Cooperación interadministrativa (Art. 13)

La **Dirección de Tecnologías** de la Información y las Comunicaciones **propondrá** a la **Secretaría de Estado de Administraciones Públicas** las [1]**líneas de actuación**, [2]**orientaciones comunes** y la [3]**creación de órganos de cooperación** necesarios para favorecer el **intercambio** de **ideas**, **estándares**, **tecnología** y **proyectos** orientados a **garantizar** la **interoperabilidad** y **mejorar** la **eficacia** y **eficiencia** en la prestación de los **servicios públicos** de las distintas **Administraciones Públicas**, que serán **tratadas** en la **Conferencia Sectorial** de Administraciones Públicas, en cuyo seno se establecerán.

PRINCIPIOS Y RECOMENDACIONES BÁSICAS EN CIBERSEGURIDAD DEL CCNCERT

Sobre CNN-CERT (Nº 1)

El **CCN-CERT** es la **Capacidad de Respuesta a Incidentes de Seguridad de la Información** del **Centro Criptológic Nacional**. Este servicio **se creó** en el año **2006** como el **CERT Gubernamental/Nacional español** y sus **funciones** quedan recogidas en la **Ley 11/2002** reguladora del Centro Nacional de Inteligencia, el **RD 421/2004** regulador del CCN y en el **RD 3/2010**, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), **modificado** por el **RD 951/2015**, de 23 de octubre.

De acuerdo a todas ellas, es **competencia** del **CCN-CERT** la **gestión** de **ciberincidentes*** que **afecten** a [1]**sistemas** del **Sector público**, a [2]**empresas** y **organizaciones** de **interés estratégico** para el **país** y a cualquier [3]**sistema clasificado**.

Su **misión** es contribuir a la **mejora** de la **ciberseguridad** española, siendo el **centro de alerta** y **respuesta nacional** que coopere y ayude a **responder** de forma **rápida** y **eficiente** a los **ciberataques** y a **afrontar** de forma **activa** las **ciberamenazas**.

Introducción (Nº 2)

La **concienciación**, el **sentido común** y las **buenas prácticas** son las **mejores defensas** para **prevenir** y **detectar contratiempos** en la **utilización** de sistemas de las Tecnologías de la Información y la Comunicación (**TIC**).

Se puede decir que **no existe** un **Sistema** que **garantice** al **100**% la **seguridad** del **servicio** que presta y la **información** que maneja **debido**, en gran medida, a las [1]**vulnerabilidades** que presentan las **tecnologías** y lo que es más importante, la [2]**imposibilidad** de disponer de los suficientes **recursos** para hacerlas frente.

Por tanto, siempre hay que **aceptar** un riesgo; el conocido como **riesgo residual**, asumiendo un **compromiso** entre el **nivel de seguridad**, los **recursos disponibles** y la **funcionalidad deseada**.

La **implementación de seguridad** supone **planificar** y **tener en cuenta** los **elementos** siguientes:

- **Análisis de Riesgos**. **Estudiar** los **posibles riesgos** y **valorar** las **consecuencias** de los mismos sobre los **activos**. (Información y servicio)
- **Gestión de Riesgos**. **Valorar** las diferentes **medidas** de **protección** y **decidir** la **solución** que más se adecue a la entidad. (Determinación del riesgo residual).
- **Gobernanza**. **Adaptar** la **operativa habitual** de la **entidad** a las **medidas de seguridad**.
- **Vigilancia**. **Observación continua** de las **medidas de seguridad**, así como la **adecuación** de las mismas a la aparición de **nuevas tecnologías**.
- **Planes de Contingencia**. **Determinación** de las **medidas** a adoptar ante un **incidente** de **seguridad**. La **combinación** de estas prácticas ayuda a **proporcionar** el **nivel** de **protección mínima** para mantener los datos a salvo.

Factores de amenaza (Nº 3)

La **generalización** del **uso** de los **medios electrónicos** en el normal desenvolvimiento de la sociedad **ha incrementado** la superficie de **exposición a ataques** y, **en consecuencia**, los **beneficios potenciales** derivados, lo que **constituye** sin duda uno de los **mayores estímulos** para los **atacantes**.

