GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN-CERT

CCN-CERT BP/01

Principios y recomendaciones básicas en Ciberseguridad

Octubre 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.09.04 17:19:01 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). 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 **sistemas del Sector público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, 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.

2. INTRODUCCIÓN

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 vulnerabilidades que presentan las tecnologías y lo que es más importante, la 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.

3. FACTORES DE LA AMENAZA

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**, consistentes 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 político, estratégico, de seguridad o económico.

A modo de resumen, podemos decir que el ciberespionaje presenta las siguientes características generales:

- Origen en Estados, industrias o empresas.
- Utilización, generalmente, de ataques dirigidos (Amenazas Persistentes Avanzadas).
- 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, al que podríamos denominar *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, pero a la vez consiguiendo que dichas acciones aparezcan como deliberadamente ambiguas.

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.

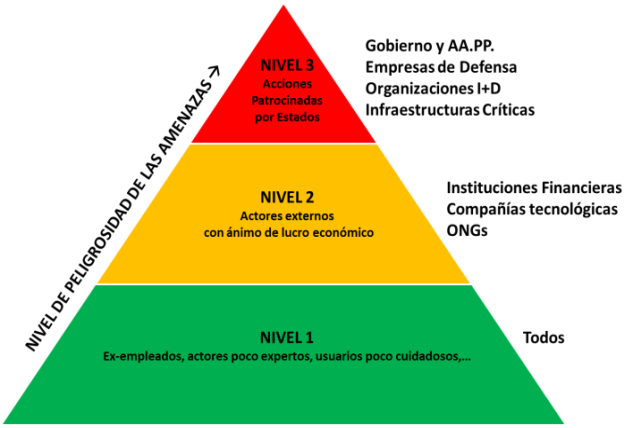


Figura 1.- Pirámide del Daño

3.1 ATAQUES DIRIGIDOS (APT)

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

En este sentido, los grupos APT[1] (Advanced Persistent Threat) buscan recabar la mayor cantidad de información posible y útil de la víctima, con el objetivo de preparar un ataque lo más efectivo posible.

Figura 2.- Fases de una APT

Los parámetros que caracterizan las técnicas del ataque (APT) se basan en:

- **Capacidad de desarrollo**: *exploits*[2] 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*[3], *bootkit* utilizadas para ocultarse.

[1] Amenazas Persistentes Avanzadas.

[2] Programa o código que se aprovecha de una vulnerabilidad en una aplicación o sistema para provocar un comportamiento no deseado o imprevisto.

- **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.

4. LA INTERNET PROFUNDA

Internet se ha visto dividida en la Internet profunda y la superficial. La superficial se compone de páginas estáticas o fijas, mientras que la 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, Yahoo!, Bing, etc.) de encontrar o indexar gran parte de la información existente en ella.

Un subconjunto de la Internet profunda sólo es accesible utilizando determinados navegadores web. Es el caso, por ejemplo, de la red *TOR*, donde los usuarios han de disponer del software de navegación adecuado para poder acceder a dominios que son inaccesibles desde un navegador convencional.

Además, los usuarios han de conocer previamente la dirección a la que han de dirigirse. Existen listados con algunos dominios públicos de la red *TOR* que los usuarios pueden consultar (The Hidden Wiki, Silk Road, Agora, Evolution, Middle-Earth, etc…) y buscadores como "*Grams*" (el Google de la *dark web*).

4.1 LA RED TOR

The Onion Router (TOR) fue un proyecto diseñado e implementado por la Marina de los Estados Unidos, lanzado en 2002, con el fin de fortalecer las comunicaciones por Internet y garantizar el anonimato y la privacidad.

A diferencia de los navegadores de Internet convencionales, *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 tres (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 tres (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.

[3] Herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo

4.2 BITCOINS

Bitcoin es una moneda electrónica cifrada, descentralizada, de ordenador a ordenador (*peer-to-peer*) 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, existen cajeros automáticos y cada vez hay más vendedores/comercios que la aceptan. Como riesgos, representa un mecanismo muy práctico para blanquear dinero y evadir impuestos (exención fiscal).

5. APLICACIONES

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.

- 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.

5.1 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[4] para cifrar los equipos informáticos, clasificables en tres (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.

5.2 CORTAFUEGOS PERSONALES

Los cortafuegos[5] personales o *firewall*s 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.

5.3 APLICACIONES ANTIMALWARE

[4] Véase **Guía CCN-STIC-955B Recomendaciones de empleo de GPG** (https://www.ccn-cert.cni.es/series-ccn-stic/900-informes-tecnicos/1816-ccn-stic-955b-recomendaciones-de-empleo-de-gpg/file.html)

[5] Véase **Guía CCN-STIC-408 Seguridad Perimetral-Cortafuegos** (https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html)

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

Las funciones mínimas que se pueden esperar en una buena **herramienta antimalware**[6] (más conocidas por **antivirus**) son las de filtrado entrante y saliente de contenidos maliciosos, protección en el correo electrónico, en la navegación y en las conexiones de todo tipo en redes profesionales o domésticas. También deben ser capaces de analizar los ficheros en dispositivos removibles como discos externos o memorias USB y permitir programar análisis exhaustivos cada cierto tiempo.

Las aplicaciones antimalware deben disponer de actualizaciones regulares (últimas definiciones y motores de búsqueda) 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.

5.4 BORRADO SEGURO DE DATOS[7]

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. Para simplificar la tarea, lo más sencillo es utilizar alguna aplicación especializada que permita eliminar la información de forma sencilla.

[6] El CCN-CERT tiene disponible para los usuarios registrados de su portal la **plataforma multiantivirus MARIA** para el análisis estático de código dañino a través de múltiples motores antivirus y antimalware para plataformas Windows y Linux (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/maria-publico.html)

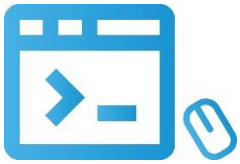
[7] Véase **Guía CCN-STIC-305 Destrucción y sanitización de soportes informáticos** (https://www.ccn-cert.cni.es/series-ccn-stic/300-instrucciones-tecnicas/60-ccn-stic-305-destruccion-y-sanitizacion-de-soportes-informaticos/file.html)

En el caso de fotografías digitales, archivos de audio o vídeo y documentos ofimáticos existen metadatos[8] 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.

