security
	D .Íñigo Ugalde Blanco	Intertrade
	D. Óscar Téllez	Stanley Security Solutions
	D. Eduardo Mata Lorenzo	Tecnoexpress
	D. Jorge Afonso	UTC Fire&Security
Directora Ejecutiva:	Dª. Paloma Velasco Merino	

Si volvemos la mirada hacia la historia ella nos revela que en la antigua Roma los principales políticos sostenían su propia red de vigilancia, la cual proveía de la oportuna información, de tal modo es así que en los escritos de Julio Cesar consta como el gran estratega poseía su servicio de informadores que lo mantenían al tanto de las intrigas y complots, aunque algo debió fallar cuando su propio hijo Bruto junto con otros conspiradores acabaron con su vida sin que la traición fuese detectada, quizás porque dejase en el cajón del olvido que jamás se conoce la realidad si te cuidan o espían.

"No debe sorprender que el espionaje sea o fuese parte importante del ser humano

Muchos empresarios, creadores, industriales, fabricantes importantes no conciben los graves riesgos que contraen si son escrutados, investigados, vigilados, pues aunque los métodos cambien la intención persiste; es difícil que las compañías subsistan al saqueo o sustracción de las tecnologías que tantos años de trabajo y esfuerzo costaron. Miles de firmas viven con esa amenaza ignorantes de ello, solo cuando las ventas decrecen, desaparecen los beneficios por la competencia desleal en los precios, es cuando los ejecutivos y empresarios demasiado tarde comprueban que han sido desvalijados, tanto en su información confidencial de datos como en los procesos productivos de la empresa, pese a contar con una seguridad que no ha detectado la intrusión

Son muchas las horas invertidas por los creativos en idear nuevos métodos de producción, novedosos productos o servicios a base de innovación con el fin de insuflar a la empresa aires vivificadores que permitan su continuidad unos años más en el negocio, eso sí, merced a los beneficios y con el pensamiento puesto en que el esfuerzo en el trabajo obtendrá su premio al diferenciarse de la competencia, sin olvidar que para minimizar el riesgo es útil acompañar a la idea en su crecimiento. Jeffry Timmons sugiere la búsqueda de información capaz de responder a interrogantes con respecto a tres temas fundamentales: la oportunidad, los recursos y el equipo.

Estamos inmersos en continuos cambios en cuanto a los avances tecnológicos en los cuales algunos jóvenes superan a las veteranas generaciones desbordadas ante tanto progreso, si bien creo que frente al espionaje industrial a la juventud le falta conocer muchos de los peligros que les acechan, tan viejos como el propio mundo, pues en el espionaje corporativo las mismas personas son los riesgos directos por tener acceso a la información confidencial, es decir, la mal llamada "inteligencia corporativa", en verdad espías de pago que ofrecen información privilegiada. Prestemos la debida atención con respecto a la seguridad de la información y el almacenamiento correcto de los datos, para no tener que sufrir las consecuencias. Joseph Shumpeter sugiere que el primer obstáculo del emprendedor o innovador es la incertidumbre.

El soborno es el modo de corromper al custodio responsable del saber que a cambio de dinero vende el conocimiento protegido durante años. Nadie duda de la existencia de los ejecutivos infieles que comercian con las técnicas capaces de sustraer información de otras personas, las cuales tienen como base la interacción social sin que la víctima sea consciente de ello; se manipula a un administrador de redes de un departamento de sistemas para que facilite datos tanto del inicio como de autentificación para obtener el acceso a las informaciones.

La necesidad de saber ha ido estrechamente unida al desarrollo de la civilización, el espionaje ha singularizado las guerras su desarrollo imprimió la historia. Concluyo, en un mercado competitivo como el nuestro la información es un bien impagable, atentos, el espionaje industrial no está condenado a desaparecer más bien al contrario ha de acrecentar su presencia de manera considerable en el futuro; no dejemos de lado que un oportuno informe es capaz de desbaratar la conspiración mejor planeada así como de destruir al enemigo más temible o hacer retroceder una mala decisión.

Más de 5.500 visitantes en la III edición de Security Forum

La tercera edición de Security Forum, la mayor tanto en número de expositores como de visitantes, tuvo lugar los días 27 y 28 de mayo en Barcelona.