En los **últimos años** se ha mantenido la tendencia, **incrementándose** el **número**, **tipología** y **gravedad** de los **ataques** contra los **sistemas de información** del Sector público, de las empresas e instituciones de interés estratégico o de aquellas poseedoras de importantes activos de propiedad intelectual e industrial y, en general, contra todo tipo de entidades y ciudadanos.

Siguen estando **presentes** las acciones de **Ciberespionaje**, consistente en **ciberataques** originados o patrocinados por **Estados** y perpetrados **por ellos mismos** o por otros **actores a sueldo**, y siempre con la **intención** de **apropiarse** de **información sensible** o **valiosa** desde los puntos de vista [1]**político**, [2]**estratégico**, de [3]**seguridad** o [4]**económico**. El **ciberespionaje** presenta las siguientes **características** generales:

- **Origen** en **Estados**, **industrias** o **empresas**.
- **Utilización**, generalmente, de **ataques dirigidos** (Amenazas Persistentes Avanzadas).
- **Realizado contra** los **sectores público** (información política o estratégica) y **privado** (información económicamente valiosa).
- Con una **enorme dificultad** de **atribución**.
- **Persiguiendo obtener ventajas políticas**, **económicas**, **estratégicas** o **sociales**.

La **seguridad** en sus **actividades** hace **más difícil analizar** estos **ataques**. De hecho, en los últimos años las **tácticas**, **técnicas** y **procedimientos** han **evidenciado** una creciente **profesionalización** mostrando con claridad un **nuevo tipo** de comportamiento **delictivo crime-as-a-service**. Este pone a disposición de terceros la **posibilidad** de desarrollar **ciberataques** de **alto impacto** y, generalmente, con el **objetivo** de obtener **beneficios económicos ilícitos**.

Otro elemento a tener en cuenta es la **utilización** del **ciberespacio** en la **denominada Guerra Híbrida**, que mediante la **combinación** de diferentes **tácticas** busca **desestabilizar** y **polarizar** la **sociedad** de los **estados evitando** el **conflicto armado**. A efectos de **categorizar** la **amenaza**, la figura siguiente muestra la **Pirámide del Daño**, atendiendo a la **mayor** o **menor peligrosidad** de las **ciberamenazas**, según sea su origen.

Los ataques (APT)

Los **ciberataques** se han convertido en una **alternativa real** a las **herramientas convencionales de inteligencia**, debido a su [1]**bajo coste**, a la [2]**dificultad de probar su autoría** y al importante [3]**volumen de información** que puede ser obtenido por esta vía.

Los **grupos APT*** **buscan recabar** la mayor cantidad de **información** posible y útil de la **víctima**, con el objetivo de **preparar** un **ataque** lo más efectivo posible.

Los **parámetros** que **caracterizan** las **APT** se basan en:

- **Capacidad de desarrollo**: **exploits*** y **vulnerabilidades** utilizadas.
- **Persistencia**: tras **reinicios**, **actualizaciones** e incluso actividades de **formateo**.
- **Cifrado**: **métodos de cifrado** y **fortaleza de claves** para intercambiar la información exfiltrada.
- **Técnicas exfiltración**: **protocolos** utilizados para la **extracción** de **información**.
- **Ocultación**: técnicas de **rootkit*** utilizadas para **ocultarse**.
- **Resistencia a ingeniería inversa**: **técnicas** que **dificultan** el **análisis** del **código**.

La **información exfiltrada**, en función de la **motivación** de los **atacantes**, puede ser de índole muy **variada**: **económica**, **sensible**, **propiedad intelectual**, **secretos industriales** o de **estado**, etc.

La internet profunda (Nº 4)

Internet se ha visto **dividida** en la Internet **profunda*** y la **superficial**. La [1]**superficial** se compone de **páginas estáticas** o **fijas**, mientras que la [2]**web profunda** está compuesta de **páginas dinámicas** donde el **contenido** se **coloca** en una **base** de **datos** que se **proporciona** a **petición** del **usuario**.