6. NAVEGACIÓN SEGURA



La comunicación en Internet se sustenta en una idea básica: clientes (ordenadores, teléfonos, tabletas, …) llaman a servidores (web, bases de datos…) que proporcionan (sirven) información. Esta comunicación se lleva a cabo a través de un protocolo (http, https[9], 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.
- Cada vez que se visita un sitio web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio.
- Al sitio web le resulta trivial averiguar la dirección de Internet de la máquina desde la que se está accediendo, sistema operativo, etc.
- Con ayuda de las "*cookies*" se puede personalizar aún más la información recabada acerca de los visitantes, registrando las páginas más visitadas, preferencias, tiempo de la visita, software instalado, etc.

Un navegador web, en favor de la máxima usabilidad, permite que se acceda a información aparentemente inofensiva.

- La dirección IP pública con que se conecta el usuario.
  - Tu dirección IP es xxx.xxx.xxx.xxx.
  - Tu navegador está utilizando 128 bits de clave secreta SSL.
  - El servidor está utilizando 1024 bits de clave pública SSL.
- La resolución de la pantalla.

[8] Véase **Guía CCN-STIC-835 Borrado de Metadatos en el marco del ENS** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2031-ccn-stic-835-borrado-de-metadatos-en-el-marco-del-ens/file.html)

[9] Véase **Informe de Buenas Prácticas CCN-CERT BP-01/17 Recomendaciones implementación HTTPS** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html)

- Qué páginas se leen y cuáles no, qué figuras se miran, cuántas páginas se han visitado, cuál fue el sitio recientemente visitado "*Referer*".
- El valor del campo "*User-Agent*".
  - Mozilla/5.0 (Windows NT 6.1; rv:16.0) Gecko/20100101 Firefox/16.0
- El idioma y zona GMT del sistema operativo.
- Si se aceptan o no "*cookies*".
- Las fuentes cargadas en el sistema o *plugins* instalados y activados.

Algunas **recomendaciones** para mantener una **navegación segura**[10] son:

- Acceder únicamente a sitios de confianza.
- Mantener actualizado el navegador a la última versión disponible del fabricante.
- Configurar el nivel de seguridad del navegador según sus preferencias.
- Descargar los programas desde sitios oficiales para evitar suplantaciones maliciosas.
- Configurar el navegador para evitar ventanas emergentes.
- Utilizar un usuario sin permisos de "*Administrador*" para navegar por Internet e impedir la instalación de programas y cambios en los valores del sistema.
- Borrar las "*cookies*", los ficheros temporales y el historial cuando se utilicen equipos ajenos para no dejar rastro de la navegación.
- Desactivar la posibilidad "*script*" en navegadores web, como Firefox (NoScript) o Chrome (NotScript), para prevenir la ejecución de los mismos por parte de dominios desconocidos.
- Se recomienda hacer uso de HTTPS (SSL/TLS) frente a HTTP incluso para aquellos servicios que no manejen información sensible. Algunas funcionalidades como HSTS y extensiones como *HTTPS Everywhere* servirán de gran ayuda para garantizar el uso preferente de HTTPS sobre HTTP durante la navegación web.
- En la medida de lo posible, emplear máquinas virtuales para navegar por Internet.

Además, hay que tener en cuenta que los sistemas de navegación anónima permiten el uso de algunos servicios de Internet, principalmente los basados en navegación web (http/https), de forma desvinculada de la dirección IP origen de la comunicación.

- Anonimizadores.
  - Actúan como un filtro entre el navegador y sitio web que se desea visitar.
  - Al conectarse al anonimizador, se introduce la URL a visitar y entonces éste se adentra en la red filtrando cookies, javascripts, etc.
- Servidores Proxy.
  - Un servidor proxy actúa de pasarela entre la máquina cliente e Internet.
  - El servidor proxy actúa de intermediario, se encarga de recuperar las páginas web en lugar del usuario que navega.
- Túneles de Cifrado (TOR, VPS y Darknets).

[10] Véase **Informe de Buenas Prácticas CCN-CERT BP-06/16 Navegación segura** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html)

- Red de "túneles" por las cuales los datos de navegación, debidamente cifrados, atraviesan múltiples nodos hasta llegar a su destino.

7. CORREO ELECTRÓNICO

Actualmente el correo electrónico[11] sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información a pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros.

El incremento y efectividad de la ingeniería social para engañar a los usuarios por medio de correos electrónicos ha modificado el paradigma de la seguridad corporativa.

Actualmente los cortafuegos perimetrales y la securización de los servicios expuestos a Internet no son contramedidas suficientes para proteger una organización de ataques externos.

Algunas **recomendaciones**[12] para utilizar el correo electrónico de forma segura:

- No abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
- No confiar únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
- Antes de abrir cualquier fichero descargado desde el correo, hay que asegurarse de la extensión y no fiarse del icono asociado al mismo.
- No habilitar las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
- No hacer clic en ningún enlace que solicite datos personales o bancarios.
- Tener siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los *plugins*/extensiones instaladas).
- Utilizar herramientas de seguridad para mitigar *exploits* de manera complementaria al software antivirus.
- Evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
- Utilizar contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas y si es posible utilizar doble autenticación.
- Cifrar los mensajes de correo que contengan información sensible.
-

[11] Véase **Guía CCN-STIC-814 Seguridad en correo electrónico** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/524-ccn-stic-814-seguridad-en-servicio-de-correo/file.html)

[12] Véase **Informe de Buenas Prácticas CCN-CERT BP-02/16 Correo electrónico** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico/file.html)

8. VIRTUALIZACIÓN

La virtualización se entiende como la recreación de un recurso físico (hardware) o lógico (software), por medio de un hipervisor (hypervisor) que permite su ejecución por más de un entorno al mismo tiempo. En el entorno de máquinas virtuales, el hipervisor permite el uso simultáneo del hardware en más de un sistema operativo.

El apogeo de la virtualización ha llegado con la **utilización de la nube**[13], donde este sistema de reparto de los recursos se hace casi indispensable. Aunque ya existían múltiples sistemas de muchos fabricantes, el desarrollo y avances de los mismos se han incrementado de una forma exponencial. Actualmente se puede optar, entre otros, por XenServer de Citrix, VMware ESXi de Dell, VirtualBox de Oracle, Oracle VM Server e Hyper-V de Microsoft.