5.512 visitantes, un 37% más que en la edición anterior, 245 congresistas acreditados para Diálogos Security Forum y 73 expositores.

Todos ellos han confirmado y avalado el éxito de este evento que ha reunido, durante dos días, a todo el sector de la seguridad en el CCIB de Barcelona, consolidando a Security Forum como punto de encuentro y referencia en el sector.

En la inauguración de los Diálogos, que este año tenían como lema “Comparte la energía. Renueva tus ideas”, el presidente del Security Forum, Eduard Zamora, expresó su satisfacción al ver cómo el evento se puede considerar consolidado, después de superar su 2ª edición. El Security Forum, explicó, gira en 4 ejes: el negocio, el conocimiento, el networking y la innovación.

Se celebraron los 300 números de Cuadernos de Seguridad.

Por su parte, Ignacio Rojas, Director General de Ediciones Peldaño, explicó que el objetivo del evento era compartir ideas en este sector que nos une. Churchill decía que el precio de la grandeza es la responsabilidad, y lo que esperaban era no defraudar la confianza y las expectativas de los asistentes y participantes en el Security Forum.

Lo consideran una plataforma de negocio, abierto al mercado internacional. La seguridad privada es una industria dinámica e innovadora. Como bien decía Kofi Annan, la seguridad se entiende cada vez más como la ausencia de conflictos, y es lo que quiere transmitir la seguridad privada.

María de los Llanos de Luna, Delegada del Gobierno en Cataluña, destacó el extraordinario desarrollo de la Seguridad Privada en España en los últimos años y su gran importancia desde el punto de vista económico y laboral. Es, además un actor fundamental en políticas globales y nacionales de seguridad.

La nueva ley, que cumplirá un año de vigencia el próximo mes, ha introducido medidas que permiten su avance e impulso.

Especial relevancia tuvo la conferencia titulada “Legislación de Seguridad Privada: un año después. El nuevo reglamento de Seguridad Privada”. En la misma, diferentes representantes de las Fuerzas y Cuerpos de Seguridad, Policía Nacional, Guardia Civil, Mossos d' Esquadra y Ertzaintza, abordaron el interesante tema de nuestra legislación en materia de Seguridad Privada.

Manuel Yanguas, Comisario Jefe de la Brigada Central de Empresas y Personal de la Unidad Central de Seguridad Privada de la Policía Nacional, explicó que a 31 de diciembre de 2014 estaban registradas 1535 empresas de seguridad, lo que supone un 2,6% de incremento sobre 2013. De ellas, 1227 son de instalación y mantenimiento y 156 centrales receptoras de alarmas.

Sobre el nuevo reglamento avanzó que está prácticamente terminado. Se está dando forma al texto. Consta de un preámbulo, 10 títulos y 390 artículos, en los que se han intentado recoger todas las aportaciones de la industria.

El Coronel Jefe del Seprose, César Álvarez, quiso destacar el potencial del guarda de seguridad, como figura más antigua de la Seguridad Privada en España, que data de 1859 con la creación de los guardas de campo. En la actualidad hay muchos bienes a proteger en los campos, afirmó.

Carles Castellano, Jefe de la UCSP de Mossos d' Esquadra, señaló que la nueva ley había significado una simplificación burocrática, como ejemplo, la validación de las medidas de seguridad por parte del director de seguridad. Además se deja bien patente la complementariedad entre la seguridad privada y la pública, como por ejemplo en la vigilancia de los espacios públicos bajo la supervisión de las Fuerzas y Cuerpos de Seguridad.

También destacó la protección jurídica del personal de Seguridad Privada como agente de la autoridad.

(continúa en página 5)

Francisco Llaneza, Jefe de la USP de la Ertzaintza, avanzó el plan de colaboración con la Seguridad Privada, plan Lagundu (ayudar, cooperar, en euskera). Han empezado a trabajar con los centros de formación y los despachos de detectives a raíz de la nueva ley.

El Secretario General Técnico, Juan Antonio Puigserver, explicó que aún falta tiempo para la publicación del Reglamento, ya que quedan muchos trámites complicados por el proceso electoral de finales de año. Por su experiencia, antes de las elecciones no se publicará.

