EUSKO JAURLARITZA
GOBIERNO VASCO

nº 55
Marzo de 2016

Aurrera!

Boletín divulgativo de Innovación y Nuevas Tecnologías

Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

El Archivo Electrónico de un expediente es considerado hoy en día una pieza clave para cualquier Administración. De hecho, son muchas las Leyes y Normas que contemplan y regulan ya su funcionamiento. Existe además un tema estrechamente relacionado con el Archivo Electrónico, y es la denominada «*Política de Gestión de Documentos Electrónicos*» (PGDE), que todo organismo o entidad pública tiene la obligación de elaborar.

Dada la importancia que tiene la PGDE para cualquier Administración, en el primer artículo de este boletín os explicamos cuáles son los trámites que el Gobierno Vasco ha llevado a cabo en este ámbito, la legislación a aplicar y su relación con la interoperabilidad.

En el segundo tema de este boletín os hablamos de una nueva amenaza que durante los últimos meses ha ido en auge: el llamado *ransomware*. Cada día son más los enemigos que acechan a nuestros ordenadores, y dado que la mejor defensa ante ellos es estar bien informados, a lo largo del artículo os detallamos cuál es su origen, cómo funciona, qué variantes tiene y, sobre todo, cuál es la mejor forma de evitar y restablecerse de un ataque de este tipo.

En el apartado Alboan queremos daros a conocer un caso de éxito que han conseguido nuestros compañeros y compañeras de Eustat: la consecución de la Certificación ISO9001 para su área de Sistemas de Información. Un logro que es consecuencia de un trabajo de varios años y que constituye un hito más dentro de la mejora continua de sus procesos.

Dentro del apartado Breves, os presentamos un nuevo tipo de tarjeta denominada eSIM, la cual vendrá integrada en un futuro próximo en los teléfonos móviles, tal y como se ha adelantado recientemente en el *Mobile World Congress* celebrado en Barcelona.

En el apartado Breves, también, os informamos que la Oficina Técnica de apoyo al Software Libre en el Gobierno Vasco, conocida como SALE, acaba de estrenar su nueva web.

La importancia del Archivo Electrónico

Son muchos los expedientes que diariamente tramita la Administración Pública vasca. Y también son muchos los documentos que acompañan a estos expedientes, los cuales normalmente suelen llegar a la ventanilla de nuestras administraciones en formato papel, aunque cada vez es más habitual recibirlos también en formato electrónico o digital.

En los últimos años, el Gobierno Vasco ha dedicado muchos recursos, tanto humanos como económicos, a implantar la tramitación electrónica de los expedientes[1].

Todos sabemos que los expedientes tienen un inicio y un final. Muchas personas, sin embargo, piensan que al cerrarse un expediente termina la gestión del mismo y de sus documentos anexos. Pues bien, la «vida real» de estos expedientes (y de los documentos asociados a ellos) va más allá, ya que, tanto los tramitados en papel como los electrónicos, deben ser **archivados.**

Hasta ahora, y debido principalmente a la tendencia que tenemos a resolver los problemas inmediatos, la gestión de documentos electrónicos únicamente se ha centrado en la **fase de tramitación**. Como consecuencia de ello, muchos sistemas de administración electrónica que se han ido desarrollando abarcaban sólo la tramitación del expediente, pero no contemplaban el archivado final del mismo. En estos casos, los responsables de esas áreas dejaban ese tema pendiente con la idea de abordarlo en el futuro.

Sin embargo, esto puede suponer un gran problema, ya que si no abordamos el ciclo de vida completo, puede ocurrir que perdamos una importante parte de patrimonio documental, que se añadirá al fondo irrecuperable de tramitaciones electrónicas que se han realizado en el pasado, antes de la adecuación al **Esquema Nacional de Interoperabilidad (ENI)**[2]. El ciclo de vida completo de un expediente termina con el **archivo electrónico**, es decir, con la conservación del documento, proceso que debe cumplir una serie de requisitos para garantizar la recuperación (lectura), integridad, autenticidad, disponibilidad y validez de los documentos.