La seguridad en la virtualización tiene la misma premisa que cualquier otro sistema, que es la *minimización de la superficie de ataque*. No obstante, cuenta con particularidades que hacen que la aseguración sea más difícil como por ejemplo la multitud de recursos compartidos o los sistemas operativos que funcionan simultáneamente con sus propias aplicaciones sobre una misma máquina física.

Como norma general, es **conveniente seguir las siguientes indicaciones** a la hora de configurar un *host* de máquinas virtuales:

- Tener instaladas en el sistema operativo las últimas actualizaciones de seguridad.
- Tener la última reversión disponible del programa de virtualización.
- Si es posible, tener al menos un adaptador de red en exclusiva para la infraestructura de virtualización.
- Crear un entorno de laboratorio aislado del entorno de producción.
- Disponer de un grupo de seguridad para gestionar la plataforma de seguridad.
- Proteger los dispositivos de almacenamiento en los que guardan los archivos de recursos y de definición de la máquina virtual.
- Mantener estancos a los administradores de los *guest* respecto a los de *host*.

Para la creación de *guest*, se recomienda seguir las siguientes normas:

- Hacer un esquema previo de lo que será la infraestructura de virtualización.
- Dimensionar la creación de máquinas virtuales a las necesidades reales y a los recursos de hardware disponibles en el *host*.
- Cifrar los ficheros de máquinas virtuales, instantáneas y discos duros virtuales destinados al almacenamiento de la plataforma de virtualización.
- Instalar las últimas actualizaciones de seguridad en cada sistema operativo *guest*.
- Valorar la instalación de los agentes de hipervisor, tipo Guest Additions, y en caso de hacerlo, mantenerlos actualizados.
- Asegurar con antimalware y firewalls todos los sistemas operativos invitados.

[13] Véase **Guía CCN-STIC-823 Seguridad en entornos Cloud** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html)

- Conectar DVD, CD y medios de almacenamiento externos solo cuando sea necesario y desactivar tras su uso.
- Mantener activas solamente las máquinas virtuales imprescindibles.
- Usar para la conexión con la red corporativa o con Internet una interfaz de red virtual diferenciada que se deberá desactivar cuando no se vaya a utilizar.
- Cifrar los medios de almacenamiento externos que contengan ficheros de virtualización de respaldo y custodiarlos convenientemente.

9. SEGURIDAD EN DISPOSITIVOS MÓVILES

El incremento de posibilidades y capacidades que llevan asociados los dispositivos móviles[14] en la actualidad implica igualmente mayores riesgos para la seguridad de los mismos. Es muy importante que los usuarios sean conscientes de la importancia de la seguridad en los aparatos móviles y los peligros que pueden llevar consigo su mal uso.

Es conveniente seguir los siguientes consejos[15]:

- Establecer un método seguro para desbloquear el terminal, por ejemplo, utilizando una *passphrase* robusta.
- Es recomendable eliminar las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance.
- Deshabilitar las conexiones inalámbricas (WiFi, Bluetooth, etc.) y todas aquellas innecesarias mientras no vayan a utilizarse.
- Mantener actualizado el software del dispositivo y utilizar una configuración de seguridad aprobada por el responsable TIC de la entidad.
- Tener cuidado con el acceso y las solicitudes de permisos de las aplicaciones que se ejecuten en el teléfono.
- Ignorar y borrar mensajes (SMS, MMS u otros) de origen desconocido que invitan a descargar contenidos o acceder a sitios web.
- Activar el acceso mediante PIN a las conexiones Bluetooth y configurar el dispositivo en modo oculto. No aceptar conexiones de dispositivos no conocidos.
- Descargar aplicaciones únicamente desde las tiendas oficiales. En ningún caso, descargar software de sitios poco fiables y en todo caso solicitar al responsable TIC de la entidad las aplicaciones necesarias.
- Evitar realizar *jailbreaking* o *rooting* del terminal, ya que puede comprometer y reducir considerablemente la seguridad del teléfono a pesar de ser tentador para acceder a aplicaciones o servicios específicos.
- Utilizar una red privada virtual (VPN[16]) para proteger el tráfico de datos desde el dispositivo móvil hasta la infraestructura de la entidad. Siempre es una buena práctica para evitar la posible monitorización por parte de intrusos.

[14] Véase diversas **Guías CCN-STIC 450-451-452-453-454 y 455 Seguridad en dispositivos móviles** (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html)

[15] Véase **Informe de Buenas Prácticas CCN-CERT BP-03/16 Dispositivos móviles** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1807-ccn-cert-bp-03-16-dispositivos-moviles-1/file.html)

- Evitar en lo posible el uso de impresoras, faxes o redes WiFi públicas, como las ofrecidas en hoteles o aeropuertos, salvo que se disponga de las herramientas necesarias para asegurar sus comunicaciones.
- Muchos teléfonos móviles y cámaras digitales añaden las coordenadas GPS en la información de las imágenes tomadas, por lo que es oportuno limitar la compartición de las imágenes en la red o bien utilizar aplicaciones que eliminen dicha información.
- Separar las comunicaciones personales de las profesionales es una buena práctica de seguridad. Disponer de compartimentos estancos en un solo dispositivo aumentará la seguridad.
- Implementar la gestión centralizada de dispositivos móviles mediante el empleo de agentes *MDM* (Mobile Device Management).
- Para manejar información sensible, utilizar únicamente soluciones aprobadas por el responsable de seguridad TIC de la entidad.

10. SEGURIDAD EN REDES INALÁMBRICAS

Si se trabaja con una red inalámbrica, para maximizar la seguridad en la red WiFi es necesario prestar atención a las siguientes recomendaciones[17]:

- Cambiar la contraseña de acceso por defecto para la administración del Punto de Acceso.
- Modificar el SSID configurado por defecto no empleando nombres que pudieran identificar a la entidad y que permitan pasar desapercibidos con el entorno.
- Ocultar el identificador SSID al exterior dificulta obtener el nombre de la red, aunque la trazabilidad de los clientes sigue siendo posible con independencia de la ocultación del SSID.
- Activar el filtrado de direcciones MAC de los dispositivos WiFi para permitir que se conecten a la red los dispositivos con las direcciones MAC especificadas.
- Configurar WPA2-AES en el modo de confidencialidad de datos, obteniendo autenticación y cifrado de datos robusto.
- Limitar la cobertura WLAN. Una antena multidireccional ubicada en el centro de la casa/oficina es la opción más común.
- Desconectar la red cuando no se utilice. Si bien no es práctico hacerlo diariamente, es muy recomendable durante largos períodos de inactividad.
- Desactivar UPnP (Universal Plug and Play) cuando su uso no sea necesario, para evitar que un código dañino de la propia red lo utilice para abrir una brecha en el cortafuegos del router y permitir así que otros atacantes accedan a él.
- Actualizar el "*firmware*" del router periódicamente, pues muchas de las actualizaciones y parches que se van incorporando afectan a la seguridad.

