POLÍTICA DE SEGURIDAD
y nociones básicas de seguridad

Javier Rojo Fernández

Jefe del Servicio de Seguridad de la DGTIC, Principado de Asturias.

Miembro del Grupo de trabajo de Seguridad del Comité Sectorial de Administración Electrónica y miembro del Comité de Seguridad de la Información de las Administraciones Públicas.

Javier.rojofernandez@asturias.org

La seguridad…

- Seguridad= mecanismo para garantizar que algo esté seguro, entendiendo por tal libre y exento de todo peligro, daño o riesgo.

  -La seguridad de un equipo o red informático es imposible de alcanzar al 100%, por tanto la pretensión es llegar a máximos de seguridad…pero la seguridad cuesta…hay que comprar sw. y hw., hay que formar a los usuarios y hay que diseñar los mecanismos de seguridad más convenientes..

Seguridad de la información

- La Seguridad de la Información se establece a través de un conjunto de medidas técnicas, organizativas y legales que permiten a una organización asegurar **la confidencialidad, autenticidad, integridad y disponibilidad de su información**.
- El concepto de seguridad de la información no debe confundirse con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Política de Seguridad de la Información

- **La Política de Seguridad de la Información** (en adelante PSI) tiene por objeto proteger la información, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la misma.
- Así mismo, pretende establecer las directrices que rigen la actuación de una persona o entidad en relación a la seguridad de los sistemas de información, entendiendo por sistema de información un conjunto organizado de recursos (físicos, lógicos, comunicación, datos, procedimientos y personal) destinados a recoger, almacenar, procesar, presentar o transmitir la información.
- La seguridad es un proceso de mejora continuo por lo que las PSI establecidas para la protección de la información deberán revisarse y adecuarse, de ser necesario, ante los nuevos riesgos que surjan, a fin de tomar las acciones que permitan reducirlos y en el mejor de los casos eliminarlos. Por tanto, la PSI de un Organismo debe mantenerse actualizada en todo momento, a efectos de asegurar su vigencia y nivel de eficacia.

Política de Seguridad de la Información de la Administración del Principado de Asturias

- El Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero, establece el marco regula-torio para las Política de Seguridad de la Información (PSI), y obliga a los órganos superiores de las Administraciones Públicas a dotarse formalmente de una PSI que permita la adecuada protección de la información. Dicha PSI debe mantenerse actualizada en todo momento, a efectos de asegurar su vigencia y nivel de eficacia.

- En este sentido la **Resolución de 19 de septiembre de 2014**, de la Consejería de Economía y Empleo, acuerda **la apro-bación de la actualización de la PSI de los sistemas de información en la Administración del Principado de Asturias**. (BOPA del 30/09/2014).

- Esta PSI aplica "*a todos los sistemas TIC (Tecnologías de la Información y las Comunicaciones) dentro del ámbito de gestión de la Dirección General de Tecnologías de la Información y las Comunicaciones, y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Administración del Principado*."

documentación de la PSI

- **Primer nivel**: documento de Política de Seguridad de la Información (anexo de la Resolución de 19 de septiembre de 2014). Marca las directrices generales en materia de seguridad de la información y es de obligado cumplimiento para todo el personal.
- **Segundo nivel:** Normativa de Seguridad. Normas que tomando como base el primer nivel de desarrollo, dan respuesta a qué se puede hacer y qué no, en relación a un cierto tema desde el punto de vista de la seguridad de la información y a qué se considera un uso apropiado o inapropiado de los activos.

Å Estas dos niveles de desarrollo son de obligado cumplimiento para todo el personal, se pueden consultar en la intranet Para tu trabajo - Seguridad de la Información - Política de Seguridad de la Información (PSI).

-Tercer nivel: Procedimientos operativos e Instrucciones técnicas. Son de obligado cumplimiento para el personal que gestiona y opera los sistemas de información y se almacenan en el repositorio establecido por la DGTIC para su manejo por el personal debidamente autorizado.