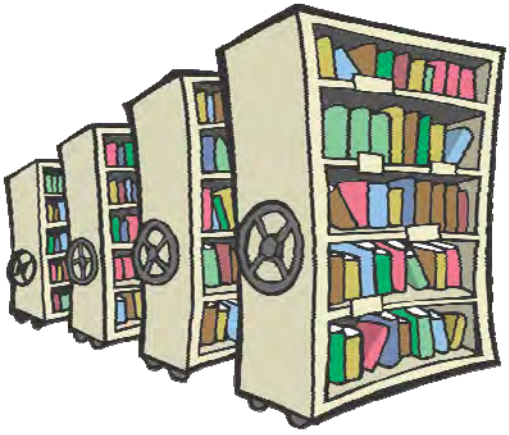
El ARCHIVO ELECTRÓNICO de un expediente es considerado hoy en día una pieza clave para la Administración Electrónica. Tanto es así que las normativas y leyes que han ido surgiendo en los últimos años dan cada vez más importancia a este aspecto.

EL ARCHIVO ELECTRÓNICO

La **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas en su artículo 17 indica lo siguiente:

«Artículo 17. Archivo de documentos.

1. ***Cada Administración deberá mantener un archivo electrónico único*** *de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.*



DICCIONARIO

[1] **Expediente electrónico:** es el conjunto de documentos electrónicos correspondientes a una instancia de un procedimiento administrativo.

Un **documento electrónico**, por su parte, es información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

[Fuente: Ley 11/2007, de 22 de junio, de Acceso electrónico de los ciudadanos a los Servicios Públicos]

[2] **ENI**: (Esquema Nacional de Interoperabilidad).

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. *Los documentos electrónicos deberán **conservarse en un formato que permita garantizar la autenticidad, integridad y conservación** del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.*
3. *Los medios o soportes en que se almacenen documentos, deberán contar con **medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad**, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos»*

El Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad, establece que un **Repositorio electrónico** es un archivo centralizado donde se almacenan y administran datos y documentos electrónicos, así como sus metadatos[3].

Según la legislación vigente, en 2017, todos los Organismos deberán disponer de un archivo electrónico único para los documentos electrónicos que se correspondan a procedimientos finalizados. En este sentido, el Gobierno Vasco dispone de su propio Sistema de Gestión Documental, denominado dokusi[4], que ya contempla el ciclo completo de los documentos, incluido su archivo.

La puesta en marcha de un **Archivo Electrónico único** requiere de un gran esfuerzo por parte de distintos colectivos (personas expertas en tecnología, administración, gestión, archivística, normativa, servicios jurídicos...).

Detallamos a continuación los aspectos más relevantes que, en opinión del Ministerio de Hacienda y Administraciones Públicas (incluidas en el documento «*El archivo electrónico es la última etapa del documento electrónico*» de julio de 2015, elaborado por el Observatorio de Administración Electrónica) hay que abordar para tener éxito en la gestión del «Documento Electrónico»:

- Se requiere la **colaboración multidisciplinar** de especialistas en archivo y en nuevas tecnologías, así como un tratamiento administrativo coordinado en el que se implique personal archivero, profesionales del ámbito de las Nuevas Tecnologías y gestores.

- Es necesario reconocer y ordenar el escenario de **herramientas preexistentes** de gestión documental y gestión de expedientes, e integrarlas con otras herramientas que puedan ya existir en la entidad.
- Es necesario **formar al personal** en gestión documental y fomentar la concienciación cultural de la importancia del patrimonio documental.
- Hay que arbitrar un tratamiento inteligente de los **expediente mixtos** (papel y electrónico).
- Se necesita contar con una **política de gestión de documentos electrónicos**, siendo este punto una de las piezas clave de todo el proceso.

El punto de partida, por tanto, debe ser la elaboración de dicha Política de Gestión de Documentos Electrónicos (PGDE).

