CSTIC 2010

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC

COMITÉ DE LOS SISTEMAS Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

INTECO

Instituto Nacional de Tecnologías de la Comunicación

Patronos:

Aena Aeropuertos Españoles y Navegación Aérea

AENOR

fundación enresa

Patrocinadores

Caelum Information & Quality Technologies

indra

Seguridad en el uso de las TIC. Conductas delictivas e ilícitas.

"Gestión de las TIC: Calidad y Sostenibilidad"

Universidad Pontificia Comillas

5 de octubre de 2010

luis.hidalgo@inteco.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza2

Índice – 1ª Parte

1. El Instituto Nacional de las Tecnologías de la Comunicación, **INTECO**

2. Principales acciones del área de seguridad de **INTECO**

   a. El **Centro de Respuesta a Incidentes** de Seguridad para PYMES y Ciudadanos, **INTECO-CERT**

   b. Oficina de Seguridad del Internauta **(OSI)**

   c. Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información **(AEI-SRSI)**

Índice – 2ª Parte

3. La **Seguridad de la Información** en la **Empresa**

    a) Introducción: **una mirada a la empresa en España**
    b) Conceptos generales de la **SI**
    c) La **SI** desde el punto de vista **LEGAL**
    d) La **SI** desde el punto de vista **de los DELITOS TIC**
    e) La **SI** desde el punto de vista de **NEGOCIO**

4. Todo tiene **solución**…

5. Turno de preguntas

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

1- El Instituto Nacional de Tecnologías de la Comunicación, INTECO

¿Qué es INTECO?

Instituto Nacional de Tecnologías de la Comunicación

✓**Sociedad estatal** adscrita al Ministerio de Industria, Turismo y Comercio **(MITYC)** a través de la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información **(SETSI)**

✓ **Herramienta** para la **Sociedad de la Información**

✓ **Gestión**, **asesoramiento**, **promoción** y **difusión** de proyectos para la S.I.

✓ Sus pilares son la **investigación aplicada**, la **prestación de servicios** y la **formación**

Objetivos de INTECO

Nace con varios objetivos

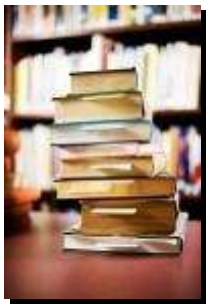
✓Contribuir a la **convergencia de España con Europa** en la Sociedad de la Información

✓ **Promoción** del sector TIC

✓ Creación de **Clúster-TIC en León** con alta capacidad de innovación

✓ Facilitar la **transversabilidad tecnológica** entre sectores de actividad

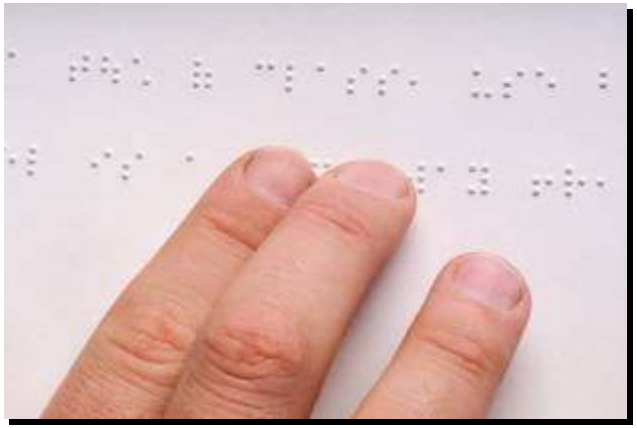


Líneas estratégicas de INTECO

Líneas actuales de trabajo

- ✓ **Seguridad tecnológica**
- ✓ Accesibilidad
- ✓ Calidad del software



Líneas de INTECO

- **Seguridad Tecnológica:**

  - **Promoción de servicios de la Sociedad de la Información**:
    - ✓ Más seguros,
    - ✓ LOPD,
    - ✓ Integridad de la información,
    - ✓ Cumplimiento de la normativa
  - **Iniciativas públicas en torno a la seguridad de las TIC:**
    - ✓ Observatorio de la Seguridad de la Información,
    - ✓ Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT)
    - ✓ Oficina de Seguridad del Internauta (OSI).

- **Accesibilidad:**

  - **Promoción de servicios de la Sociedad de la Información:**
    - ✓ más accesibles,
    - ✓ que supriman las barreras de exclusión,
    - ✓ faciliten la integración progresiva de todos los colectivos de usuarios
    - ✓ orientados a garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AA.PP.
  - **Iniciativas:**
    - ✓ Centro de Referencia en Accesibilidad y Estándares Web
    - ✓ I+D+i
    - ✓ TV Interactiva
    - ✓ CENTAC

- **Ingeniería del Software:**

  - **Promoción de servicios de la Sociedad de la Información:**
    - ✓ de mayor calidad,
    - ✓ mayor robustez de aplicaciones y sistemas, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios.
  - **Iniciativas:**
    - ✓ Laboratorio Nacional de Calidad del SW

Área de seguridad tecnológica

¿Cuáles con sus objetivos?

✓ **Sentar las bases** de coordinación de iniciativas públicas entorno a la Seguridad de la Información

✓ **Coordinar** la investigación aplicada y la formación especializada en el ámbito de la seguridad de la información

✓ **Convertirse** en centro de referencia en Seguridad de la Información a nivel nacional

INTECO-CERT

OSI

OBSERVATORIO

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

2.a- Principales acciones del área de seguridad

El Centro de respuesta a incidentes para PYMES y Ciudadanos, INTECO-CERT

Misión y objetivos de INTECO-CERT

Objetivos

- **Impulsar la confianza en las nuevas tecnologías**, promoviendo su uso de forma segura y responsable
- **Minimizar los perjuicios ocasionados por incidentes de seguridad**, accidentes o fallos facilitando mecanismos de prevención y reacción adecuados
- **Prevenir, informar, concienciar y formar a la PYME y el ciudadano** proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en Internet

Servicios prestados por INTECO-CERT

Servicios GRATUITOS en materia de seguridad informática

Servicios de información

- o Actualidad, noticias y eventos
- o Estadísticas en tiempo real

Servicios de protección

- o Útiles gratuitos de seguridad
- o Actualizaciones software

Servicios de formación

- o Manuales sobre legislación
- o Configuraciones de seguridad
- o Guías de resolución de problemas
- o Guías de buenas practicas y prevención

Servicios de respuesta y soporte

- o Gestión y resolución de incidencias de seguridad
- o Gestión y soporte ante fraude electrónico
- o Asesoría legal