PSI-Normativa de Seguridad

Å La Normativa de Seguridad establece lo qué se puede hacer y lo qué no, en relación a un cierto tema desde el punto de vista de la seguridad de la información, y está compuesta por las siguientes normas:

- ï **Gestión de activos**
- ï **Control de acceso**
- ï **Seguridad física y del entorno**
- ï **Gestión de incidentes de seguridad**
- ï **Comunicaciones y operaciones**
- ï **Adquisición, desarrollo y mantenimiento**
- ï **Cumplimiento**
- ï **Gestión de la continuidad TI**
- ï **Seguridad ligada a los recursos humanos**

Entre estas normas cabe destacar, por afectar a todos los usuarios, la norma **“Gestión de activos”** en la que se establecen las reglas básicas para el empleo aceptable de los activos, entendiendo por activo cualquier recurso, tanto hardware como software, de los sistemas de información y sistemas informáticos o relacionado con éstos (por ejemplo; pc, identidades, aplicaciones, correo electrónico, internet…)

Å

Y cuáles son (algunos) de los riesgos para la seguridad y sus características

- Robo, pérdida o modificación de datos
- Alteración en el funcionamiento de aplicaciones, redes y máquinas

---

- Los mecanismo de actuación, además de catástrofes físicas, pueden ser "ataques", "virus" (malware), y todo etc. imaginable.
- Y la procedencia de la agresión: interna o externa.
- Y la motivación: voluntaria o involuntaria

peligrosa ignorancia o las creencias de los usuarios posiblemente erróneas

- Las empresas y consultorías de seguridad contratan a hackers para fabricar virus y ataques que justifiquen su negocio pero por fortuna si estoy protegido con antivirus actualizados, aunque sean piratas, me puedo considerar a salvo de todo peligro.
- Puedo tener mi equipo personal desprotegido porque lo que contiene mi ordenador no es de interés para nadie.
- Los datos que envío hacia Internet estarán de alguna forma cifrados y protegidos y nadie puede capturarlos; igualmente mis accesos a páginas o redes sociales sólo son controlados si estoy haciendo algo ilegal.
- Puedo navegar sin “infectarme” salvo si descargo ciertos archivos en páginas de intercambio de películas, música o pornográficas.

peligrosa ignorancia o las creencias entre los profesionales de la seguridad posiblemente erróneas

- Con talento y esfuerzo, impidiendo o filtrando el uso de internet y redes sociales, y disponiendo de antivirus, firewalls e IPS, tengo seguridad completa.
- Lo que a otros les ha funcionado a mí también me debe de funcionar.
- Quizás sea bueno para los responsables de sistemas, para el propio “negocio” y para los usuarios pero desde seguridad frenaré la nube o los dispositivos móviles porque son sinónimo de inseguridad.

Los términos (positivos)de los que hablan los de seguridad informática y otros puntos de discusión

- El Centro Criptológico Nacional y el INCIBE
- El convenio de Budapest y La Estrategia de Ciberseguridad
  http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

- Los protocolos seguros, las máquinas y aplicaciones de seguridad perimetral (IPS, firewalls, WAFs, filtros, antispams, antivirus), la actualización de los sistemas, la fortaleza y buen uso de las contraseñas, los bloqueos de equipos, las limitaciones de accesos a la nube, los sistemas de firma y certificados, la formación y concienciación del usuario/a.....

Los términos (negativos)de los que hablan los de seguridad informática y otros puntos de discusión

- Malware (virus, gusanos, troyanos, ataques de fuerza bruta...)
- Phishing
- Botnet
- Inyecciones de código
- Denegaciones de servicio (DoS, DdoS)
- APT (Flame, Stuxnet, Carbanak, Cryptolocker)
- Equation Group (¿me puedo fiar de alguien?)
- La desinformación y falta de concienciación del usuario/a

Algunas noticias recientes..

- 'Hackers' de Rusia y China lanzaron ataques contra cuatro ministerios (el país, dic. 2014)
- Los hospitales sufren un aumento exponencial de robos de información personal (MIT, sep. 2014 sobre el robo de datos de 4,5 millones de personas que habían recibido tratamiento en Community Health Systems (CHS, en EEUU), una empresa que gestiona más de 200 hospitales)
- Tu información médica es más codiciada por los hackers que tu tarjeta de crédito (WebSense, dic.2014, sobre el aumento en el 2014 en un 600% los ataques a datos y sistemas hospitalarios en EEUU)
- El CNI vigila el robo de historiales médicos por hackers chinos (El Confidencial, oct. 2014)

Y en el futuro qué..

- *La seguridad imposible*: ”El único sistema seguro es el que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada y rodeada por guardias armados” Eugene Spafford
- *Y nadie sabe, ni los mejores, por dónde evolucionará la tecnología*: “Podría parecer que hemos llegado a los límites alcanzables por la tecnología informática, aunque uno debe ser prudente con estas afirmaciones..” Von Neumann (el padre de los ordenadores programables, en 1950)
- Posiblemente las nuevas Políticas de Seguridad deberán tratar cuestiones como el BYOD, los dispositivos móviles, los Big data, los Open Data, el Cloud