[16] Véase **Guía CCN-STIC-836 Seguridad en redes privadas virtuales (VPN)** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html)

[17] Véase **Guía CCN-STIC-816 Seguridad en Redes Inalámbricas** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html)

- Usar direcciones IP estáticas o limitar el número de direcciones reservadas (DHCP) cuando sea posible, para evitar que usuarios no autorizados puedan obtener una dirección IP de la red local.
- Activar el cortafuegos del router, para que sólo los usuarios y los servicios autorizados puedan tener acceso a la red.
- Activar la opción de registro (*login*) para el router y analizar periódicamente el historial de accesos.
- Es recomendable cambiar el DNS que por defecto trae configurado el router por otro que preserve la privacidad del usuario y mejore su seguridad, por ejemplo, *DNSCrypt*.

11. MENSAJERÍA INSTANTÁNEA

Las aplicaciones de mensajería instantánea permiten enviar mensajes de texto mediante la conexión a Internet (WhatsApp[18] y Telegram[19] son las más conocidas). En el caso de WhatsApp, lanzada al mercado en el año 2009, por ejemplo, gestiona actualmente alrededor de mil millones de mensajes al día.

Se tratan de plataformas que al poder tener un comportamiento semejante al de una red social convencional son propensas a su expansión. Además, el uso compartido de la información personal y la escasa percepción de riesgo que los usuarios tienen con la seguridad las han convertido en un entorno atractivo para intrusos y ciberatacantes que intentan obtener datos e información de sus usuarios.

Uno de los fallos más comunes en las aplicaciones de mensajería es la forma que utilizan para borrar las conversaciones almacenadas en el teléfono ya que no implica la eliminación directa de los mensajes, sino que estos quedan marcados como libres, de tal forma que puedan ser sobrescritos por nuevas conversaciones o datos cuando sea necesario siendo accesible por técnicas forenses.

Además, hay que tener en cuenta las implicaciones cuando se tenga activa la opción de copia de seguridad (almacenando una posible conversación ya borrada) que podría ser recuperada en un futuro.

Durante el establecimiento de conexión con los servidores, se puede intercambiar en texto claro información sensible acerca del usuario quedando expuesta a cualquiera en el caso de utilizar redes WiFi públicas o de dudosa procedencia.

- Sistema operativo del cliente.
- Versión de la aplicación en uso.
- Número de teléfono registrado.

Al utilizar una conexión basada en redes privadas virtuales (VPN), todos los datos enviados y recibidos pasan cifrados entre el emisor y el receptor, añadiendo una nueva capa de seguridad para evitar posibles atacantes que estén interceptando el tráfico de red (*man-in-the-middle*).

[18] Véase **CCN-CERT IA-21/16 Riesgos de uso de WhatsApp** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html)

[19] Véase **CCN-CERT IA-23/17 Riesgos de uso de Telegram** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2443-ccn-cert-ia-23-17-riesgos-de-uso-de-telegram-1/file.html)

Por otro lado, la base de datos de conversaciones, ficheros, mensajes, así como otros datos que manejan este tipo de aplicaciones se almacena de forma local dentro del teléfono, con independencia de que se tenga la opción de "*backup*" en la nube activada en el dispositivo.

Aunque la información se almacena cifrada en local, existen multitud de aplicaciones[20] que por ejemplo para *WhatsApp* permiten de una forma sencilla el descifrado de la información contenida, tanto en versión local para un equipo, como a través de una aplicación en el teléfono o interfaz web.

Para evitar que un atacante pueda tener acceso a toda la información privada que se almacena en el teléfono hay que prestar especial atención a qué aplicaciones de terceros se instalan, así como el acceso físico de otra persona al terminal.

En el caso de intercambio de datos con redes sociales, como *WhatsApp* y *Facebook*, y a pesar de que los mensajes, fotos e información de perfil no serán objetivos a compartir, otra información como número de teléfono, contactos, hora de última conexión, así como tus hábitos de uso de la aplicación pueden ser compartidos.

Insistiendo en las **recomendaciones** indicadas para dispositivos móviles, será necesario adoptar determinadas precauciones en el uso de aplicaciones de mensajería instantánea como:

- Mantener el teléfono bloqueado. De esta forma, se reducirá el riesgo si el dispositivo cae en las manos equivocadas.
- Sería recomendable eliminar las previsualizaciones de los mensajes y extremar las medidas cuando no se disponga del teléfono al alcance.
- En la medida de lo posible, se recomienda la configuración de las aplicaciones para solo recibir mensajes de personas autorizadas.
- Desactivar la conectividad adicional del teléfono cuando no se vaya a utilizar, como podría ser la conexión WiFi o Bluetooth, ya que además de reducir el consumo de batería, reduce la posible superficie de ataque sobre el dispositivo.
- Utilizar aplicaciones de mensajería instantánea cuyo código fuente esté abierto a la comunidad y haya sido revisado. En ese sentido existen alternativas que, además, aseguran la confidencialidad en las comunicaciones, cifrando el tráfico extremo a extremo (*e2e*), un ejemplo es *Signal*.

12. REDES SOCIALES

Las redes sociales no solo han cambiado la manera en que los ciudadanos se informan y se comunican entre sí, sino también la manera en que los Gobiernos y organizaciones transmiten sus mensajes a los ciudadanos y la forma en que estos responden.

Comunicarse, compartir información, mantener un contacto por interés o afinidad, relacionarse, formar una identidad y reputación, reivindicarse, protestar, manipular, … son múltiples los objetivos buscados a la hora de utilizar una u otra red social.

[20] WhatCrypt: http://whatcrypt.com/

No obstante, el éxito alcanzado, las enormes posibilidades que brindan y su uso masivo, las han hecho situarse en el punto de mira de los ciberatacantes que no dudan en explotar los riesgos y vulnerabilidades que tienen tanto las plataformas que sustentan estas redes sociales como las personas u organizaciones que las utilizan.