Servicios prestados por INTECO-CERT

Servicios GRATUITOS de información

Servicios de información

- o Actualidad, noticias y eventos
- o Estadísticas en tiempo real

Para estar informado sobre qué está ocurriendo en seguridad

http://cert.inteco.es

Suscripción a boletines de correo, RSS y foros de seguridad

Servicios prestados por INTECO-CERT

Servicios GRATUITOS de formación

Servicios de formación

- o Manuales sobre legislación
- o Configuraciones de seguridad
- o Guías de resolución de problemas
- o Guías de buenas practicas y prevención

FORMACIÓN GENERAL EN SEGURIDAD

FORMACIÓN ESPECÍFICA Y PROFESIONAL

Cursos instrumentales de verano en la Universidad de León
Cursos específicos para técnicos de seguridad
Máster profesional en Tecnologías de Seguridad III
Máster en Seguridad Tecnológica (Lanzamiento Octubre)

Servicios prestados por INTECO-CERT

Servicios GRATUITOS de protección

Servicios de protección → **CATÁLOGO DE ÚTILES GRATUITOS DE SEGURIDAD**

Servicios prestados por INTECO-CERT

Servicios GRATUITOS de respuesta y soporte

Servicios de respuesta y soporte

- o Gestión y resolución de incidencias de seguridad
- o Gestión y soporte ante fraude electrónico
- o Asesoría legal

Gestión de incidencias o problemas de seguridad

- o Soporte personalizado
- o A través del web o de correo electrónico **incidencias@cert.inteco.es**

Gestión y soporte ante fraude electrónico

- o Soporte personalizado
- o A través del web o de correo electrónico **fraude@cert.inteco.es**

Asesoría legal en Derecho de las Nuevas Tecnologías

- o Soporte personalizado
- o A través del web o de correo electrónico **legal@cert.inteco.es**

Herramientas Desarrolladas por INTECO-CERT

Si necesita más información

Toda la información en:

Portal WEB de INTECO-CERT

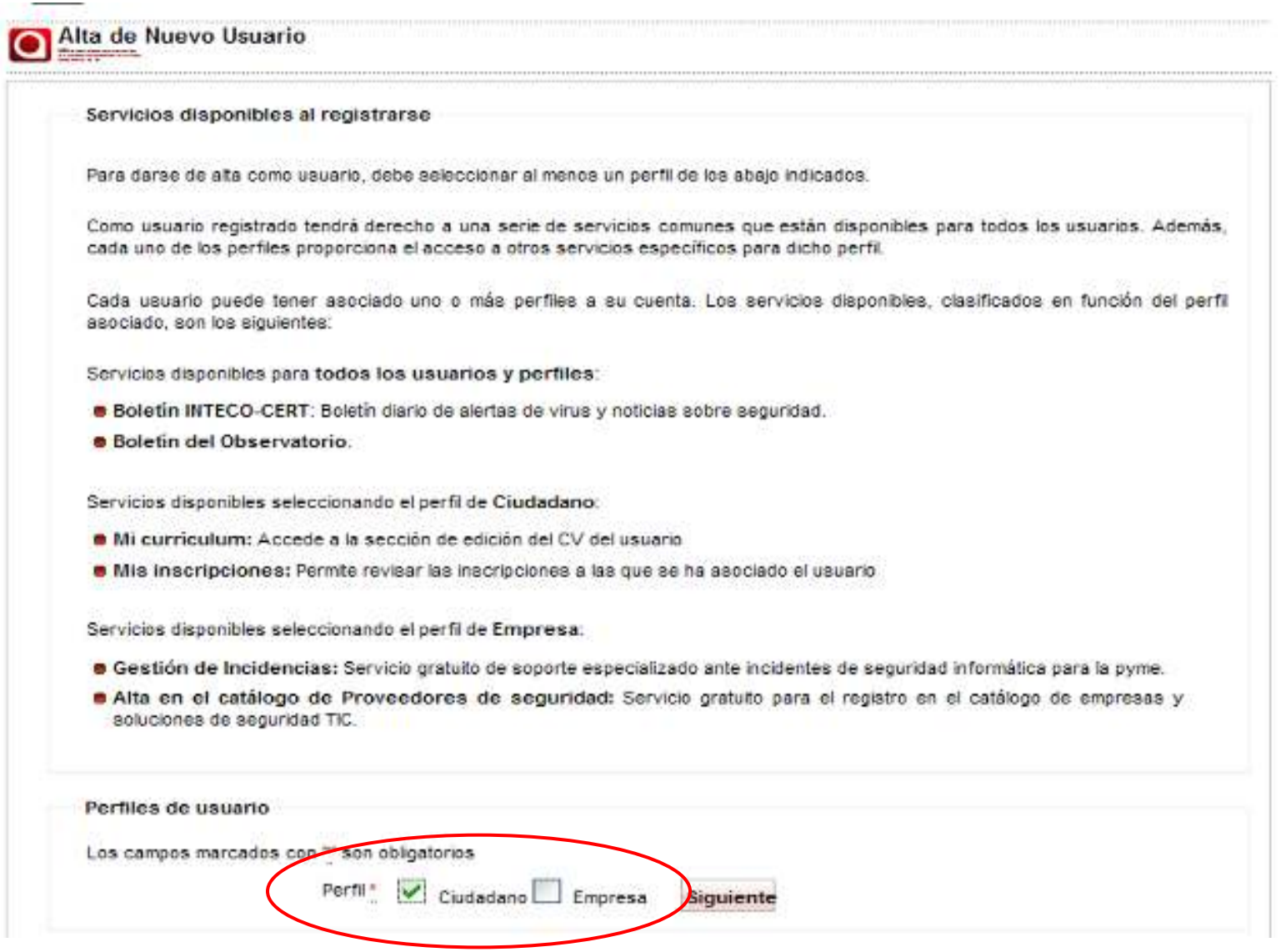
INTECO-CERT
Centro de Respuesta a Incidentes en TI

http://cert.inteco.es

Usuario registrado: atención personalizada
Buzón de contacto: contacto@cert.inteco.es
Buzón de incidentes: incidentes@cert.inteco.es
Buzón de fraude electrónico: fraude@cert.inteco.es
Buzón de asesoría legal: legal@cert.inteco.es

***INTECO-CERT** tiene vocación de servicio público sin ánimo de lucro y ofrece sus servicios de forma totalmente gratuita*