La **principal razón** de la **existencia** de la **Internet profunda** es la **imposibilidad** para los **motores de búsqueda** (**Google**, **Bing**, etc.) de **encontrar** gran parte de la **información** existente en ella.

Un **subconjunto** de la **Internet profunda** sólo es **accesible** utilizando **determinados navegadores** web. Además, los **usuarios** han de **conocer** previamente la **dirección** a la que han de dirigirse.

La red TOR

The Onion Router (**TOR**): es un **proyecto** diseñado e implementado por la **Marina** de los **EEUU** con el fin de **fortalecer** las **comunicaciones** por **Internet** y **garantizar** el **anonimato** y la **privacidad**.

TOR permite a los usuarios **navegar** por la **web** de forma **anónima**. Los **datos no viajan** de forma **directa** sino **a través** de **varios nodos** que **facilitan** el **anonimato** de las **comunicaciones**. Existe un **directorio** de **nodos intermedios** con las **claves públicas asociadas** para poder **establecer** la **comunicación cifrada**.

TOR se encarga de **crear circuitos virtuales compuestos** por **3 nodos aleatoriamente** escogidos de su **red**. De manera que la **comunicación** entre **origen**, nuestro **equipo** y el **destino**, por ejemplo, una web, ha de **recorrer** los **3 nodos asignados**, a través de los cuales la información se transmitirá de **forma cifrada**.

El **elemento origen cifra** la **comunicación** con la **clave pública** del **último nodo** de la **ruta elegida** para que de esta **forma** sea el **único elemento** que pueda **descifrar** el **mensaje** y las **instrucciones** (nodos intermedios y sus claves públicas asociadas) para **llegar al destino**.

Se **eligen rutas aleatorias** donde los **datos** se **cifran** en **capas** y una vez que la **última capa** es tratada por un **nodo de salida**, se lleva a cabo la **conexión** con la **página web destino**.

Bitcoin

El **bitcoin** es una **moneda electrónica cifrada**, **descentralizada**, de **ordenador a ordenador**, donde el **control** se realiza, de forma **indirecta**, por los propios **usuarios a través** de **intercambios P2P***.

En lugar de acuñar una **moneda** o imprimir un **billete**, se **utiliza** una **cadena** de **caracteres criptográficos** que se **intercambian** a través de **billeteras digitales** (wallets) entre el **usuario** y el **vendedor** (intercambios P2P), lo que hace que esté **fuera** del **control** de cualquier **gobierno**, **institución** o **entidad financiera**.

Cada **transacción** con bitcoins se **registra** en una **gran base de datos** llamada **"BlockChain"***. Los **datos** se **guardan** en **bloques** y **cada bloque** nuevo debe **contener** el **hash** del **bloque anterior**. Por lo tanto, **cada bloque nuevo** que se une a la cadena **posee todo** el **historial** de la **transacción**.

Este **protocolo** se **sustenta** sobre una **red** de "**mineros**" que **controlan** la **moneda**. Los **mineros ponen** a **disposición** de la **red recursos de cómputo** y como **recompensa**, **reciben bitcoins**. Estos **mineros protegen** al **sistema** para que **no** haya transacciones de **anulación** (devolución de dinero ya gastado).

Esta **moneda** es **internacional**, **fácil de utilizar**, permite transacciones de forma **anónima** y como **riesgos**, representa un **mecanismo** muy práctico para **blanquear dinero** y **evadir impuestos** (exención fiscal).

Aplicaciones (Nº 5)

La **instalación** de **programas** puede **afectar** al **rendimiento** y la **seguridad** de los **dispositivos/equipos**. Debe mantenerse la integridad de los mismos y siempre hay que **instalar software autorizado** y **proporcionado** directamente por el **fabricante**.

Hay que tener en cuenta lo siguiente para **garantizar** la **seguridad** de nuestras **aplicaciones**:

- El **empleo** de **software legal** ofrece **garantía** y **soporte**, con independencia de las implicaciones legales de utilizar software no legítimo.
- **Certificación** del **programa** para su **compatibilidad** con el **sistema operativo** y las demás aplicaciones.
- **Instalación** y **mantenimiento** de **parches** y **actualizaciones** de **seguridad**, con especial atención a aquellas de **carácter crítico** (en los últimos meses la no actualización de los programas ha provocado numerosas brechas de seguridad).