Una vez más, el eslabón más débil de esta cadena vuelve a ser el factor humano por su escasa concienciación y su exceso de confianza a la hora de emplear estas redes.

En general, los riesgos asociados a las redes sociales son los mismos que los del resto de actividades y/o servicios en Internet: grandes dificultades para eliminar la información subida, el acceso futuro por terceros (el derecho a cambiar de opinión es nulo y será muy difícil borrar cualquier opinión, fotografía o vídeo subido a la red) y la dificultad de discernir entre información veraz y propaganda o manipulación.

En este punto hay que recordar la importancia que tiene la configuración de seguridad del dispositivo (sistema operativo y navegador) utilizado para conectarse a Internet y, de esta manera, acceder a las redes sociales.

A continuación, se indican los **principales consejos** que se pueden dar como buenas prácticas en el uso de redes sociales:

- Creación cuidadosa del perfil y la configuración de privacidad. No basarse en la configuración por defecto que proporcionan las plataformas.
- Reflexión sobre todo lo que se publica y emplear un pseudónimo. Dar por sentado que todo lo que se sube en una red social es permanente, aunque se elimine la cuenta.
- Escoger cuidadosamente a nuestros amigos.
- Para evitar revelar las direcciones de correo de sus amigos, no permita que los servicios de redes sociales examinen su libreta de direcciones de correo.
- Prestar atención a los servicios basados en la localización y la información del teléfono móvil.
- Precaución con los enlaces. Evitar hacer clic en hipervínculos o enlaces de procedencia dudosa.
- Escribir directamente la dirección de su sitio de redes sociales en el navegador para evitar que un sitio falso pueda robar su información personal.
- Tener precaución al instalar elementos adicionales en su sitio ya que, en ocasiones, se usan estas aplicaciones para robar información personal.
- Revisar la información publicada. Eludir dar excesiva información sobre uno mismo entre otras cosas para evitar que puedan entrar en su cuenta al responder a preguntas del tipo su cumpleaños, su ciudad natal, clase del instituto, etc.
- Seguridad de las contraseñas, utilice contraseñas complejas que incluyan números, símbolos y signos de puntuación. Es importante no compartir la misma contraseña para todas las redes sociales ni para el resto de servicios que se utilizan en Internet (empleo de gestores de contraseñas tipo *keepass*).
- Incrementar la seguridad en el acceso a la cuenta añadiendo un segundo factor de autenticación (*2FA*) que impida a un potencial atacante que se haya hecho con la contraseña acceder al servicio,

13. INTERNET DE LAS COSAS (IOT)

En esencia, IoT[21] (*Internet of Things*) se refiere a redes de objetos físicos, artefactos, vehículos, edificios, electrodomésticos, atuendos, implantes, etc. que llevan en su seno componentes electrónicos, software, sensores con conectividad en red que les permite recolectar información para lograr una contextualización de la situación mediante técnicas de Big Data imposible de realizar por otros medios.

Se trata de una red que interconecta miles de objetos físicos ofreciendo datos en tiempo real, convirtiéndose en los sensores del mundo físico. En este punto hay que considerar el cambio cultural que suponen ya que la tecnología influye en nuestra forma de tomar las decisiones y ello afecta a la capacidad de acción, privacidad y autonomía de las personas.

La IoT es la primera evolución real de Internet, un salto que podría llevar a aplicaciones revolucionarias con capacidad para modificar de forma dramática la forma en la que vivimos, aprendemos, trabajamos y nos entretenemos o relacionamos socialmente.

Los artículos de uso diario han dejado de ser elementos aislados, dispositivos que a su vez pueden estar conectados a otros dispositivos. La pesadilla de los expertos en ciberseguridad puede convertirse en ejércitos de "*botnets*" utilizando las tostadoras inteligentes para desarrollar ataques *DDoS* o para esconder información y ejecutables lejos de la vista de los investigadores.

En la IoT hay que considerar aspectos de vital importancia como la seguridad, la interoperabilidad y manejabilidad de dichos sistemas:

- Interfaz Web.
- Mecanismos de autenticación.
- Servicios de red.
- Transporte no cifrado.
- Protección de la intimidad.
- Configuración de seguridad.
- Integridad software/firmware.
- Seguridad física de los dispositivos.

El reto se reduce a establecer una base de monitorización y control para reducir la exposición al riesgo y aplicar técnicas inteligentes a la creciente población de dispositivos IoT.

- Cambiar las contraseñas por defecto de los dispositivos y utilizar contraseñas realmente robustas.
- Mantener actualizados los dispositivos con las últimas versiones disponibles de software y firmware.
- Desactivar toda conectividad remota (con Internet) de los dispositivos cuando no sea estrictamente necesaria.

[21] Véase **Informe de Buenas Prácticas CCN-CERT BP-05/16 Internet de las Cosas** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-16-internet-de-las-cosas/file.html)

- Mantener abiertos solo aquellos puertos de comunicación que sean realmente necesarios y modificar los puertos de escucha si es posible.
- Si los dispositivos IoT no permiten la configuración de su seguridad, operar con ellos siempre en una red de área local (LAN) detrás de un dispositivo (enrutador) correctamente configurado que sí provea esa seguridad.
- En la medida de lo posible, asegurar la autenticidad, confidencialidad e integridad en todas las comunicaciones locales (LAN), especialmente si estas se realizan por enlaces radio (WiFi, Bluetooth, etc.).
- Comprobar periódicamente la configuración de seguridad de todos los elementos de la arquitectura IoT y su comunicación con el exterior.
- Mantener deshabilitados los componentes no necesarios como pueden ser, según el caso, micrófonos, cámaras de vídeo, etc...
- Comprobar la visibilidad de los dispositivos propios en buscadores de dispositivos IoT como Shodan.

14. POLÍTICA DE SEGURIDAD

El diseño de una estrategia de seguridad dentro de una organización depende en general de la actividad que esta desarrolle, su dimensión, el ámbito de actuación y la interconexión con usuarios externos (clientes, proveedores, usuarios finales, etc.). Sin embargo, en líneas generales se pueden considerar unos pasos básicos a la hora de desarrollar una estrategia:

- Crear una Política de seguridad.
- Realizar un análisis de riesgos.
- Aplicar las salvaguardas correspondientes.
- Concienciar a los usuarios.

La **Política de seguridad**[22] establece el estado en el que se encuentra la información y los servicios dentro de la entidad y define qué es lo que se desea proteger, así como los correspondientes objetivos de seguridad proporcionando una base para la planificación de la misma.