Suscripción gratuita



INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

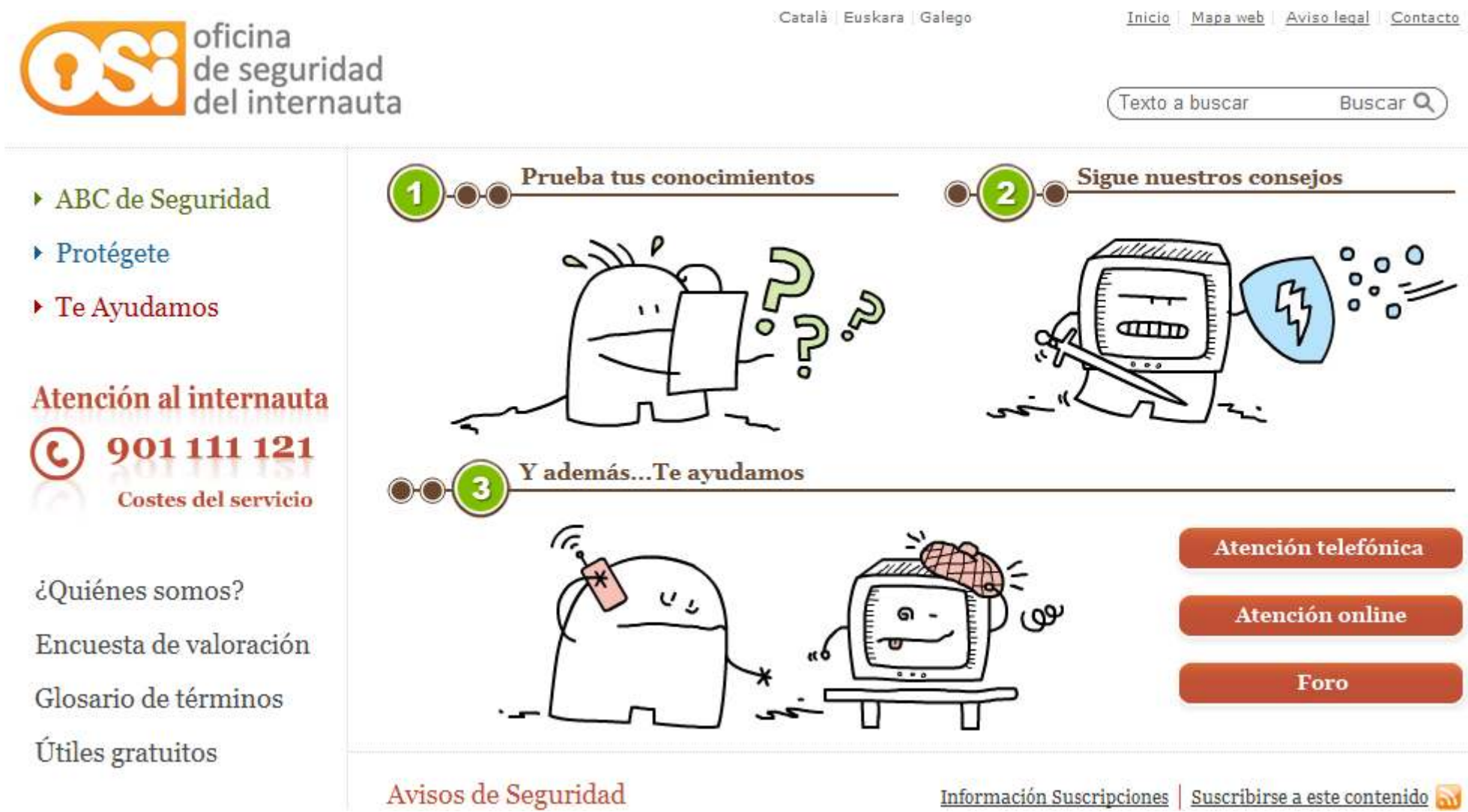
2.b- Principales acciones del área de seguridad

Oficina de Seguridad del Internauta

oficina
de seguridad
del internauta

OSI

www.osi.es



INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

2.C- Principales acciones del área de seguridad

Agrupación Empresarial Innovadora para la Seguridad de las Redes y los Sistemas de Información

aeiseguridad
Agrupación Empresarial Innovadora para la seguridad de las redes y los sistemas de información

AEI-SRSI

AGRUPACIÓN EMPRESARIAL INNOVADORA PARA LA SEGURIDAD DE LAS REDES Y LOS SISTEMAS DE INFORMACIÓN

reúne a empresas, asociaciones, centros de I+D+i y entidades públicas o privadas interesadas en la promoción del sector de las Nuevas Tecnologías, sus industrias afines y auxiliares, así como otros sectores emparejados con el mismo, que deseen contribuir a los fines de la Asociación, en el ámbito nacional de las Tecnologías de Seguridad.

Instituto Nacional
de Tecnologías
de la Comunicación

3- La Seguridad de la Información

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

a) Introducción:

Una mirada a la empresa en España

Una mirada a la EMPRESA en España

	Sin asalariados	Micro-empresas (0-9)	Pequeñas (10-49)	Medianas (50-249)	PYME (0-249)	Grandes (250 o más)	Total
Nº empresas	1.612.902	2.973.857	163.825	23.798	**3.161.480**	4.139	**3.165.619**
Porcentaje (%)	50,95	93,94	5,18	0,75	**99,87**	0,13	100

*Fuente: INE, DIRCE, 2006 (datos a **1 de enero de 2006**). Elaboración propia*

España es un país de PYME

Más del 99% de las empresas en España son PYME

PYME y LOPD

- El conocimiento de la LOPD es elevado (79,2%), pero su cumplimento muy bajo (valor aprox.)
- El 56,2% de las empresas no conocen las sanciones previstas en la LOPD
- Sólo el 17,7% de las empresas realizan las auditorias de seguridad requeridas por la ley
- Son pocos los encuestados que disponen de un documento de seguridad (23,4%)

Solo el 7,5% de los encuestados demandaría con frecuencia servicios de asesoría jurídica

Fuente: Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas. *Observatorio de la Seguridad* de **INTECO**

PYME e incidencias de seguridad

- Los propios empleados son una importante fuente de incidentes de seguridad. El enemigo está dentro
- Hay una importante ausencia en cuanto a la aplicación de políticas de seguridad en la PYME
- Muchos de los incidentes de seguridad en las PYMES no son detectados o se desconoce su origen
- Existe una falta de buenas prácticas y un uso adecuado de los recursos y los medios de la empresa

Las PYMES no se consideran un "objetivo" y la seguridad no es una prioridad

Fuente: Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas. *Observatorio de la Seguridad* de **INTECO**

Conclusiones generales

- La PYME en general no asocia un incidente de seguridad como un riesgo para su negocio o su actividad
- Se desconocen las consecuencias que puede suponer un incidente grave de seguridad
- Se desconocen el tipo de incidencias que pueden darse, así como el propio nivel de riesgo de la empresa
- La PYME de forma general, no asocia un incidente de seguridad con una pérdida económica real, de actividad, de clientes o de imagen

Existe un gran problema de percepción y de concienciación

Fuente: Estudio sobre incidencias y necesidades de seguridad en las pequeñas y medianas empresas españolas. *Observatorio de la Seguridad* de **INTECO**