- **Considerar** la superficie de **exposición asociada** a los **sistemas heredados** (legacy), **especialmente** aquellos que tienen **más** de una **década** de **antigüedad** por su **extremada vulnerabilidad**.

Los usuarios deben ser conscientes de que la **introducción** de **software no autorizado** puede causar la **infección** del **sistema más protegido**. Como **buenas prácticas** se indica lo siguiente:

- **Trabajar** habitualmente en el sistema como **usuario sin privilegios**, **no** como "**administrador**".
- **No ejecutar** nunca **programas** de **origen dudoso** o **desconocido**.
- Si se **emplea** un paquete de **software ofimático** capaz de **ejecutar macros**, hay que **asegurarse** de que esté **desactivada** su **ejecución automática**.

En cuanto a la **impresión** de **documentos**, hay que ser conscientes de que los **documentos** y **transacciones impresas** son **susceptibles** de **violaciones** de la **seguridad**.

Por lo tanto, resulta **fundamental** emplear **buenas prácticas** para **cumplir** la **normativa** existente en cada entidad y que la **información impresa** sea **segura** y **no accesible** por **personal no autorizado**.

Cifrado de datos

Cifrar los **datos** significa **convertir texto plano** en **texto ilegible**, **denominado texto cifrado**, **evitando** que la **información** sea **accesible por terceros no autorizados**. Para lo cual, **se necesita** de un **algoritmo de cifrado** y la existencia de una **clave**, que **permite** realizar el proceso de **transformación** de los **datos** y que debe **mantenerse** en **secreto**.

Existen múltiples **soluciones comerciales** para **cifrar** los **equipos informáticos**, clasificables en **3 tipos** atendiendo al **nivel** en el que actúan en el **sistema de archivos**:

- **Cifrado** de **disco**: es una tecnología que **cifra** el **disco** por **completo**, de esta manera el **sistema operativo** se **encarga** de **descifrar** la **información** cuando el **usuario** la **solicita**.
- **Cifrado** de **carpetas**: el cifrado se realiza a **nivel** de **carpeta**. El **sistema de cifrado** se **encargará** de **cifrar** y **descifrar** la **información** cuando se **utiliza** la **carpeta protegida**.
- **Cifrado** de **documentos**: el **sistema** se encarga de **mostrar** y **permitir** el **acceso** al **documento** solo para los usuarios **autorizados**, haciendo **ilegible** el contenido a los **no autorizados**.

Cortafuegos personales

Los **cortafuegos personales** son **programas** que **monitorizan** las **conexiones entrantes** y **salientes** del **equipo**. Están diseñados para **bloquear** el **acceso no autorizado** al mismo, pero **permitiendo** al mismo tiempo las **comunicaciones autorizadas**.

Lo **más complicado** de un **cortafuegos** es **configurarlo correctamente**, de modo que **no** se **bloqueen** las **conexiones legítimas** (navegación web, actualizaciones, correo electrónico, etc.).

Como criterio genérico, **no** se deben **permitir** las **conexiones** de fuentes **desconocidas**. Por tanto, deben **bloquear** todas las **conexiones entrantes** y sólo **permitir** aquellas que **se indiquen expresamente** sobre la base de un conjunto de normas y criterios establecidos. Un **cortafuegos** correctamente configurado **añade** una **protección** necesaria que **dificulta** los **movimientos laterales no autorizados** por la **red**, pero que **en ningún caso** debe **considerarse** como **suficiente**.

Aplicaciones antimalware

Entre las **acciones** que puede provocar un **código malicioso** o **malware** se encuentran: [1]**borrado** o [2]**alteración** de **archivos**, [3]**consumo** de **recursos** del equipo, [4]**acceso no autorizado** a archivos, [5]**infección remota** de los equipos, etc.

Las **funciones mínimas** que se pueden esperar en una herramienta **antimalware** (antivirus) son:

- **Filtrado entrante** y **saliente** de **contenidos maliciosos**.

