Instituto Nacional
de Tecnologías
de la Comunicación

La Seguridad en los equipos del Ayuntamiento

Jornadas Provinciales Modernización Administrativa y Nuevas Tecnologías (Real Monasterio de San Agustín - Burgos) - 26 de octubre de 2011

luis.hidalgo@inteco.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

plan avanza2

Índice

1. Instituto Nacional de las Tecnologías de la Comunicación, **INTECO**
2. Principales acciones del área de seguridad de **INTECO**
3. La seguridad de la información:
    1. Conceptos Generales
    2. Seguridad de la información: AAPP
    3. Amenazas TIC
    4. Soluciones
4. Conclusiones

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

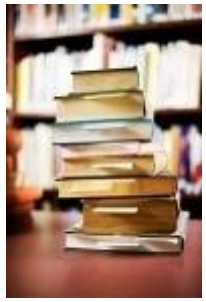
✓Contribuir a la **convergencia de España con Europa** en la Sociedad de la Información

✓ **Promoción** del sector TIC

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

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

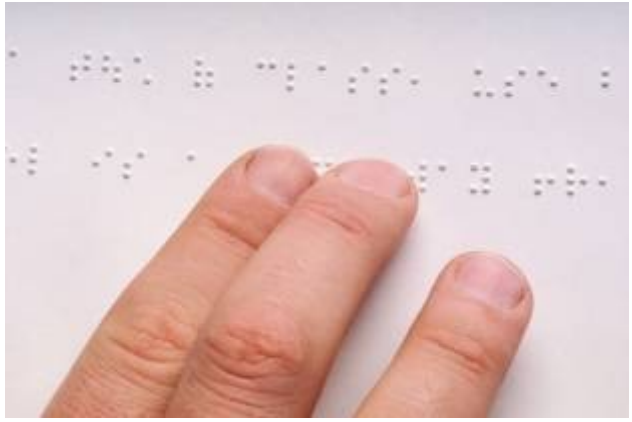


Líneas estratégicas de INTECO

Líneas actuales de trabajo

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



¿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

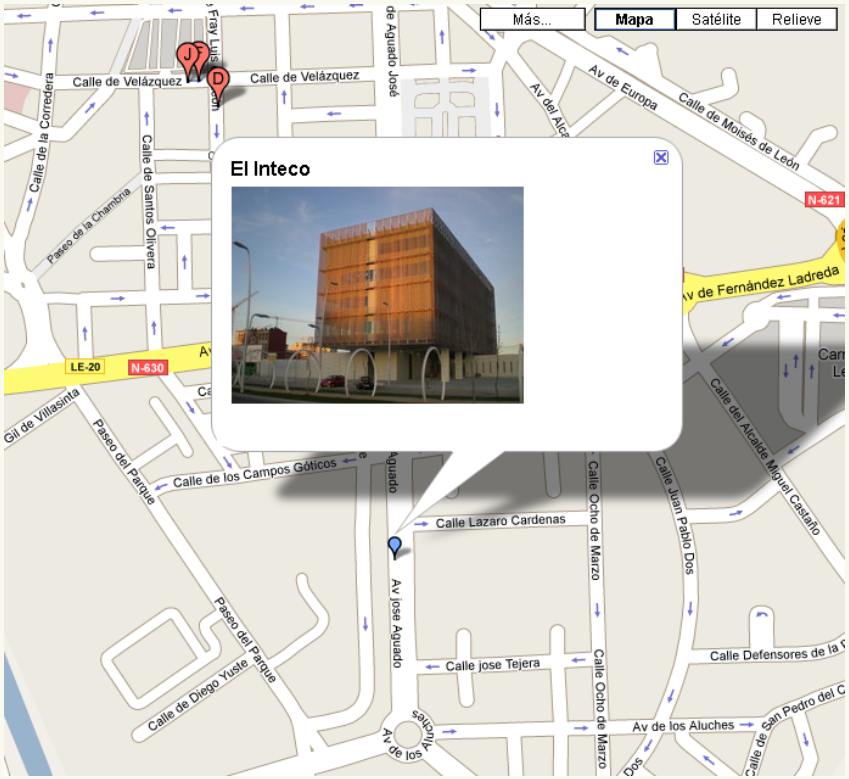
Dónde estamos

www.inteco.es

Sede de INTECO

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

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



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 en materia de seguridad informática