Los ministerios implicados en la tramitación del mismo son los siguientes: Hacienda y Administraciones Públicas, Economía y Competitividad, Educación, Empleo y Seguridad Social, Agricultura, Asuntos Exteriores y Cooperación. Además está implicado todo el sector, las Comunidades Autónomas (en especial País Vasco y Cataluña), y diferentes órganos consultivos del Ministerio de Economía, la Comisión Nacional de Seguridad Privada y el Consejo de Estado.

Por ello, no se puede decir con exactitud los meses que quedan, pero el proceso es largo.

Nuevo Secretario de AES

En la reunión de la Junta Directiva celebrada el pasado día 18 de febrero de 2015, y constituida por catorce de los quince miembros que la forman, presentes y representados, se celebraron elecciones siguiendo el Orden del Día de la convocatoria, eligiéndose nuevo Secretario de la Junta Directiva a D. Julio Pérez Carreño, por mayoría de los asistentes, y permaneciendo el resto de los miembros en sus cargos, ante la salida del cargo de D. Jesús Alonso Herrero, a quien todos los vocales agradecieron su activa labor en la Junta Directiva de AES.

El Secretario,
Julio Pérez Carreño

IV Jornadas Técnicas de Seguridad en Centros Sanitarios

Del 11 al 13 de mayo y organizadas por el Observatorio de Seguridad Integral en Centros Hospitalarios (OSICH), estas Jornadas de carácter anual y herederas de las Jornadas de Seguridad en Centros Hospitalarios se vienen realizando desde el año 2003 a lo largo de toda la geografía española teniendo una media de asistencia de unas 250 personas.

AES agradece al Observatorio y a su presidente, Carlos Ruiz, la invitación a participar en estas interesantísimas jornadas.

Asamblea General de Euralarm, Viena, 18 y 19 de mayo 2015

Con la presencia de más de 20 asociaciones europeas y de 10 empresas, se celebró en Viena la Asamblea General de Euralarm 2015.

Presentación del informe ESYS de Seguridad en España

El presidente de la Fundación ESYS, Javier Gómez-Navarro, el cual explicó el funcionamiento de la Fundación y sus actividades, para pasar a explicar los motivos que han llevado a la misma a la realización del informe, entre ellos que existen más incidentes de ciberseguridad de los que reflejan las estadísticas.

Los planes Compliance Penal en la Empresa

La DIRECTIVA 2014/24/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE (en vigor desde el 26 de febrero de 2014), a diferencia de la actual legislación española, establece un importante incentivo para que las empresas que contraten con el Estado, adopten programas de cumplimiento (Compliance Programs) penales y colaboren con la Administración de Justicia. A la vista de esta tendencia, no parece descartable, resultando incluso deseable, que se establezca la adopción de dichos programas como exigencia para las empresas que quieran contratar con el sector público.

La Directiva, no solo obliga a la exclusión de las empresas que hayan sido condenadas en sentencia firme por corrupción, entre otros delitos. También permite que dichas empresas eviten la exclusión si, entre otras cuestiones, prueban que han implementado un sistema de compliance penal adecuado (medidas técnicas, organizativas y de personal concretas, apropiadas para evitar nuevas infracciones penales o faltas). Se trata de un claro incentivo para que las empresas que contratan con la administración pública adopten programas de compliance penal apropiados.

No resulta descartable que, en el futuro, se exigiera como requisito de contratación con el sector público que el operador económico tuviera un programa de cumplimiento penal adecuado. De esta manera se asegura que todas las empresas que contraten con el Estado adopten estos programas de cumplimiento.

La Directiva europea exige que las autoridades nacionales excluyan de los procesos de contratación pública a aquellas empresas que hayan sido condenadas por determinados delitos.

En España, la vigente Ley de Contratos del Sector Público (2011) contiene un catálogo similar de delitos al de la Directiva europea.