Describe responsabilidades del usuario y cómo se supervisa la efectividad de las medidas aplicadas. En definitiva, es un conjunto de reglas que se deciden aplicar en las actividades del sistema y a los recursos de comunicaciones que pertenecen a una organización.

Estas reglas incluyen áreas como la seguridad física, personal, administrativa y de la red. Además, debe señalar la importancia de las tecnologías de la información para la Organización, el período de validez de la política, los recursos con que se cuenta y los objetivos específicos a cubrir.

[22] Véase **CCN-STIC-805 Política de Seguridad de la Información** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html)

Con el **análisis de riesgos**[23] se consigue identificar los riesgos a los cuales está expuesta la organización y cuáles son los impactos, las posibles amenazas y las vulnerabilidades que pueden ser explotadas por éstas.

Una vez que se establece la política de seguridad, determinando el riesgo residual que se está dispuesto a aceptar, se deben establecer las **salvaguardas** que den cumplimiento a la misma.

La gestión de riesgos utiliza los resultados del análisis de riesgos para seleccionar e implantar las **medidas de seguridad** adecuadas para controlar los riesgos identificados y que se pueden dividir en las siguientes:

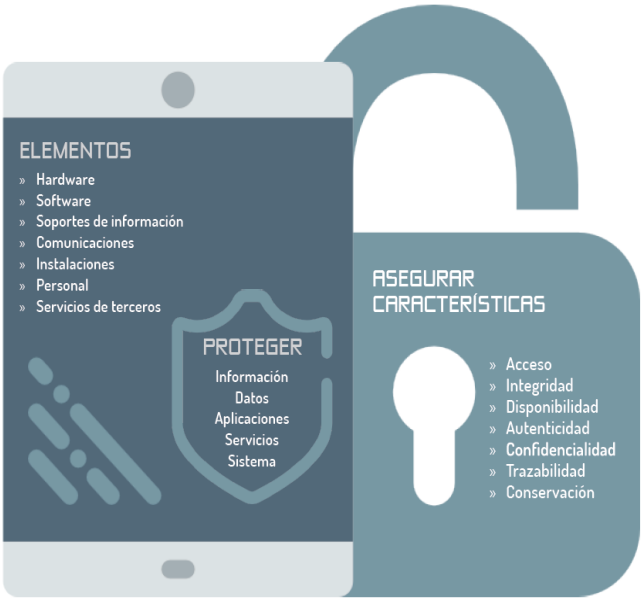


Figura 3.- Elementos a considerar en la Política de seguridad

- **Preventivas**: tienen como objeto reducir el riesgo
  - Protección Física: guardias, control de acceso, protección hardware…
  - Medidas Técnicas: cortafuegos, detectores de intrusos, criptografía…
  - Medidas Procedimentales: cursos de mentalización, actualización de conocimientos, normas de acceso a la información, sanciones…
- **Análisis**: orientadas a la identificación del riesgo
  - Protección Física: sistemas de vigilancia, detectores de movimiento…
  - Medidas Técnicas: control de acceso lógico, sesión de autenticación…
  - Medidas Procedimentales: gestión de logs, monitorización de auditoría.
- **Correctivas**: se orientan a impedir o reducir el impacto sobre los activos
  - Protección Física: respaldo de fuente de alimentación (SAI), …
  - Medidas Técnicas: programa antivirus, auditorías, respaldo de seguridad…
  - Medidas Procedimentales: planes de contingencia…

La amenaza más seria para un sistema de información son las personas, por consiguiente, la **formación y sensibilización** del personal es uno de los objetivos fundamentales que se persiguen con la implementación de un programa de cultura en ciberseguridad.

El programa de mentalización y sensibilización debe perseguir dejar claro no sólo cómo proteger los sistemas sino también porqué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos.

[23] El CCN-CERT pone a disposición del Sector público la herramienta de **Análisis de Riesgos PILAR** (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html)

Por último, incidir en que es muy importante definir, documentar y difundir una política de seguridad que demuestre el compromiso de la organización con la seguridad, así como el desarrollo de normativas que recojan las obligaciones a las que están sujetos los usuarios en lo que respecta al tratamiento y seguridad de la información.

14.1 GOBERNANZA

Los profesionales son la base del éxito de la operación de la seguridad. Por este motivo, en cualquier organización se deben considerar aspectos como gobernanza, estructura, experiencia, entrenamiento y certificaciones del personal.

Se deben establecer los mecanismos de **gerencia** y **gestión de la seguridad**, incluyendo soporte a las operaciones, niveles de escalamiento acordes con la clasificación y remediación de incidentes, frecuencia y tipos de notificación, etc. En este sentido, es recomendable implantar el denominado **SGSI** (**Sistema de Gestión de la Seguridad de la Información)** un conjunto de políticas de administración de la información, donde se definen, implantan y mantienen un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

De esta manera, la **estructura** debe permitir identificar las personas que tienen el nivel de autoridad y responsabilidad sobre las diferentes tareas.

Las **áreas de experiencia** necesaria son las que permitirán definir los roles y perfiles necesarios para la operación de los servicios siendo importante considerar planes de entrenamiento y certificaciones que den pie a la adaptación a los cambios, la incorporación de nuevas tecnologías y el crecimiento de los servicios.

Se debe considerar el establecimiento de una oficina de seguridad que asista en la implantación de las políticas, procedimientos y normativa que sienten las bases para dirigir, gestionar, comunicar, evaluar, controlar y mejorar la seguridad de la información relacionada con las actividades propias de la entidad conforme a la normativa y buenas prácticas aplicables.

- Revisar y apoyar la implantación del modelo de gobernanza.
- Análisis y adecuación normativa.
- Análisis y gestión de los riesgos asociados a los activos. (Riesgo residual asumible)
- Análisis y definición de cuadros de mando. (Medidas e indicadores)
- Auditorías de cumplimiento normativo.
- Soporte a los órganos de gobierno de la seguridad.
- Seguimiento y mejora del estado y gestión de la seguridad.

14.2 GESTIÓN DE LA CONFIGURACIÓN

La implementación efectiva de control de **configuración y gestión de software** es fundamental ya que es la única manera de asegurar que los sistemas operativos y aplicaciones son actualizados de forma correcta tras la publicación de los parches preceptivos.