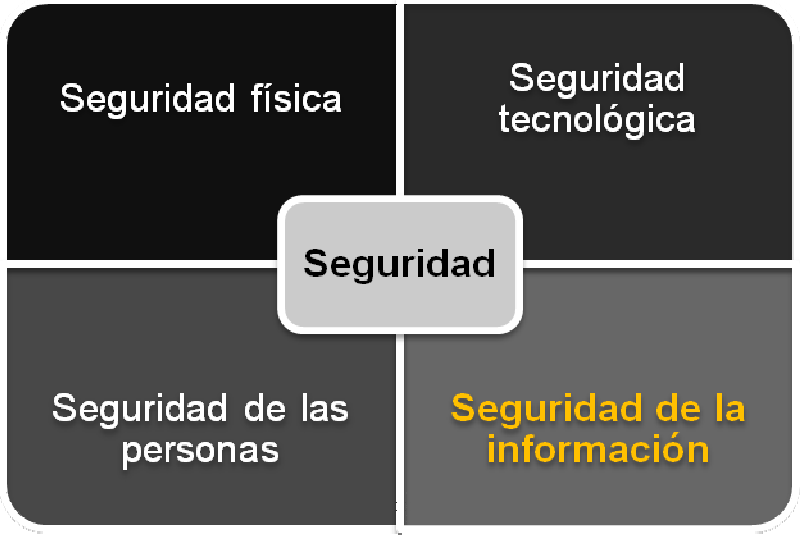
INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

b) Seguridad de la Información:

CONCEPTOS GENERALES

Enfoques de seguridad I



La seguridad afecta a los distintos activos de una organización

¿Qué es la Seguridad de la Información?

La información es un activo tangible o intangible que tiene valor para los procesos de nuestro negocio y actividad

La información tiene diversas fuentes, naturaleza y ciclos de vida

La seguridad de la información es la protección de la:

Confidencialidad, Integridad y Disponibilidad

Seguridad de la Información: Concepto

¿Qué es la Seguridad de la Información?

¿Información?

Es un activo de información tangible o intangible que tiene valor para los procesos de nuestro negocio y actividad

- **Fuentes de información**
- **Tipo de información**
- **Ciclo de vida**

Es la protección de:

- ✓ **Confidencialidad**: Acceso a la información por perfiles adecuados
- ✓ **Integridad**: Datos y sistemas fiables y sin alteración de la información
- ✓ **Disponibilidad**: Datos y sistemas accesibles en todo momento

Dos conceptos distintos

Seguridad Informática
Protección de las infraestructuras TIC que soportan nuestro negocio

Seguridad de la Información
Relativa a la protección de los activos de información de cualquier amenaza

La Seguridad Informática es parte de la Seguridad de la Información

Seguridad de la Información: ¿Qué es?

¿La Seguridad de la Información es …

- **Un programa antivirus, antispyware ?**
- **Instalar un firewall para proteger servicios?**
- **Encriptar una VPN?**
- **Analizar los logs de los sistemas?**
- **Algo que instalemos y se solucione?**

NINGUNA DE LAS ANTERIORES

La seguridad NO es un producto; es un proceso!!

“Es inevitable estar conectado: las empresas cada vez más - si no totalmente - dependen de las comunicaciones digitales .”

“Las empresas de todo el mundo necesitan comprender los riesgos asociados con hacer negocios por vía electrónica”

“No hay soluciones rápidas para la seguridad digital.”

Bruce Schneier
“Secrets and Lies”
www.schneier.com

Seguridad de la Información: Conclusión

¿Por qué es necesaria?

- Siempre hay riesgos
- Se mejora la productividad y la eficiencia
- Hay que cumplir normativas y legislación
- Se evitan interrupciones de la actividad
- Podemos ofrecer garantías y recibir garantías

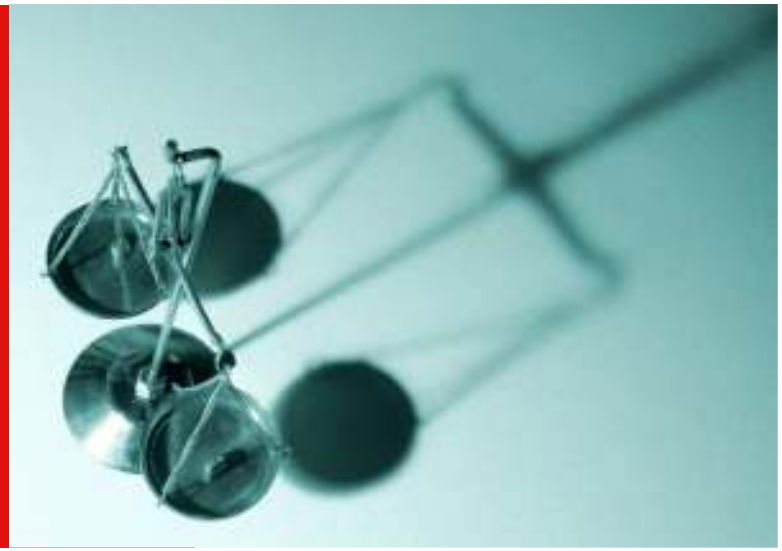
Las razones son tantas como los riesgos y las amenazas

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

C) Seguridad de la información:

El punto de vista LEGAL



El marco legal en España

- La Ley Orgánica 15/1999, de 13 de diciembre, **de Protección de Datos de carácter personal (LOPD). (BOE 298 de 14-12-1999** [pdf] [url])
- **La Ley 34/2002**, de 11 de julio, **de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).** (BOE 166 de 12-07-2002 [pdf] [url])
- **La Ley 59/2003**, de 19 de diciembre, **de Firma Electrónica** (BOE 304 de 20-12-2003 [pdf] [url]).
- **Real Decreto Legislativo 1/1996**, de 12 de abril, por el que se aprueba el texto refundido de la **Ley de Propiedad Intelectual (LPI)**. (BOE 97 de 22-04-1996 [url])
- **Otras (…)**

La normativa cambia, se amplia y se actualiza

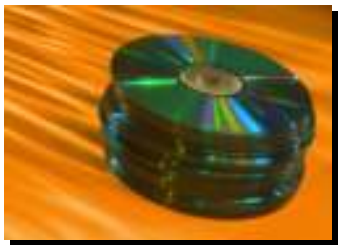
El marco legal en España

Sectores, actividad, acciones…todo cuenta







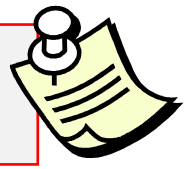
El asesoramiento PROFESIONAL es fundamental

Adecuación

Adecuarse a la normativa no es simplemente CUMPLIR la Ley, podemos ir mucho más allá

- Ofrecemos una garantía a nuestros clientes y proveedores
- Nos podemos distinguir de la competencia
- Podemos mejorar la gestión de nuestro negocio
- Nos subimos al tren de la seguridad de la información
- Es un primer paso para objetivos de mayor alcance, como la implantación de un SGSI

Hacer las cosas bien, nos aporta valor añadido, podemos y debemos aprovecharlo



INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

d) Seguridad de la información: Delitos TIC

Delito informático: Convenio sobre la Ciberdelincuencia

Con el término **delito informático** aglutinamos los hechos que, basándose en técnicas o mecanismos informáticos, pudieren ser tipificados como delito en el Código Penal, tales como: delito de estafa, delito contra la propiedad intelectual e industrial, etc.