La Directiva europea da una gran relevancia a los programas de compliance penal para lograr rehabilitar a una empresa inicialmente excluida por haber sido condenada mediante sentencia firme. De este modo permite que el operador económico demuestre su fiabilidad mediante la prueba de una serie de circunstancias, entre las cuales destaca la existencia de un programa de compliance penal adecuado. Ahora bien, la adopción de los mismos no constituye un motivo automático de inclusión. El operador económico deberá demostrar que ha pagado o se ha comprometido a pagar la indemnización correspondiente por cualquier daño causado por la infracción penal o la falta, que ha aclarado los hechos y circunstancias de manera exhaustiva, colaborando activamente con las autoridades investigadoras y que ha adoptado medidas técnicas, organizativas y de personal concretas, apropiadas para evitar nuevas infracciones penales o faltas.

Las medidas adoptadas por los operadores económicos se evaluarán teniendo en cuenta la gravedad y las circunstancias particulares de la infracción penal o falta. Las medidas técnicas, organizativas y de personal concretas deben estar orientadas a la prevención de infracciones penales.

La evolución que está experimentando la normativa europea parece conducir a que en el futuro, la administración pública exija Compliance Program penal a todas las empresas que contraten con el sector público.

Podemos asegurar que la Directiva europea sobre contratación pública de 2014, constituye un importante incentivo para que los operadores económicos que contraten o pretendan contratar con la administración pública implementen programas de cumplimiento penal adecuado.

Además proporciona idéntico incentivo para que, en caso de encontrarse en el seno de un procedimiento penal, indemnicen rápidamente, colaboren con la administración de justicia y mejoren su sistema de compliance penal. A la vista de la evolución reciente, resulta probable y deseable que en un futuro no lejano se exija como requisito de contratación con el sector público que el operador económico tenga implementado un programa de compliance penal adecuado.

Así las cosas, y centrándonos en la legislación española, podemos referirnos a la reforma del Código Penal de 2010, en cuyo artículo 31 bis, en vigor en la actualidad, sobre la responsabilidad penal de las personas jurídicas, se establece lo siguiente:

1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho o de derecho.

En los mismos supuestos, las personas jurídicas serán también penalmente responsables de los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en provecho de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en

el párrafo anterior, han podido realizar los hechos por no haberse ejercido sobre ellos el debido control atendidas las concretas circunstancias del caso.

2 La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el apartado anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.

3 La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el apartado siguiente.

4 **Sólo podrán considerarse circunstancias atenuantes de la responsabilidad penal** de las personas jurídicas haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades:

- **a)** Haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades.
- **b)** Haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos.
- **c)** Haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito.
- **d)** **Haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.**

5 Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones Públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades Públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía, administrativas o cuando se trate de Sociedades mercantiles Estatales que ejecuten políticas públicas o presten servicios de interés económico general.

En estos supuestos, los órganos jurisdiccionales podrán efectuar declaración de responsabilidad penal en el caso de que aprecien que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal."

Sin embargo, en la nueva revisión del Código Penal que está a punto de publicarse, se modifica este artículo, alineándolo con lo establecido en la Directiva europea, en el sentido de desarrollar más la responsabilidad de la persona jurídica, y establecer que solamente quedarán exentas de responsabilidad, aquellas que tengan programas de control revisados. La modificación es la siguiente y se encuentra en la actualidad publicada en la página web del Congreso de los Diputados:

"Vigésimo. Se modifica el artículo 31 bis, que queda redactado como sigue:

«1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables:

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

*2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, l**a persona jurídica quedará exenta de responsabilidad** si se cumplen las siguientes condiciones:*

*1.ª) **el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza;***

2.ª) la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiado a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control;

3.ª) los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención, y;

4.ª) no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la letra b).

En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.

*4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, **la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido.***

En este caso resultará igualmente aplicable lo dispuesto en el párrafo segundo del número 2 de este artículo.

5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior, deberán cumplir los siguientes requisitos:

1. Identificarán las actividades en cuyo ambito puedan ser cometidos los delitos que deben ser prevenidos.
2. Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.
3. Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.
4. Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.
5. Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

El modelo contendrá las medidas que, de acuerdo con la naturaleza y el tamaño de la organización, así como el tipo de actividades que se llevan a cabo, garanticen el desarrollo de su actividad conforme a la Ley y permitan la detección rápida y prevención de situaciones de riesgo, y requerirá, en todo caso:

a) de una verificación periódica del mismo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios; y

b) de un sistema disciplinario que sancione adecuadamente las infracciones de las medidas de control y organización establecidas en el modelo de prevención.»"