Servicios de información

- Actualidad, noticias y eventos
- Estadísticas en tiempo real

Servicios de protección

- Útiles gratuitos de seguridad
- Actualizaciones software

Útiles Gratuitos
Seguridad PYMES
Gestión de Incidencias
Suscripción

Servicios de formación

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

Servicios de respuesta y soporte

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

Foro de Seguridad

Indice de foros

Foros	Temas	Mensajes	Último mensaje
General			
Normas y Recomendaciones Lea esto primero	7	7	28/11/2007 10:07:44 dfirvida
Novatos Para preguntar las cosas más básicas sobre virus y seguridad informática	1386	6502	01/09/2011 13:08:11 Pedhro
Anti-Fraude Para preguntar cuestiones relacionadas con el fraude electrónico.	19	107	21/09/2010 12:50:42 nbenavides
Problemas con programas maliciosos Detección y eliminación de virus y programas maliciosos en general. Si sospecha que tiene un virus en su PC, este es el sitio adecuado para preguntar -excepto problemas con el navegador y acceso a Internet-	3317	17024	22/10/2011 10:36:03 nao666
Problemas en el acceso a Internet Problemas con la conexión a Internet o con el navegador, especialmente con secuestradores del navegador.	875	3983	12/08/2011 20:15:34 senorin
Programas Antimalware Para discutir sobre programas antivirus, antiespías, antitroyanos y similares, por ejemplo cuestiones de configuración, eficiencia y actualizaciones. No es para discutir problemas con virus.	2498	9420	10/12/2010 06:48:33 nao666
Seguridad Informática Protección de redes y ordenadores, programas cortafuegos y su configuración, intrusiones, buenas prácticas, etc.	1346	5272	07/10/2011 12:59:27 notarino
Recuperación de sistemas Recuperación de archivos y configuraciones después de un incidente. Copias de seguridad.	307	1244	23/10/2011 16:49:51 saviru

Plataforma de formación online

https://formacion-online.inteco.es

Servicios GRATUITOS de información

Servicios de información

- Actualidad, noticias y eventos
- 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

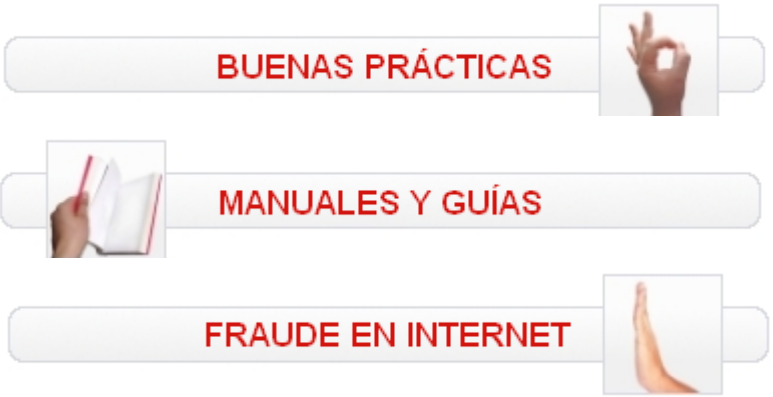
Síguenos en:

Servicios de formación

Servicios de formación

- Manuales sobre legislación
- Configuraciones de seguridad
- Guías de resolución de problemas
- 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 IV

Servicios de protección

Servicios de protección

- Útiles gratuitos de seguridad
- Actualizaciones software

CATÁLOGO DE ÚTILES DE SEGURIDAD

INFORMACIÓN SOBRE ACTUALIZACIONES Y PARCHES

Servicios de respuesta y soporte

Servicios de respuesta y soporte

- Gestión y resolución de incidencias de seguridad
- Gestión y soporte ante fraude electrónico

Gestión de incidencias o problemas de seguridad

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

Gestión y soporte ante fraude electrónico

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

Asesoría legal en Derecho de las Nuevas Tecnologías

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

Si necesita más información

Toda la información en:

Portal WEB de INTECO-CERT

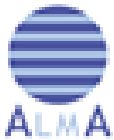
http://cert.inteco.es

Buzón de contacto: contacto@cert.inteco.es
Buzón de incidentes: incidentes@cert.inteco.es
Buzón de fraude electrónico: fraude@cert.inteco.es
Buzón cuestiones relativas a malware: analisis@cert.inteco.es

AEI SEGURIDAD

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

INTECO



INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

3- La Seguridad de la Información

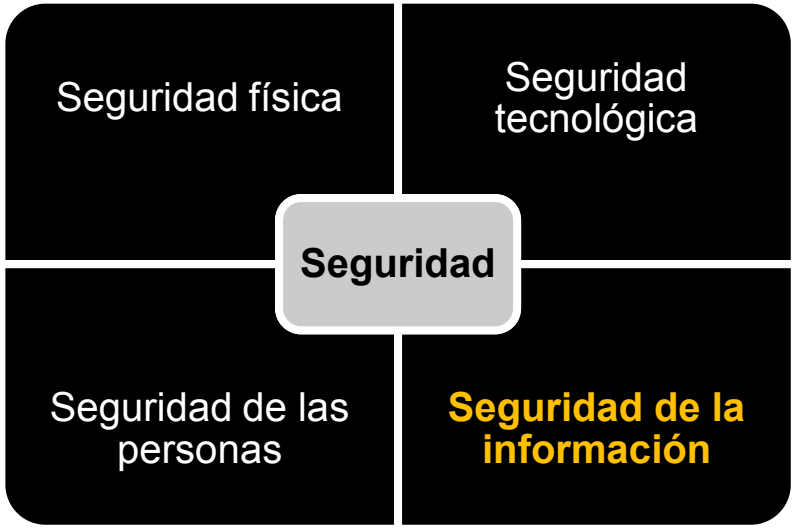
INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

a) Seguridad de la Información:

CONCEPTOS GENERALES

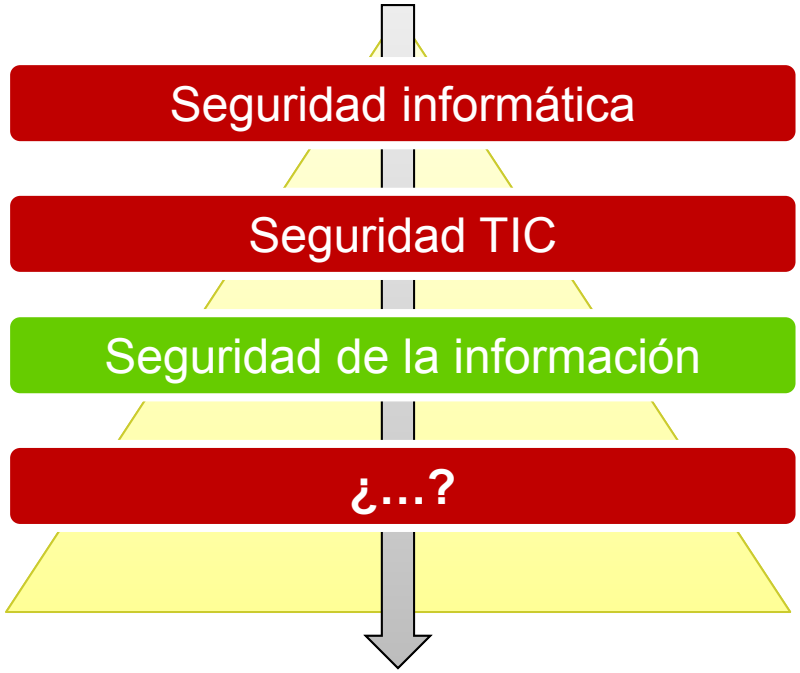
Enfoques de seguridad I



La seguridad afecta a los distintos activos de una organización

Enfoques de seguridad II

¿Qué camino seguir?