Convenio sobre la Ciberdelincuencia del Consejo de Europa es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional).

Adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

Delito informático: Características

- Los delitos informáticos son acciones de **tipo ocupacional**, ya que en la mayoría de los casos, se realizan cuando el sujeto está trabajando o sitios públicos.

- Presentan grandes **dificultades** a la hora de comprobar quien cometió el ilícito debido a la gran expansión de Internet y a al carácter técnico de estos hechos.

- Hasta hace poco, no se producían **apenas denuncias** en este ámbito, lo que dificultaba su persecución.

- También su **perpetración es relativamente fácil** en cuanto a tiempo y espacio se refiere, ya que pueden llegar a consumarse en poco tiempo y sin necesidad de presencia física del delincuente.

- Son delitos que provocan **grandes pérdidas económicas** para los afectados y grandes "beneficios" para el que comete el delito.

- Por último, señalar que en su mayoría, sólo pueden ser cometidos por personas con unos **determinados conocimientos técnicos**.

Delito informático: Perfil Criminológico

Las personas que cometen delitos informáticos, o el sujeto activo de dichos delitos, en el mayor número de los casos suelen ser **verdaderos expertos** en informática que entran sin ningún tipo de permiso a redes y ordenadores ajenos.

Así, los **Hackers**, que podrían ser los nuevos piratas.

Son personas expertas “en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker”.

Hacker ético – profesionales de la seguridad que aplican sus conocimientos de hacking con fines defensivos (y legales).

Por otro lado, los **Crackers**, son personas que “violan la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño”.

Clasificación de conductas delictivas

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos

Delitos informáticos

Delitos relacionados con el contenido

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Clasificación: Delitos contra la confidencialidad

Acceso ilícito: El acceso deliberado e ilegitimo a la totalidad o a una parte de un sistema informático, ya sea infringiendo medidas de seguridad, con la intención de obtener datos informáticos

Interceptación ilícita*:* Interceptación deliberada e ilegitima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos.

Interferencia en los Datos: Comisión deliberada e ilegitima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

Interferencia en el sistema*:* Obstaculización grave, deliberada e ilegitima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Abuso de los dispositivos*:* Comisión deliberada e ilegitima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático.

Clasificación: Delitos informáticos

***Falsificación informática**: Cometer de forma deliberada e ilegitima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.*

***Fraude Informático**: Actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante cualquier introducción, alteración, borrado o supresión de datos informáticos, cualquier interferencia en el funcionamiento de un sistema informático.*

Clasificación: Delitos de contenido

Delitos relacionados con la pornografía infantil: Comisión deliberada e ilegitima de producción de pornografía infantil con vistas a su difusión por medio de un sistema informático, la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático, la difusión o transmisión de pornografía infantil por medio de un sistema informático, la adquisición de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona, la posesión de pornografía infantil por medio de un sistema informático o en un medio de almacenamiento de datos informáticos.

Fuente; Guardia Civil

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines: Infracciones de la propiedad intelectual, de conformidad con las obligaciones asumidas por el Convenio de Berna para la protección de las obras literarias y artísticas, Tratado de la OMPI sobre propiedad intelectual, Convenio de Roma.

Fuente; Guardia Civil

Nuevos delitos informáticos

Del **Phishing** (intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), surgen otras estafas igualmente dañinas: el **SMiShing** es su equivalente en teléfonos móviles, el usuario es engañado a través de mensajes SMS presuntamente enviados por un conocido o una entidad comercial que les redirige a sitios web maliciosos incitándoles a descargar programas que suelen contener virus informáticos. El **Vishing**, por su parte, lleva a cabo ese mismo engaño a partir de llamadas de voz.

Más novedoso es el **Phishing Car**: a través de este engaño, los criminales informáticos captan potenciales compradores de coches a bajo coste y les exigen el pago una señal por adelantado con una transferencia a una cuenta de un banco extranjero.

Con objetivos más perversos los *ciber-delincuentes* recurren al **Grooming**, una forma de captación de nuevas víctimas de las redes de pedófilos y pederastas. Éstos entran en contacto con menores de edad mediante correos electrónicos o *chats* haciéndose pasar por otra persona (normalmente una mujer u otro menor).

Por último, el **Cyber-bullying,** es un delito informático destinado a acosar a una persona. Los criminales utilizan la información electrónica procedente de correos electrónicos, mensajería instantánea, SMS, blogs, o incluso webs difamatorias para acosar a sus víctimas.

Fraude en Internet: Elementos utilizados

El fraude en Internet se basa en la utilización maliciosa de tres elementos sobre los que se construye el engaño. La presencia de estos elementos varía según el tipo de fraude y son utilizados de manera complementaria.

La **ingeniería social** es la herramienta más utilizada para llevar a cabo toda clase de estafas, fraudes y timos sobre los usuarios más confiados a través del engaño. Estas técnicas consisten en utilizar un reclamo para atraer la atención del usuario y conseguir que actúe en la forma deseada, por ejemplo convenciéndole de la necesidad de que reenvíe un correo a su lista de direcciones, que abra un archivo que acaba de recibir que contiene un código malicioso, o que, como ocurre en el **phishing**, proporcione sus códigos y claves bancarias en una determinada página web..

El **correo masivo y no deseado**, conocido como **spam**, constituye el mejor y más barato mecanismo de difusión de cualquier información y, por lo tanto, de cualquier intento de fraude.

El **malware, virus, gusanos, troyanos, keyloggers, capturadores de pantalla**, etc, diseñados específicamente para realizar tareas fraudulentas interceptan los datos que el usuario intercambia con una determinada entidad o las pulsaciones de su teclado.

Fraude en Internet: Elementos utilizados, páginas web

Las páginas web falsas persiguen diferentes finalidades:

Ofrecer **servicios inexistentes** por los que el usuario deberá realizar un pago y tras el que no se proporcionará el servicio o producto ofrecido.

Suplantación de páginas oficiales que imitan el contenido de ciertas páginas web pertenecientes a sitios web oficiales de entidades bancarias, comercio o administraciones públicas, con el objetivo de robar la información que el usuario intercambia habitualmente con dicha entidad.

El timador intenta que el usuario visite la página web falsa para conseguir la finalidad por la que fue creada a través de diversos medios y según el medio utilizado se establecen los siguientes conceptos:

Phishing: El defraudador intenta engañar al usuario a través de un correo electrónico que envía de forma masiva con el fin de aumentar sus probabilidades de éxito. Este correo electrónico aparenta haber sido enviado por la entidad suplantada para lo que utiliza imágenes de marca originales o direcciones de sitios web similares al oficial.