Los planes de compliance penal deberán:

1. Identificar los riesgos delictuales.
2. Definir medidas de control para evitar la comisión de delitos.
3. Monitorizar las medidas de control con chequeos regulares para comprobar que funcionan.
4. Formar a los trabajadores.
5. Elaborar informes trimestrales y un documento del plan anual.

Adopta el cloud en toda confianza

El uso de la computación en cloud se ha disparado, y en 2016 este crecimiento aumentará para convertirse en la mayor parte de los nuevos gastos de TI, de acuerdo con Gartner Inc. Pero a medida que se coloca en el cloud más y más información sobre las personas y las empresas, se plantea la preocupación acerca de cuán seguro es el entorno.

Será grande, si los números son exitosos. Según la firma analista Gartner (2013), el mercado de la computación en el cloud crecerá un 18,5 %, de USD 111 mil millones en 2012 a USD 131 mil millones en 2017. Lo que es más, el 2016 será un año decisivo para el cloud, cuando la tecnología de vanguardia se vuelva más sofisticada en los próximos años.

Creciente preocupación

Sin embargo, a pesar de la rápida escalada del uso de los servicios en el cloud, muchos siguen siendo reticentes. Peor aún, existen algunos que se niegan a adoptar todas las aplicaciones basadas en el cloud en absoluto, mencionando las preocupaciones de seguridad y privacidad, los desafíos operativos o la incapacidad de controlar la información una vez que sale del perímetro. De acuerdo con un estudio global en 2014 de BT, la seguridad de los datos y la confianza en los servicios basados en el cloud son un motivo de inquietud entre los que toman decisiones de TI dentro de las grandes organizaciones. De hecho, el estudio mostró que la seguridad era la principal preocupación del 76 % de todos los encuestados cuando se utilizan servicios basados en el cloud. Casi la mitad de los encuestados (49 %) admitió que están “ muy o extremadamente ansiosos ” sobre las implicaciones de seguridad que rodean el cloud.

Incluso mientras que el 79 % de los encuestados en los EE.UU. (70 % a nivel mundial) siguen adoptando las aplicaciones Web y de almacenamiento en el cloud dentro de su negocio, es claro que la confianza en torno a la seguridad en el cloud está en su mínimo histórico.

La investigación ha demostrado que el 89 % de la comunidad de la fuerza laboral global carece actualmente de comprensión sobre las formas en las que se aplica la protección de la seguridad en el cloud. El problema no es la seguridad del cloud en sí misma, sino el conocimiento disponible para los usuarios.

¡No entre en pánico!

Un temor tan genuino por la seguridad de uno de los más preciados activos almacenados en el cloud, tal como la información personal, es absolutamente comprensible, pero también exagerado en gran medida.

Un especialista en derecho de computación en el cloud de la firma de abogados global Covington & Burling, Maria-Martina Yalamova, dice que, con frecuencia, los proveedores de servicios del cloud de renombre ofrecen mucha mayor seguridad de la que los individuos o empresas pueden lograr por sí solos. “ Estos proveedores invierten importantes recursos en asegurar que sus sistemas utilicen medidas de vanguardia en seguridad y rutinariamente realizan pruebas de estrés y fortalecen estas medidas. Muchos cumplen con normas de seguridad internacionales y están sujetos a las obligaciones contractuales y legales/reglamentarias para mantener los datos seguros y privados. Y ofrecen a los clientes una amplia gama de controles de privacidad para proteger sus datos, en función del tipo de datos en cuestión”.

La historia del cloud ya mudo desde sus inicios. Al igual que con cualquier tecnología o modelo de prestación, las etapas embrionarias generan miedo, incertidumbre y duda. Recuerde también que no fue hace mucho tiempo cuando nos preguntábamos si los ordenadores personales serían capaces de resistir la embestida de las amenazas de seguridad a las que se enfrentaban.

(sigue en pág. 10)

(viene de pág.9)

Lo mismo se aplica al cloud, según el Dr. Knut Blind, Profesor de Innovación y Tecnología en el Instituto Fraunhofer de Sistemas de Comunicación Abierta en Berlín, Alemania. Él cree que los tiempos han cambiado sin duda cuando se trata de la seguridad y los temores asociados.