El futuro

Hay diferentes enfoques, pero al final, lo importante es proteger la información

¿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

Conceptos básicos de seguridad

- **Activo:** Recurso del sistema de información, necesario para que la organización funcione correctamente.
- **Amenaza:** Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en los activos.
- **Impacto:** Medir la consecuencia de materializarse una amenaza.
- **Riesgo:** Posibilidad de que se produzca un impacto determinado en un activo.
- **Vulnerabilidad:** Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.
- **Ataque:** Evento, exitoso o no que atenta sobre el buen funcionamiento del sistema.

Los tres conceptos mas importantes de seguridad

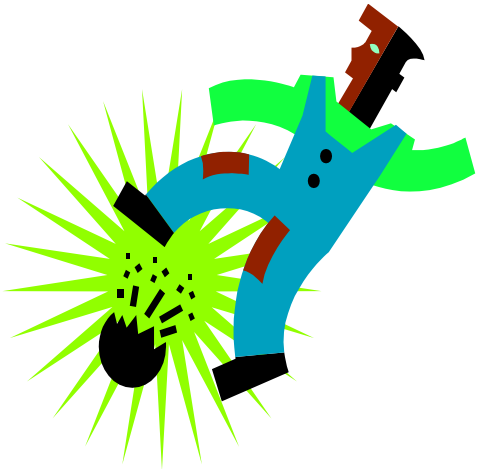
- **Confidencialidad**
- **Integridad**
- **Disponibilidad**

Conceptos importantes de seguridad

- **Confidencialidad**
  - Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
  - Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático

Conceptos importantes de seguridad

- **Integridad**
  - Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas
  - Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informatico



Conceptos importantes de seguridad

- **Disponibilidad**
  - Es la características, cualidad o condición de encontrarse a disposición de quienes deben acceder a ella.
  - Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático

¿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**

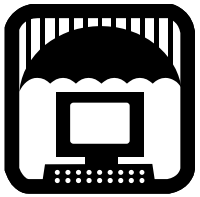
Es la protección de:

- ✓ **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

Seguridad Informática: Definición

- Un conjunto de métodos y herramientas destinados a proteger sistemas informáticos y la información ante cualquier amenaza.
- Tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

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”

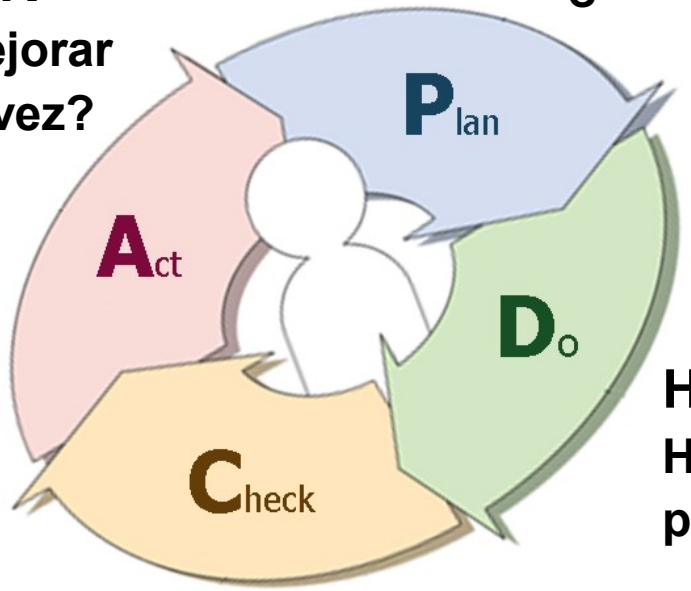
“No hay soluciones rápidas para la seguridad digital.”

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

Ciclo PHVA o PDCA (Plan, Do, Check, Act)

PLANIFICAR
¿Qué hacer?
¿Cómo hacerlo?

ACTUAR
¿Cómo mejorar la próxima vez?



HACER
Hacer lo planificado

VERIFICAR
¿Sucedió como se planificó?

- **Conocido como Ciclo Deming**
- **Muy ligado a calidad (sistemas de mejora continua)**

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 <u>riesgos</u> y las <u>amenazas</u>

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

b) Seguridad de la información: AAPP

Cuestiones fundamentales

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

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

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

¿Qué puede aportar a nuestro organización?

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

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

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

¿Mi organización 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

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

Medios e infraestructuras

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

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 organización 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 organización puede superar contingencias?