- **Protección** en el **correo electrónico**, en la **navegación** y en las **conexiones** de todo tipo.
- **Analizar** los **ficheros** en **dispositivos removibles** como **discos externos** o **memorias USB**.
- Permitir **programar análisis exhaustivos** cada cierto tiempo.

Las **aplicaciones antimalware** deben disponer de **actualizaciones** y **ser productos** de **casas comerciales de confianza** que permitan una combinación de los siguientes **métodos**:

- Escáner de **acceso**: permite **examinar** los **archivos** cuando son **abiertos**.
- Escáner a **demanda**: **análisis** en base a un **calendario establecido**.
- Escáner de **correos electrónicos**: en dispositivos de **protección de perímetro** o **servidores de correo**.
- **Control de firmas**: permite **detectar cambios no legítimos** en el contenido de un **archivo**.
- **Métodos heurísticos**: **búsqueda** de **anomalías** en los **archivos** y **procesos** en base a experiencias previas de comportamiento del malware.

Pero una **aplicación antimalware** sola **no** es **suficiente**; hay que proporcionar un **enfoque centralizado** (cliente-servidor) para **proteger** todos los **puntos finales** (servidores, sobremesas, portátiles, teléfonos inteligentes, etc.) **conectados** a la **red**. Algunos **proveedores** ofrecen **sistemas** de **Endpoint Security*** que incluyen **antivirus**, **cortafuegos** y **otro software** de seguridad.

Borrado seguro de datos

Se puede pensar que un simple formateo del disco duro impedirá que los datos almacenados en el mismo puedan ser recuperados. Sin embargo, **hay aplicaciones** que **permiten deshacer** el **formateo** de una **unidad** existiendo **incluso métodos** para **recuperar** los **datos** de los **discos**, **aunque** estos hayan sido **sobrescritos**.

Si se quiere **garantizar** que **no** se está **distribuyendo información sensible**, se deben **sobrescribir** los **datos** siguiendo un método (**patrón de borrado**) que **no permita** su **recuperación** de modo alguno.

Para tal fin, es necesario **realizar diversas pasadas de escritura** sobre cada uno de los sectores **donde** se **almacena** la **información**.

En el caso de **fotografías digitales**, archivos de **audio** o **vídeo** y **documentos ofimáticos** existen **metadatos*** que pueden **almacenar información oculta** y **no visible usando** la configuración estándar de las **aplicaciones**, necesitando de una **configuración específica** o incluso un **software concreto** para **revelar** esos **datos**.

Estos **metadatos** son útiles ya que **facilitan** la **búsqueda** de **información**, **posibilitan** la **interoperabilidad** entre **organizaciones**, **proveen** la **identificación digital** y **dan soporte** a la **gestión** del ciclo de vida de los **documentos**.

Sin embargo, el **borrado** de **metadatos** o **datos ocultos** mediante **procedimientos** y **herramientas** de **revisión** y **limpieza** de **documentos/archivos** es fundamental para **minimizar** el **riesgo** de que se **revele información sensible** en el almacenamiento e intercambio de información.

Navegación segura (Nº 6)

La **comunicación** en **Internet** se sustenta en una **idea básica**: **clientes** (ordenadores, teléfonos, tabletas, ...) **llaman** a **servidores** (web, bases de datos...) que **proporcionan información**. Esta **comunicación** se lleva a cabo **a través** de un **protocolo** (**http**, **https**, **ftp**, etc.).

El **cliente** está **identificado** en la **red** a través de una **dirección IP** (TCP/IP) y cada vez que se **conecta** a un **sitio web**, éste **conoce automáticamente** la **dirección IP**, **nombre de máquina**, la **página de procedencia**, etc.

Se **produce** un **intercambio** de **información** que habitualmente **no** es **visible** donde el **navegador web** es el que **facilita** la mayoría de estos **datos**:

- Un alto porcentaje de los **usuarios no** es **consciente** de la cantidad de **información** que, de forma **inadvertida** e **involuntaria**, está **revelando** a **terceros** al hacer **uso** de **Internet**.