Hay que considerar lo siguiente:

- Todos los archivos ejecutables y plantillas de documentos "*templates*" compartidos deben estar colocados en un directorio de sólo lectura.
- Cada usuario debe tener su propio directorio personal en la red con acceso lectura/escritura y restringido para lectura para otros usuarios para prevenir previsibles diseminaciones de software malicioso de la máquina local a la red.
- Los directorios compartidos por varios usuarios es un modo habitual de trabajo por lo que hay que prevenir la diseminación de posibles infecciones.

Las **contraseñas** son el principal mecanismo de autenticación utilizado por las personas en su acceso a los sistemas de información. La seguridad que proporcionan las contraseñas depende, en gran medida, de su confidencialidad.

- No podrá ser asociada con facilidad a cualquier información relacionada con el usuario de la cuenta.
- Tendrá una longitud mínima de ocho (8) caracteres con diferentes tipos de caracteres tipográficos.
- Cambiar la contraseña periódicamente.
- No compartir las cuentas y contraseñas con otros usuarios.
- No anotar las contraseñas en sitios de fácil acceso, ni almacenarlas en ficheros en el ordenador sin ninguna protección.
- Limitar la posibilidad de "*Recordar Contraseña*" que ofrecen algunos navegadores web.

Existen programas que permiten almacenar todas las contraseñas con nombre de usuario asociado en un único lugar, de forma que siempre estén disponibles y no haga falta recordar todas ellas. Habitualmente, estos programas disponen también de un generador de contraseñas, de forma que se puedan generar de manera segura.

Los **soportes extraíbles** constituyen una de las principales amenazas de fuga de información, así como de infección por malware. Limitar la utilización de dispositivos USB, quizá sea una medida demasiado drástica. No obstante, se debe evaluar la posibilidad de bloquear estos puertos y eliminar las unidades lectoras/grabadoras de soportes ópticos de los equipos de usuarios.

14.3 VIGILANCIA

Junto con el control de configuración y gestión del software se debe valorar un proceso continuo de análisis de vulnerabilidades ya sea automático como manual.

- **Análisis de vulnerabilidades automáticas**: despliegue de herramientas para la realización de escaneos de vulnerabilidades a infraestructuras y servicios.
- **Análisis de vulnerabilidades manuales**: realización por parte de un grupo de analista de una revisión periódica de las diferentes aplicaciones, principalmente de las expuestas a Internet, desde las perspectivas de caja negra y caja blanca.

No hay que perder de vista que mediante la constitución de un **Centro de Operaciones de Seguridad (SOC)** se mejoran las capacidades de vigilancia y detección de incidentes y se optimiza la capacidad de reacción y respuesta ante cualquier ataque.

Hay que considerar desplegar un bloque de servicios basados en:

- **Monitorización de seguridad**

  Despliegue de sondas de alta capacidad que reciban una copia del tráfico, tanto entrante como saliente en Internet. Tratamiento de los eventos generados por un sistema de información de seguridad y administración de eventos (SIEM).

  Asimismo, se deben considerar módulos de aprendizaje automático (Machine Learning) para análisis de eventos y alertas y poder detectar nuevas amenazas.

- **Protección y filtrado de contenido malicioso**

  Proteger a los usuarios que navegan en Internet ante este tipo de amenazas. Dispositivos de nueva generación, los cuales cuentan, además de las capacidades tradicionales de los cortafuegos, con prevención de intrusiones y control de aplicaciones.

- **Respuesta a Incidentes**

  Servicio avanzado de soporte a la gestión de incidentes mediante profesionales que se podrán coordinar, de forma remota o in situ, con el personal de la entidad con el objeto de realizar análisis forenses, colaborar en la estrategia de mitigación y/o recuperación, etc.

- **Análisis de Vulnerabilidades**

  Análisis periódico de vulnerabilidades tanto de forma automatizada como manual. Para ello se aportarán tecnologías de escaneo de sistemas y de aplicaciones web que facilitarán la realización de estas pruebas de forma periódica tanto automatizada como pruebas manuales.

14.4 CONTINUIDAD DE NEGOCIO/POLÍTICAS DE RESPALDO

El término "*Continuidad de Negocio*" supone pensar y disponer de un plan alternativo en caso de que ocurra un desastre en los sistemas TIC de la entidad. Este plan debe estar documentado para que llegado el caso se tengan claro los pasos a seguir para mitigar el problema y volver a la situación previa de normalidad con la mayor brevedad posible.

Asimismo, en la medida de lo posible, se deberían realizar **pruebas de los planes** de continuidad para confirmar que se encuentran debidamente actualizados y responden de manera eficaz a la a necesidad.

Es fundamental realizar **copias de respaldo** de manera regular para asegurar la integridad/disponibilidad del sistema. La realización de copias de seguridad implica crear una copia de los datos en un medio diferente del que se encuentran con el fin de que las mismas puedan utilizarse para restaurar la copia original después de una eventual pérdida de datos.

La pérdida de datos puede deberse a robos, fallos en el sistema, catástrofes naturales o simplemente a errores en el hardware del sistema. Existen muchos tipos diferentes de dispositivos empleados para el almacenamiento de datos para realizar "*backups*" con ventajas y desventajas que hay que tener en cuenta en su elección.

Por último, es muy recomendable verificar las copias de seguridad con relativa frecuencia mediante la restauración real de los datos en una ubicación de prueba.

14.5 GESTIÓN DE INCIDENTES

La gestión de incidentes[24] forma parte de la cultura de gestión de riesgos. Cuando se produce un incidente[25] de seguridad es crítico para una entidad disponer de un protocolo eficaz de respuesta que ayude a los equipos de seguridad a minimizar la pérdida o filtración de información, evitar la propagación del incidente o, incluso, la propia interrupción del servicio. La velocidad con la cual se reconozca, analice y responda al incidente limitará el daño y minimizará el coste de la recuperación.

Las entidades tienen que habituarse a notificar y compartir incidentes con las organizaciones correspondientes, máxime teniendo en cuenta que, en numerosas ocasiones, los patrones de actuación se repiten. Es esencial establecer buenas prácticas sobre notificación, utilización de una taxonomía común y procedimientos para la notificación de los mismos, incluyendo aquellos de los que se desconoce el impacto.