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

Desastres naturales

Incidentes provocados

Servicios críticos

Faltas de personal

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 (…)

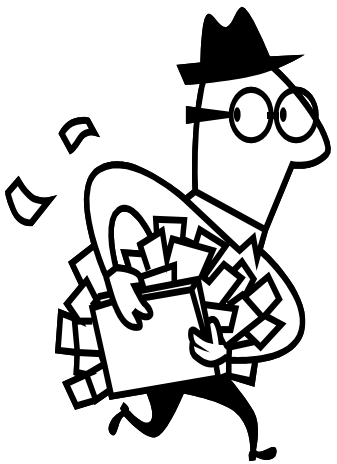
Fuego indiscriminado
Un incendio destruyó la mayoría de los contenidos e informaciones de una oficina, sólo se salvaron unos pocos CD. El escollo del asunto es que estos CD se habían fundido en el interior de sus cajas, fue un trabajo notable para los ingenieros (…)

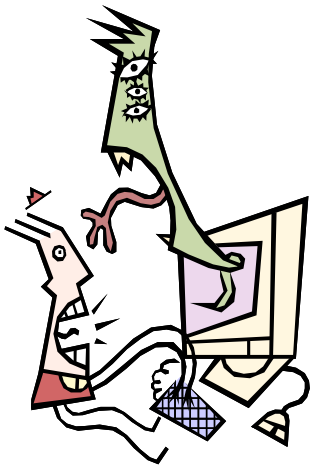
Roban un portátil de General Electric con datos de más de 50.000 trabajadores
General Electric reveló esta semana el robo, a principios de septiembre, de un ordenador portátil de la compañía con los nombres y datos de la Seguridad Social de 50.000 empleados.

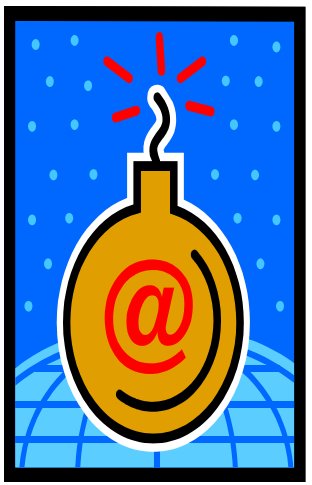
INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

C) Seguridad de la información: AMENAZAS TI





¿Qué puede amenazar mi organización?

Hacking, accesos no autorizados, harvesting, hacktivismo, etc.

Ingeniería social, spam, fraude bancario, robo de identidad, etc.

Malware, virus, troyanos, ad-ware, keyloggers, etc.

Fuga de información, robo de información, propiedad intelectual, espionaje industrial, etc.

Algunos ejemplos

Nueve de cada diez internautas españoles han sufrido algún percance en sus datos informáticos

Casi el noventa por ciento de los internautas españoles que participaron en una encuesta realizada por la empresa Recovery Labs han tenido en algún momento problemas con los ficheros de sus ordenadores, pero sólo el 6,6 por ciento ha recurrido a una empresa especializada en esta materia. El percance más habitual es la pérdida de datos (43 por ciento) (…)

Nuevo intento de estafa sobre los usuarios de la banca electrónica

Se ha detectado un nuevo envío masivo de e-mails que simula ser un mensaje de Banesto, donde se solicita a los clientes dirigirse a su sitio web para reactivar su cuenta atendiendo a un nuevo sistema de seguridad (…)

Aumenta el riesgo de virus en los teléfonos móviles

A medida que se estandariza cada vez más los sistemas sobre los que corren los llamados "smartphones" o teléfonos inteligentes, aumenta las probabilidades de que un gusano o virus creado especialmente para un determinado sistema se difunda por la red celular (…)

1 de cada 12 correos está infectado por el virus Mydoom

El Centro de Alerta Temprana sobre Virus y Seguridad Informática (CAT) ha elevado a "extremo" el nivel de peligrosidad del gusano Mydoom que continúa su expansión masiva por la Red y ha provocado en España más de 372.000 infecciones en día y medio. Este código malicioso ya ocupa el sexto puesto del ranking histórico de incidencias (…)

El 90% de las aplicaciones web son inseguras

Según un estudio realizado durante los últimos cuatro años por WebCohort, tan solo un 10 por ciento de las aplicaciones web pueden considerarse seguras ante cualquier tipo de ataque. En estos datos se incluyen sitios de comercio electrónico, banca online, B2B, sitios de administración, (…)

Anatomía de las amenazas TI – El antes

¿Quiénes eran?