El **Pharming** modifica los mecanismos de resolución de nombres sobre los que el usuario accede a las diferentes páginas web tecleando la dirección en su navegador. Esta modificación provoca que cuando el usuario introduce en el navegador la dirección del sitio web legítimo, automáticamente es dirigido hacia una página web fraudulenta.

SMiShing: En este caso es un mensaje SMS el gancho utilizado para el engaño y su funcionamiento es similar al del Phishing. Aprovecha las funcionalidades de navegación web de los terminales de telefonía móvil para que el usuario acceda de manera inmediata a la página web falsa y proporcione allí sus datos.

El **Scam** utiliza también el correo electrónico para la divulgación de la página web falsa, pero el contenido del mensaje no intenta suplantar a ningún tercero sino que ofrece cantidades de dinero a conseguir fácilmente después de proporcionar cierta información personal y/o bancaria.

La mejor manera de evitar este tipo de fraude consiste en utilizar el sentido común y desconfiar de cualquier oferta con beneficios muy superiores a los que obtendríamos para un mismo servicio al acudir a un establecimiento convencional.

Fraude en Internet: Elementos utilizados, malware bancario

La utilización de código malicioso, o **malware** que se instala en el ordenador del usuario utilizando las técnicas habituales de los virus o gusanos, para la captura de datos intercambiados por el usuario, evoluciona continuamente. De forma general, se distinguen los siguientes casos:

Keyloggers: Toman este nombre aquellos códigos maliciosos que recogen las pulsaciones del teclado del usuario o incluso capturas de lo visualizado en pantalla cuando el usuario pulsa el botón izquierdo del ratón. Pueden utilizarse para capturar usuarios y contraseñas o claves de acceso a diversos sitios web, incluidos los servicios de banca online, comercio electrónico o administración. Esta captura puede estar limitada, activándose sólo cuando el usuario visita ciertos sitios web.

Troyano bancario: Este código malicioso se especializa en determinadas entidades bancarias modificando el aspecto de su página web legítima. El efecto habitual de un troyano es la superposición de una ventana, que no se muestra como tal, cuando el usuario accede al servicio online de la entidad afectada. La ventana superpuesta simula, en parte o en su totalidad, a la página web legítima con el fin de que el usuario introduzca la información en ella bajo la creencia de que lo está haciendo en la auténtica.

El nivel de protección ante este tipo de fraude vendrá marcado por la utilización de un software antivirus que nos permita la detección y borrado de dichos códigos maliciosos.

Fraude en Internet: Fraude Bancario

PROCESO DEL FRAUDE:

1. **Robo de códigos de acceso a banca electrónica.**
   - Phishing
   - troyanos / keyloggers
   - Hacking (pharming, bugs, ...)
2. **Usurpación de identidad y orden de transferencia bancaria electrónica a colaboradores financieros (MULAS).**
3. **Lavado de dinero y transferencia a defraudador.**

ACTORES:

1. **Vícitmas:**
   - Entidades finacieras
   - Clientes
2. **Autores:**
   - Grupo hackers
   - colaboradores finacieros (MULAS)
   - Grupo de recaudadores / blanqueadores

Fuente; Guardia Civil

Fraude en Internet: Elementos utilizados, otros timos

Según la forma que toma este fraude se distinguen los siguientes casos:

Cartas Nigerianas: El usuario recibe un correo electrónico donde le ofrecen el acceso a una gran suma de dinero, previo pago de un anticipo que el timador justifica bajo la necesidad de liberar una fortuna en alguna divisa extranjera o país en conflicto, y ofrece una pequeña parte de la misma una vez haya sido liberada.

Estafa Piramidal: Normalmente llega a través de un correo electrónico que ofrece un trabajo basado en la promoción de productos y en la captación de nuevos empleados. Al contactar con la presunta empresa, nos comunican que los nuevos miembros deben abonar una tasa de iniciación. Una vez incluidos en la organización, se descubre que los beneficios obtenidos no vienen tanto por la venta o promoción de los productos sino por la captación de nuevos miembros.

Mulas: Un correo electrónico ofrece al usuario la posibilidad de quedarse con un porcentaje de una transacción electrónica por el simple hecho de realizar otra transferencia del importe recibido, menos la comisión acordada, a otra cuenta que se le indica. Este caso no sólo se corresponde con un fraude, sino que además la persona se convierte en colaborador de un delito de blanqueo de dinero.

HOAX: Con este nombre se designan aquellos mensajes electrónicos que contienen el típico bulo o noticia falsa y se utilizan para sensibilizar al usuario con el fin de que realice aportaciones económicas.

Vishing: El usuario recibe un correo electrónico o mensaje SMS en el que se le indica que deberá llamar a un determinado número telefónico. Al llamar a dicho número se accede a un servicio que utiliza telefonía IP en el que se le solicita información personal como números de tarjetas, números de cuentas bancarias o usuarios/contraseñas de acceso.

Fraude con otros dispositivos: Móviles y WI-FI

ESTÉ PREVENIDO ANTE FRAUDES MEDIANTE MECANISMOS DE "INGENIERÍA SOCIAL", QUE INTENTAN EMBAUCARLE PARA LLAMAR Y/O ENVIAR MENSAJES A DETERMINADOS NÚMEROS

Este tipo de fraudes consisten en engañar a los usuarios para que utilicen el desvío de llamadas mediante la pulsación de una combinación de teclas (*#9...), envíen mensajes de texto o realicen llamadas a números de tarificación adicional (77xx, 80x, 90x). Están normalmente relacionados con trabajos (que no existen), premios (sin haber jugado) o paquetes recibidos (sin haberlos pedido).

NO SE CONECTE A PUNTOS DE ACCESO NO CONOCIDOS

Hoy en día existen multitud de puntos de acceso Wi-Fi todavía sin securizar, por lo que se puede acceder a ellos fácilmente. El peligro aparece cuando el punto de acceso está abierto intencionadamente con un propósito malicioso. De esta manera un usuario pensará que está usando "Internet gratis", pero lo que realmente sucede es que al conectarse a esa red se está permitiendo el acceso a toda la información del dispositivo a una persona no autorizada.

Privacidad en Internet: Concepto

Según el diccionario de la **Real Academia Española**, cuando se habla de Privacidad se hace referencia al *"ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".* No obstante, no puede hablarse de un único concepto de privacidad, sino que se trata de un concepto variable en función de los elementos y circunstancias que acompañen a cada caso.