Migre con confianza

El hecho es que no todos los clouds son iguales, y la calidad del servicio y el apoyo puede variar dramáticamente de un proveedor a otro.

El problema primordial aquí es la confianza. Al mejorar la confianza, las personas y las empresas serán más propensas a aceptar los beneficios de la computación en el cloud, como ser la reducción de costos y mejora la capacidad de ampliación y tiempos de implementación. El tema es que este nivel de confianza sólo puede construirse si se tiene en cuenta el tipo de datos a la hora de planificar cualquier uso del cloud.

El Prof. Edward Humphreys, Coordinador del grupo de trabajo de ISO responsable de las normas de gestión de seguridad de la información, incluyendo las normas ISO/IEC 27001, ISO/IEC 27002 y la norma de seguridad en el cloud ISO/IEC 27017, cree que la creación de un clima de confianza es el requisito más importante a la hora de externalizar las TI. “Las empresas necesitan tener garantías en el proveedor del cloud subyacente”.

“Muchos usuarios no entienden que tienen que seleccionar un proveedor de servicios en el cloud que tenga un buen gobierno sobre el tratamiento de los datos personales; y los que lo saben pueden enfrentar dificultades para saber cómo verificar si el buen gobierno está implementado. Esta situación puede conducir a un incremento de los riesgos para la protección de los datos personales”.

Entonces, ¿qué se puede hacer ? Ciertamente, los proveedores de servicios en el cloud deben tomar medidas para mejorar la confianza de los clientes, dice Humphreys. En la práctica, esto significa: “Un proveedor de servicios de cloud necesita, como parte de su proceso de gobierno, tener un sistema de controles funcionando que se ocupe específicamente de la protección de datos personales. Comenzando con un acuerdo de procesamiento de datos, que describa el proceso de gobernanza y los temas importantes que pueden ser relevantes para el cumplimiento de sus obligaciones legales, esto ayudará a los clientes a tener confianza en la selección del proveedor correcto de servicios en el cloud. Demostrar el cumplimiento con la norma ISO/IEC 27001, ampliar los controles sobre la protección de los datos personales de la norma ISO/IEC 27018, puede añadir, además, un nivel adicional de confianza en los clientes. ”

> ***Las empresa necesitan tener garantías en el proveedor del cloud subyacente***

El Prof. Knut Blind está de acuerdo: “Al tener más y más personas utilizando servicios en el cloud, los proveedores del cloud deben proporcionar controles de seguridad fáciles de usar y bien diseñados. Las empresas tienen que establecer sistemas apropiados de gestión de seguridad de la información. ”

Servicio seguro en el cloud

Entonces, ¿cómo pueden las empresas crear un nivel de servicio estándar para los servicios en el cloud? ¿ Cómo pueden tomar decisiones mejor informadas, al evaluar si se debe utilizar una solución de computación en el cloud y qué solución se adapta mejor a sus necesidades de negocio ?

Publicada en 2013, ISO/IEC 27018 es la primera Norma Internacional que se centra en la protección de los datos personales en el cloud. Aunque existe desde hace poco más de un año, la nueva norma finalmente proporcionar confianza a los usuarios en el cloud de que su proveedor de servicios está en buena posición para mantener los datos privados y seguros.

Yalamova añade, “la norma ISO/IEC 27018 especifica ciertos tipos mínimos de medidas de seguridad que deben adoptar los proveedores del cloud, incluyendo controles de cifrado y de acceso. La norma también requiere que los proveedores del cloud implementen políticas de sensibilización sobre seguridad y hacer que el personal pertinente esté al tanto de las consecuencias potenciales (para el personal, el proveedor del cloud y el cliente) de violar las reglas de privacidad y seguridad. ”

Siendo la primera norma que se ocupa de la protección de datos de carácter personal para el cloud, la ISO/IEC 27018 tiene los siguientes objetivos principales:

- Ayuda a los proveedores de servicios en el cloud que procesan datos personales a hacer frente a las obligaciones legales aplicables así como a las expectativas del cliente
- Habilita la transparencia para que los clientes puedan elegir servicios en el cloud bien gobernados
- Facilita la creación de contratos de servicios en el cloud
- Proporciona a los clientes en el cloud un mecanismo para garantizar que los proveedores del cloud cumplan con las obligaciones legales y otras

En pocas palabras, la norma ISO/IEC 27018 proporciona una base práctica para inducir la confianza en la industria del cloud. Al mismo tiempo, la industria pública del cloud contará con una orientación clara con el fin de cubrir algunos de los temas legales y regulatorios de sus clientes. ¿Qué más se puede pedir?