A este respecto, las autoridades competentes y los CERT/CSIRT[26] de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

Las entidades afectadas deberán realizar una primera notificación sin dilación. Posteriormente, efectuarán aquellas que sean precisas para actualizar la información sobre la evolución del incidente mientras no esté resuelto. Una vez se resuelva (las redes y sistemas de han restablecido y el servicio opera con normalidad) deberán enviar una notificación final del incidente.

Los CSIRT monitorizan las redes para detectar de un modo temprano posibles incidentes[27], difundir alertas sobre ellos y aportar soluciones para mitigar sus efectos. Dichos Equipos deben ser la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a los mismos.

La gestión de incidentes de seguridad tendrá en cuenta:

- El establecimiento de sistemas de detección y reacción frente a código dañino.
- El registro de los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan.
- El soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad.

[24] Véase **Guía CCN-STIC-817 Gestión de Incidentes** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)

[25] Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

[26] Ambos términos son utilizados para denominar a un Equipo de Expertos en Gestión de Incidentes. ***CERT**: Computer Emergency Response Team* y ***CSIRT**: Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad*. La primera de las denominaciones está registrada por el CERT CC, el primer equipo de estas características de la Universidad estadounidense Carnegie Mellon.

[27] Ejemplo de ello es el Sistema de Alerta Temprana del CCN-CERT (SAT INET y SAT SARA)

- Proporcionar información sobre vulnerabilidades, alertas y avisos de nuevas amenazas. Incluye la investigación y divulgación de las mejores prácticas sobre seguridad de la información.
- La formación al objeto de mejorar las capacidades para la detección y gestión de incidentes.

Un esquema básico de actuación frente a un ciberincidente puede ser:

- La DETECCIÓN de la amenaza, puede ser realizada por la propia entidad y/o por las sondas desplegadas por el Equipo de Respuesta a Ciberincidentes (CSIRT) de referencia, que generarán el correspondiente aviso.
- En caso de confirmarse el ciberincidente, el organismo realizará la notificación formal (por ejemplo, herramienta LUCIA) a la autoridad competente, a través del CSIRT de referencia, y las acciones de la fase de CONTENCIÓN.
- Una vez ERRADICADA la amenaza, la entidad, usando la misma herramienta, notificará a la autoridad competente, a través del CSIRT de referencia, el cierre del ciberincidente.

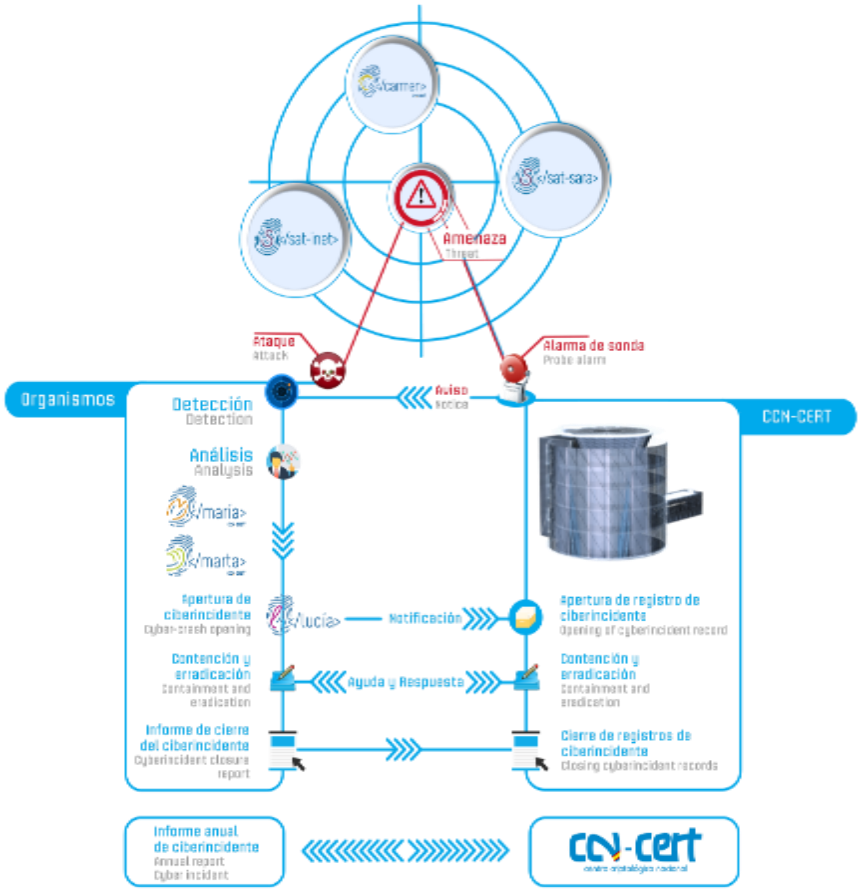


Figura 4.- Esquema Básico actuación ante Ciberincidente

La gestión de los ciberincidentes (asignación de prioridades y recursos, etc.) exige determinar la peligrosidad potencial que el ciberincidente posee. Para ello, es necesario fijar los criterios de determinación de la peligrosidad con los que comparar las evidencias que se disponen del ciberincidente en sus estadios iniciales.

15. DECÁLOGO BÁSICO DE SEGURIDAD

Este decálogo de buenas prácticas pretende sentar las bases para establecer una cultura de seguridad.

	Decálogo Básico de Seguridad
1	La cultura de la ciberseguridad, la concienciación del empleado, debe ser uno de los pilares en lo que se asiente la ciberseguridad de cualquier Organización.
2	No abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
3	Utilizar software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc. debe ser algo irrenunciable cuando se utiliza un sistema de las TIC.
4	Limitar la superficie de exposición a las amenazas, no solo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.
5	Cifrar la información sensible, no hay otra alternativa.
6	Utilizar contraseñas adaptadas a la funcionalidad siendo conscientes de que la doble autenticación ya es una necesidad.
7	Hacer un borrado seguro de la información una vez que esta ya no sea necesaria o se vaya a retirar de uso el soporte en cuestión.
8	Realizar copias de seguridad periódicas, no existe otra alternativa en caso de infección de código malicioso tipo *ransomware*, pérdida de datos, averías del hardware de almacenamiento, borrado de información involuntaria por parte del usuario, etc.
9	Mantener actualizadas las aplicaciones y el sistema operativo es la mejor manera de evitar dar facilidades a la potencial amenaza.
10	Revisa regularmente la configuración de seguridad aplicada, los permisos de las aplicaciones y las opciones de seguridad.

Figura 5.- Decálogo de seguridad