El derecho a la intimidad y la privacidad se encuentra regulado en el **art. 18 de la Constitución Española de 1978** y ha sido desarrollado por el propio Tribunal Constitucional, estableciendo éste que la privacidad *"preserva un ámbito propio y reservado frente a la acción y conocimiento de los demás, el cual es necesario para mantener una calidad de vida mínima".*

Privacidad en Internet: Buscadores

La mayor controversia se encuentra en las **políticas de privacidad** ofrecidas por los buscadores, ya que el lícito tratamiento de los datos personales de los usuarios requiere del cumplimiento de una serie de garantías adicionales, como ha establecido la propia AEPD en su Declaración sobre los Buscadores de Internet.

Para un tratamiento legítimo de los datos de carácter personal, el afectado debe conocer:

- Qué datos se van a recabar.
- Quién va a tratar estos datos de carácter personal.
- Con qué finalidades se van a tratar.
- Si estos datos van a ser objeto de cesión y, en su caso, de qué tipo.

En relación con la privacidad, cabe destacar dos problemáticas:

- La **responsabilidad del buscador**, al indexar sitios web con perfiles y datos de carácter personal de los integrantes de la red social.

- La **responsabilidad de la propia red social**, a la hora de disponer de los perfiles de sus integrantes, así como de la realización de publicidad personalizada y contextualizada con la información y los datos que el propio usuario ha introducido en la red.

Para la lícita difusión de los datos de carácter personal contenidos en la red social, deberá recabarse el consentimiento inequívoco del afectado, así como que este consentimiento ha sido prestado conforme a los criterios suficientes de accesibilidad y claridad.

La regla general establecida por la ley es la de solicitar a los titulares de los datos el ***"consentimiento libre, específico, informado e inequívoco"*.**

Adolescente a la cárcel por sacar en Internet foto de ex novia desnuda

Associated Press

Un adolescente que publicó en su página web MySpace una fotografía desnuda de su ex novia menor de edad fue sentenciado a 30 días de cárcel.

Anthony D. Rich, de 19 años, se declaró "nolo contendere" de abuso infantil y de intento de abuso infantil. Se cree que comenzará a cumplir su sentencia en octubre.

Los fiscales redujeron los cargos de delito sexual que hubieran manchado de por vida a Rich como agresor sexual. El joven tenía 17 años cuando publicó la foto de la chica que entonces tenía 15 años en la popular página de la Internet.

Rich y la muchacha habían sido novios durante más de dos años. Publicó la foto después que rompieron la relación. La adolescente había permitido que se le tomara la foto, pero no que se publicara, dijeron las autoridades a cargo del caso.

Detenidos 3 que menores colgaron en internet grabaciones de sus actos

Noticias EFE | 24/05/2007|16:54h

Según informó el cuerpo policial, los arrestos tuvieron lugar el martes pasado, aunque la investigación se inició tras detectar los agentes en un sitio web, que permite subir, ver y compartir vídeos, cuatro grabaciones en las que se podía observar a unos jóvenes causando daños en el apeadero.

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

e) Seguridad de la información: NEGOCIO

Cuestiones fundamentales

¿**Por qué** es **importante** la **SEGURIDAD de la INFORMACIÓN** para **mi empresa**?

¿Qué debo hacer para alcanzar un **NIVEL ADECUADO** de seguridad TIC en mi empresa?

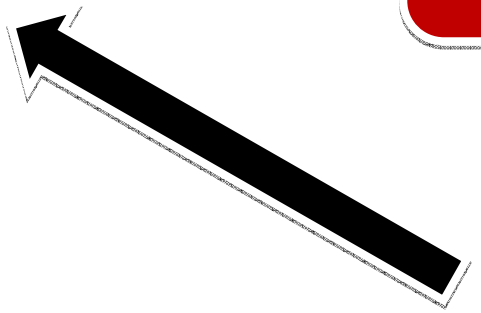
Nosotros podemos responder a la primera pregunta, la segunda la debe responder el profesional

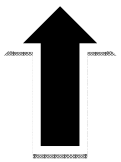
La seguridad y el negocio

¿Qué puede aportar a nuestro negocio?

Gestión, organización, productividad, procedimientos, eficacia, etc.

Valor añadido, para el cliente, garantía, calidad, imagen y marca, etc.





Recuperación, continuidad de negocio, reducción de interrupciones, etc.

La seguridad y el negocio

¿Mi negocio puede ser más eficaz y productivo?

Hábitos, usos y responsabilidad

- Plantilla poco concienciada
- Plantilla sin formación
- No se aplican buenas practicas
- Malos hábitos laborales
- Uso inadecuado de infraestructuras

Medios e infraestructuras

- Falta de procedimientos
- Control y gestión de recursos
- Puntos únicos de fallo
- Desconocimiento de activos de información
- Falta de personal cualificado

Conciencia corporativa

- La dirección o la gerencia no se involucra
- La seguridad es un gasto sin retorno
- La seguridad no está integrada en la gestión
- Usuarios VIP

Algunos ejemplos

Un fallo informático en la página de la CNMV deja ver el NIF de los consejeros

Un fallo informático en la página de Internet de la Comisión Nacional del Mercado de Valores (CNMV) -www.cnmv.es- permitió hoy acceder a los Números de Identificación Fiscal (NIF) de los consejeros de las empresas cotizadas en bolsa (…)

CD-Rom con datos de clientes hipotecarios

El Bank of Scotland, fundado en 1695, ha reconocido la pérdida de un CD-ROM que contenía los datos de 62.000 clientes hipotecarios. El CD-ROM no estaba cifrado y había sido enviado por correo ordinario a una agencia de créditos (…)

Protección de Datos multa a CCOO por filtrar a través de eMule 20.000 ficheros

La Agencia Española de Protección de Datos (AEPD) ha sancionado con 6.000 euros al sindicato CCOO porque uno de sus trabajadores filtró, accidentalmente, 20.000 ficheros con datos personales al utilizar el software de intercambio por internet eMule (…)

Tres de cada cuatro usuarios utilizan siempre la misma clave en sus diferentes actividades 'online‘

Tres de cada cuatro usuarios utilizan siempre la misma clave cuando se registran en portales de Internet, ya sea para realizar compras en la Red, recoger de billetes de avión, consultar el correo electrónico o realizar operaciones de banca 'online', según se desprende de un estudio realizado por Citylogo.com (…)

Seis de cada diez trabajadores pierden el tiempo en el trabajo

Una encuesta online a 2.057 empleados realizada por la compañía de compensaciones salari.com ha revelado que seis de cada 10 admiten perder el tiempo en el trabajo, con una media de 1,7 horas perdidas sobre una jornada de 8,5 horas, lo que supone el 20% de su tiempo (…)

¿Mi negocio puede mejorar su imagen?