Ordenando el caos del cloud

Cuanto más rápidamente puedan los usuarios confiar en usar el cloud correctamente (contando con las precauciones de seguridad completas puestas en vigor), mejor será para el negocio y los datos, y la rentabilidad de su empresa. Y ya se ha producido una gran mejora gracias a la norma ISO/IEC 27018 a medida que los proveedores del cloud han tomado mayores medidas de seguridad para los datos de sus clientes.

Por supuesto, nosotros como individuos también esperamos evaluar los beneficios, riesgos e implicaciones para la privacidad cuando se considera un servicio de computación en el cloud. Y, no nos olvidemos de tomar la responsabilidad de mantener a nuestros datos personales a salvo, por ejemplo, mediante la elección de contraseñas seguras y haciendo doble comprobación de que el proveedor del cloud que elegimos ha adoptado las medidas de seguridad apropiadas y sigue siendo transparente sobre sus prácticas de procesamiento de datos.

Así que no deje que la exageración y la pérdida de confianza lo alejen de adoptar la nube – el ahorro y la utilidad del negocio es demasiado importante como para dejarla pasar.

¿Ha sido usted una víctima?

No se desespere. Usted no está solo.
Según María-Martina Yalamova, una abogada que se especializa en la protección de datos de la firma de abogados Covington & Burling, existen una serie de remedios:

- El primer paso será investigar la intrusión, y luego monitorear cómo y dónde se está utilizando los datos, prediciendo los próximos pasos en lo posible.
- Los remedios precisos variarán de acuerdo con la ley local, pero con frecuencia los malos actores recibirán una mejor resolución por parte de la policía, a la que se puede proporcionar la información sobre los individuos pertinentes. Los malos actores pueden no responder a las medidas civiles (como las medidas de cese y desistimiento, u órdenes judiciales).
- Una vez que se identifica un mal actor, también podría ser posible reclamar una compensación de parte de ellos. Si los beneficios de hacerlo son mayores que los costos dependerá de las circunstancias del caso.
- Finalmente, el individuo y sus asesores deben tener en cuenta que una respuesta desmesurada arriesga atraer la atención pública sobre la intrusión, erosionando aún más la intimidad de la víctima.

Cortesía de Maria-Martina Yalamova

5 Cosas que usted debe saber acerca de ISO/IEC 27018

1 - La nueva norma se basa en las normas de seguridad de la información existentes, incluyendo ISO/IEC 27001 e ISO/IEC 27002
2 - La combinación de un conjunto común de objetivos de control, controles y directrices basados en ISO/IEC 27002, y los objetivos específicos de control adicionales en el cloud y otros controles, ayuda a gobernar el tratamiento de los datos personales en el cloud
3 - Los proveedores de servicios en el cloud pueden cumplir con las obligaciones aplicables
4 - La transparencia permite a los clientes de los servicios en el cloud seleccionar servicios de procesamiento de datos personales bien gobernados en el cloud
5 - El mecanismo para el ejercicio de los derechos de auditoría y cumplimiento ayuda a prevenir los riesgos para proteger los datos personales

Elizabeth Gasiorowski-Denis
Fuente ISOfocus

La Seguridad Privada celebra su día nacional en Madrid, el 21 de mayo.

El Secretario de Estado de Seguridad, Francisco Martínez, presidió el pasado día 21 de mayo, en Madrid, el "Día Nacional de la Seguridad Privada", en un acto en el que estuvo acompañado por el presidente de la Confederación Empresarial de Usuarios de Seguridad y Servicios, Rafael Araujo; la Delegada del Gobierno en Madrid, Concepción Dancausa; el subsecretario del Ministerio del Interior, Luis Aguilera; el Director General de la Policía, Ignacio Cosidó; el Director General de la Guardia Civil, Arsenio Fernández de Mesa, y los directores adjuntos operativos de la Policía y de la Guardia Civil, Eugenio Pino y Cándido Cardiel, entre otras personalidades.