- Personas con gran interés por la tecnología
- Los ordenadores no fueron el comienzo
- Existe una sub-cultura de la tecnología
- Distintos grupos: Phreakers, Hackers, Lamers, Crackers, Spamers, Hackitivistas

¿Por qué lo hacían?

- Era un reto y conseguirlo era el objetivo
- Una búsqueda de conocimiento
- Se trataba de ir contra las normas, romper las reglas
- Se buscaba el reconocimiento personal

Se trataba de un "juego". La satisfacción consistía básicamente en ser capaz superar barreras u obstáculos

Algunos ejemplos

El 'Gusano de Morris'
El primer 'gusano' de Internet nació la tarde del 2 de noviembre de 1988, cuando un estudiante estadounidense, Tappan Morris, liberó un programa creado por él mismo que infectó entre 2.000 y 6.000 ordenadores sólo el primer día, antes que fuera rastreado y eliminado. Para que su 'gusano' tuviera efecto, Morris descubrió dos errores en el sistema operativo UNIX, que le permitieron tener acceso no autorizado a miles de ordenadores (…)

Hacker Britanico Accede a la Nasa y Al Departamento de Defensa de Estados Unidos
Las autoridades estadounidenses dicen que McKinnon, de 42 años, intervino 97 computadoras de la NASA y otras.
McKinnon dijo haber estado buscando evidencia sobre ovnis y que tuvo éxito debido a las deficiencias en seguridad. Sus abogados han señalado que cualquier crimen supuesto ocurrió en suelo británico y en consecuencia debe ser juzgado en su país (…)

Un adolescente sería el hacker del Pentágono
Es apenas un adolescente. Pero desde su habitación en la casa que su familia tiene en el norte de San Francisco, en California, el joven logró ingresar en las computadoras del Pentágono en Washington poniendo en jaque todo el sistema de seguridad militar cibernética (…)

El joven detenido ayer confiesa ser el autor del virus Sasser
El joven de 18 años detenido por la policía alemana, bajo la sospecha de crear el virus informático "Sasser" confesó a la policía que había sido él quien programó el 'gusano', dijo un portavoz de la policía. "Hizo una confesión a la policía", dijo el portavoz Frank Federau (…)

Omar Kahn accedió al ordenador de su instituto y cambió sus suspensos por excelentes para acceder a la universidad
Kahn, de 18 debe responder a los 69 cargos que se le imputan y a una condena que le confinaría en la cárcel durante 38 años. El joven intentaba mejorar sus notas para acceder a la universidad y cambió sus calificaciones y las de otros 12 amigos suyos del prestigioso Tesoro High School de la localidad californiana de Las Flores. Además, Kahn consiguió el examen se acceso a la universidad (equivalente a la selectividad) y lo envió a sus compañeros (…)

Anatomía de las amenazas TI – En la actualidad

¿Quiénes son?

- Empleados y personal descontento
- Organizaciones criminales perfectamente coordinadas
- Delincuentes sexuales, pederastas, etc

¿Por qué lo hacen?

- Venganza personal, daño de imagen, etc
- Beneficio económico, chantaje, extorsión, etc
- Búsqueda de satisfacción sexual, etc

El escenario ha cambiado radicalmente, los "hackers" al uso, son el menos de nuestros males

Algunos ejemplos

MySpace revela que ha echado de su red a 90.000 depravados

MySpace ha cumplido con dos citaciones judiciales de sendos fiscales y ha entregado una lista de 90.000 depravados sexuales registrados a los que localizó y expulsó de su red social. La cifra supera en más de 40.000 nombres la estimación inicial de la compañía y ha sido calificada por Richard Blumenthal, uno de los fiscales, "como una revelación impactante“ (..)

La Policía ha detectado subastas falsas y casos de 'phising' en toda España por importe de tres millones de euros.