Aportar garantía

- Adecuación y cumplimiento de la normativa
- Auditorias internas y externas
- Garantía a clientes
- Garantía de proveedores

Marca y diferenciación

- Somos mejores y más seguros
- Nos preocupa la seguridad y las amenazas
- Nos preocupan sus datos
- Somos eficientes, organizados y eficaces
- Aplicamos estándares y procedimientos

Nivel de servicio

- Podemos ofrecer servicios confiables
- Podemos hacer frente a contingencias
- Garantizamos tiempos de recuperación

Algunos ejemplos

Secretos militares USA enviados por error a un web turístico

Un sitio web particular, dedicado a promocionar una pequeña ciudad, ha sido finalmente desconectado por su responsable a "sugerencia" de altos mandos militares, tras recibir por error miles de correos electrónicos destinados en realidad a una base cercana de la fuerza aérea estadounidense (…)

Disco duro comprado en eBay contiene documentos de campaña del gobernador de Arkansas

El disco se anunciaba como nuevo en eBay y fue adquirido por 55 euros por un consultor informático, quien se encontró con que el disco aún guardaba documentos creados por funcionarios de alto nivel del Partido Demócrata de Arkansas durante la campaña a favor de Mike Beebe (…)

Monster.com vuelve a sufrir el robo de millones de datos personales

Es la segunda vez en 18 meses que la página *web* de búsqueda de empleo Monster.com ve cómo un agujero de seguridad en sus sistemas propicia el robo de millones de datos confidenciales de sus clientes. Y es la segunda vez que la compañía trata de tapar el suceso, del que sus usuarios se tienen que enterar por los medios (…)

La Marina británica pierde un portátil con los datos de 600.000 personas

El ordenador fue robado durante la noche del coche de un oficial, que ahora podría enfrentarse a un tribunal militar. Se desconoce si los datos estaban o no cifrados, o si existía alguna protección por contraseña (…)

La Agencia de Protección de Datos multa por primera vez el envío de correo basura

La Agencia de Protección de Datos comunicará próximamente a varias empresas españolas sanciones de 30.000 euros por enviar correos electrónicos publicitarios no pedidos ('Spam') **indiscriminadamente**, según anunció a Servimedia el director de la agencia, José Luis Piñar (…)

¿Mi negocio puede superar contingencias?

- Desastres naturales
- Incidentes provocados
- Servicios críticos
- Faltas de personal

- o Tornados, huracanes, inundaciones
- o Tormentas eléctricas, de nieve, arena
- o Riadas, hundimientos, heladas, terremotos
- o **Fuego**, fallo energético, salud, terrorismo
- o Fallos de energía y comunicaciones
- o Falta de personal, huelgas, protestas

Algunos ejemplos

Desaparecieron como un rayo

Una trabajadora de una empresa médica completó 1.200 entradas de facturación de clientes -un proceso que tardó varios días- cuando un rayo cayó sobre el transformador que había fuera del edificio. No quedó nada, ni siquiera las facturas que acababa de preparar (…)

Trifulca empresarial

Durante una acalorada discusión en Australia, un empresario lanzó una memoria USB a su socio. El dispositivo, que contenía importantes planos de la empresa, terminó hecho pedazos en el suelo. Por suerte fue posible salvar tanto los planos como la relación empresarial.

Calamidad en la construcción

Durante la construcción de un gran edificio de oficinas, se cayó una viga de acero en un ordenador portátil que contenía los planos del edificio, aplastando el ordenador (…)

Fuego indiscriminado

Un incendio destruyó la mayoría de los contenidos e informaciones de una oficina, sólo se salvaron unos pocos CD. El escollo del asunto es que estos CD se habían fundido en el interior de sus cajas, fue un trabajo notable para los ingenieros (…)

Roban un portátil de General Electric con datos de más de 50.000 trabajadores

General Electric reveló esta semana el robo, a principios de septiembre, de un ordenador portátil de la compañía con los nombres y datos de la Seguridad Social de 50.000 empleados.

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

4- Todo tiene solución (...)

Todo tiene solución (…)

¿Cómo pasar de…



…a?



Todo tiene solución (…)

Hoja de ruta

- Buscar asesoramiento profesional
- Aplicar seguridad desde el “negocio”
- Cumplir las normativas aplicables
- Buscar las mejores soluciones
- Actuar por fases, no precipitarse

Un buen asesoramiento es FUNDAMENTAL

Todo tiene solución (…)

Debemos tener en cuenta

- El mercado ofrece multitud de soluciones, productos y servicios
- La seguridad no es sólo de carácter tecnológico, sino también organizativo y jurídico
- La soluciones tecnológicas no son la soluciones definitiva, hay otros aspectos a tener en cuenta
- Las buenas practica son un arma fundamental
- Existen multitud de guías, recomendaciones e información disponible y de acceso gratuito
- La seguridad 100% no es posible, pero con poco esfuerzo se puede conseguir un nivel muy elevado

La seguridad es cosa de "todos" y empieza por "nosotros"

Todo tiene solución (…)

La seguridad es como una “cebolla”

(más)

Políticas y buenas practicas

Anti-Malware, Anti-Fraude, Cortafuegos

Actualizaciones y parches

¡¡Las copias de seguridad!!

La seguridad se implementa por “capas”

Todo tiene solución…

…podéis contar con nosotros

Catálogo de Empresas y Soluciones de Seguridad TIC

oficina de seguridad del internauta

Cursos de formación on-line

Guías y documentación

ENCUENTRO INTERNACIONAL DE LA SEGURIDAD DE LA INFORMACIÓN

LEÓN, ESPAÑA, DEL 26 AL 28 DE OCTUBRE DE 2010

INTECO-CERT Centro de Respuesta a Incidentes en TI

OBSERVATORIO de la Seguridad de la Información

Asesoramiento legal y tecnológico de primer nivel

www.inteco.es

5. Conclusiones

Internet presenta nuevos caminos: nuevos mercados, posibilidades de socialización, relaciones nuevas... Internet, y en general las tecnologías de la información, han supuesto un avance decisivo para la sociedad. El uso de la red y de todas sus aplicaciones debe hacerse sobre el **conocimiento, la información y la responsabilidad.**

Se hace vital contar con una mayor información sobre Internet y redes sociales, a todos los niveles, y una **mayor formación**, dar a conocer a menores y mayores las herramientas para salvaguardar su privacidad, cómo se pueden usar los contenidos, qué es lícito o no...

Es necesario **incrementar el diálogo de las organizaciones de consumidores** con la Administración y parece deseable que exista una especialización en materia de privacidad por parte de algunas organizaciones de consumidores.

Es necesario buscar una **colaboración activa entre usuarios**, asociaciones, gestores de redes sociales y Administraciones públicas, para identificar los principales problemas y buscar su solución

Dónde estamos

www.inteco.es

Sede de INTECO

Avda. Jose Aguado 41
Edificio INTECO
24005 **LEÓN**

Tel: (+34) 987 877 189
Fax: (+34) 987 261 016

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
plan avanza2
INTECO
Instituto Nacional de Tecnologías de la Comunicación