En su intervención, el Secretario de Estado Francisco Martínez Vázquez, señaló que la Seguridad Privada en España es un sector puntero a nivel europeo y mundial.

Explicó que la nueva Ley de Seguridad Privada se preocupa por el capital humano que integra el sector, "acentuando su preocupación por la formación y la motivación de las personas como las que hoy han sido galardonadas, tratando de erradicar el intrusismo profesional".

Francisco Martínez señaló asimismo, que la seguridad privada en España es, hoy en día, un sector puntero a nivel europeo y mundial, integrado por más de 100.000 profesionales, 1.600 empresas, más de 1.000 centros de formación y que facturó alrededor de 3.300 millones de euros en 2014. Además, destacó que se trata de "un sector sólido e innovador que aglutina a profesionales muy cualificados, que presenta grandes posibilidades de crecimiento y factura a nivel europeo 34.000 millones de euros, cuenta con 2,2 millones vigilantes de seguridad privada y 60.000 empresas".

En este sentido, el secretario de Estado de Seguridad detalló que en España hay un vigilante de seguridad por cada 513 habitantes frente a otros países como Francia con un vigilante de seguridad por cada 438 habitantes; Alemania, un vigilante de seguridad cada 322 habitantes; o Reino Unido, con un vigilante de seguridad cada 170 habitantes.

Francisco Martínez recordó que durante esta Legislatura se han aprobado varias leyes que han modernizado la arquitectura normativa de todos los ámbitos de la seguridad, entre ellas, la Ley de Seguridad Privada. El secretario de Estado de Seguridad destacó que el escenario que facilita la nueva Ley de Seguridad Privada "está presidido por la colaboración entre lo público y lo privado, consolidando la relación y el respeto hacia un sector con entidad propia que, de manera innegable, es parte coadyuvante de la seguridad pública, en una labor auxiliar y complementaria de las Fuerzas y Cuerpos de Seguridad".

El secretario de Estado señaló además que la ley aprobada es la norma que merece "un sector maduro, pujante y altamente especializado" que está presente en el medio rural y en el medio urbano, que presta servicio en complejas instalaciones, con uso expansivo de nuevas tecnologías, con presencia en aeropuertos, centros penitenciarios, en alta mar o dedicados a labores de investigación privada. En este punto, Francisco Martínez ha anunciado que el desarrollo de la Ley de Seguridad Privada tendrá continuidad en el próximo reglamento que el Ministerio del Interior está preparando.

Entrega de Menciones Honoríficas

Durante este acto, se ha hecho entrega de varios Menciones Honoríficas al personal de Seguridad Privada que han destacado por su labor en el desempeño de sus actividades en materia de seguridad y protección y colaboración con las Fuerzas y Cuerpos de Seguridad del Estado.

El secretario de Estado de Seguridad, Francisco Martínez, mostró su agradecimiento a todos los trabajadores de la seguridad privada, y en particular, a los profesionales que recibieron las Menciones Honoríficas por su destacada contribución en beneficio de la seguridad de todos los españoles, y les ha animado a todos a continuar, con un impulso renovado, el excelente trabajo que desarrollan las 24 horas del día los 365 días del año en España y en el exterior.

AES, Asociación Española de Empresas de Seguridad, es socio fundador de UAS (Unión de Asociaciones de Seguridad)

De acuerdo con la Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento de desarrollo, le informamos de que los datos personales utilizados para el envío de la presente comunicación publicitaria, están almacenados en un fichero responsabilidad de la Asociación Española de Empresas de Seguridad, con domicilio social en C/Alcalá, 99 2ºA 28009 Madrid (en adelante AES). El interesado puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición en la dirección indicada o en aquella que la sustituya y se comunique en el Registro General de Protección de Datos.

Agradecemos las colaboraciones que hacen posible esta edición trimestral y animamos a nuestros lectores a que nos remitan informaciones o artículos de opinión para su publicación en el boletín. AES no se hace responsable de las opiniones vertidas en este boletín.