La Policía Nacional ha detenido a 76 personas acusadas de perpetrar estafas por Internet, en el mayor despliegue realizado por las Fuerzas de Seguridad contra el fraude en la Red. La investigación, denominada 'operación Ulises', se ha desarrollado hasta ahora en todas las comunidades autónomas, a excepción de Extremadura y de Melilla (…)

Florece el fraude online con tarjetas de crédito

Un informe sobre la economía clandestina, encargado y difundido por Symantec, la mayor empresa mundial de seguridad informática, advierte que esta actividad ilegal en Internet ha madurado para convertirse en un mercado global y eficaz. Aunque los números de las tarjetas de crédito se vendían entre 0,10 y 0,25 dólar por tarjeta, el límite de crédito promedio de tarjetas robadas anunciadas, fue superior a los 4.000 dólares (…)

Los ciberdelincuentes utilizan cada vez más troyanos para sus ataques

De esta forma, el 70% de los ataques con fines económicos durante 2007 se llevó a cabo con la técnica del "phishing", mientras que el 30% restante vino a través de troyanos. Este porcentaje se ajustó en 2008 (60% frente a un 40%) y es previsible que se iguale o incluso cambie este año, que ha empezado con el ataque más fuerte de los últimos cuatro años, el gusano "Downadup", también conocido como "Conficker".

Me han vaciado la cuenta

Me di cuenta cuando fui al cajero y observé un montón de movimientos en mi cuenta corriente que yo no había ordenado, había dos transferencias por importe de 1.000 y 1.200 euros...”; “...habían realizado varias trasferencias a otros bancos, robándome unos 12.000 euros”; “...comprobé el estado de mi cuenta a través de Internet y ví que mi saldo estaba al descubierto, habían realizado una transferencia que yo no había ordenado por importe de 2.432,43 euros”; “Me han robado todos mis pocos ahorros, 3.125 euros. Me dejaron solo 35 euros”...

Todos podemos ser ciber-delincuentes…

Antes

- Era necesario poseer conocimientos muy técnicos
- Había relativamente pocas herramientas disponibles
- La información estaba muy localizada y era poco conocida
- No existían las redes de banda ancha y las comunicaciones eran mucho mas limitadas

Ahora

- No es necesario poseer conocimientos
- Existen cientos de herramientas disponibles
- Hay mucha información y es muy fácil de localizar
- Se puede causar mucho daño con poco esfuerzo

Cualquiera puede ser una amenaza, solo hace falta una motivación, el resto está disponible

Todos somos un “objetivo”

Antes

- Sistemas militares, grandes empresas y universidades
- Ataques masivos, sin objetivos concretos
- Las redes y las comunicaciones eran limitadas y poco difundidas
- El número de ordenadores conectado a INTERNET era relativamente bajo

Ahora

- Todos tenemos algo “valioso” o “útil”
- Los ataques son sectorizados
- Tienen un objetivo definido
- La motivación económica se ha convertido en la principal

Cualquiera puede ser una amenaza, solo hace falta una motivación, el resto está disponible

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

- Contar con asesoramiento profesional
- Aplicar seguridad desde la AAPP
- 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

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

INTECO (cert)

ENISE 5
ENcuentro Internacional de SEguridad de la información

Asesoramiento legal y tecnológico de primer nivel

www.inteco.es

Conclusiones

La búsqueda del equilibrio entre libertad y seguridad es tarea de todos.

El sector privado y los agentes públicos han de **conocerse, cooperar y trabajar de forma conjunta**

El incremento de la importancia de la criminalidad informática ha de traducirse en un **incremento de medios personales y materiales** para su persecución.

Los riesgos del **"Mundo Conectado"** que preveíamos ayer, son una realidad hoy.

No hay sistema totalmente Aislado ni Invulnerable.

El paradigma de la seguridad tiene que cambiar hacia un **enfoque eminentemente proactivo**, desde el enfoque reactivo actual.

Es necesario **promover estándares**.

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

Para finalizar

"Me interesa el futuro porque es el sitio donde voy a pasar el resto de mi vida"

Woody Allen

Gracias por su atención

luis.hidalgo@inteco.es

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