LA POLÍTICA DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

La legislación vigente establece la **obligatoriedad que tiene** todo organismo o entidad pública de contar con una «*Política de gestión de documentos electrónicos*». A día de hoy, sin embargo, son pocos los **ejemplos** reales completamente desarrollados, ya que algunos incluso se pueden considerar como una primera aproximación de lo que será la Política completa. A modo de ejemplo, mencionar los siguientes: en el ámbito universitario (Murcia,

DICCIONARIO

[3] **Metadatos:** Son los datos que describen otros datos. Los **metadatos** sirven para identificar, autenticar y contextualizar documentos.
Los documentos y los expedientes electrónicos llevan unos metadatos mínimos obligatorios y pueden tener unos metadatos complementarios.

[4] **Dokusi:** (*Dokumentu Kudeatea Sistema Integrala*, Sistema Integral de Gestión Documental) es el proyecto de gestión documental corporativo con **archivo digital** del Gobierno Vasco.
Señalar que en el sistema de archivo de la Administración Pública de la CAE ya se conservan —organizados— expedientes y documentos electrónicos a los cuales se puede acceder a través del sistema informático de gestión de archivo AKS/SGA (aplicación S54b)

Más información en el artículo «*La nueva gestión documental con dokusi*» (boletín Aurrera de septiembre de 2008).

Navarra, País Vasco[5]), administración local (Cartagena, Diputación de Barcelona, Arganda del Rey, Diputación de Valencia), administración autonómica (Cataluña, Islas Canarias) y Administración General del Estado (Ministerio de Hacienda y Administraciones Públicas, Ministerio de Educación, Cultura y Deporte).

De todas formas, la elaboración de una política de gestión de documentos electrónicos no es sólo un requisito legal que hay que cumplir. Básicamente podemos considerarla como una herramienta imprescindible para desarrollar adecuadamente la gestión de documentos electrónicos dentro de una organización, siempre de acuerdo con lo establecido por el ENI.

Pero, ¿qué es exactamente la Política de Gestión de documentos electrónicos? De forma resumida, diremos que es el **conjunto de las directrices** de una organización que nos van a permitir crear y gestionar documentos auténticos, fiables y disponibles a lo largo del tiempo.

En este documento se establecen, por tanto, las **especificaciones técnicas** y los criterios y recomendaciones necesarios para garantizar la interoperabilidad, la recuperación y la conservación de los documentos y expedientes electrónicos que se pueden generar en la Administración.

Esta Política debe ser aprobada al más alto nivel dentro de la organización, y asigna / distribuye **responsabilidades** en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de todo su ciclo de vida.

La Política de Gestión de documentos electrónicos debe garantizar, además, el cumplimiento de lo establecido en el **Esquema Nacional de Interoperabilidad (ENI)**, siguiendo lo dispuesto en la Norma Técnica de Interoperabilidad de obligado cumplimiento y en su correspondiente Guía de Aplicación.

Para ello, se establece que deberán conservarse en soporte electrónico todos los documentos electrónicos utilizados en actuaciones administrativas que formen parte de un expediente administrativo y aquellos que tengan valor probatorio de las relaciones entre la ciudadanía y la Administración, en el formato original o en cualquier otro que asegure su integridad.

«El Archivo electrónico es una pieza clave para la Administración Electrónica»

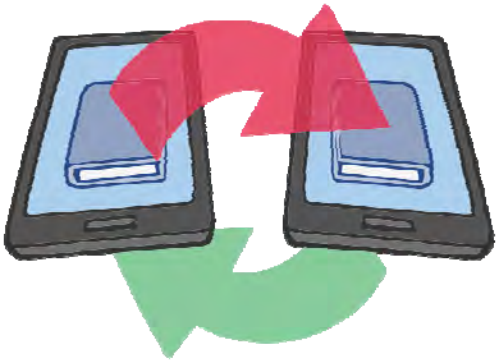
Desde el año 2013 el comité técnico de **dokusi** ha elaborado su propuesta de PGDE pendiente de aprobación por parte del Gobierno Vasco con la que se pretende normalizar y mejorar la gestión, tramitación, organización y archivo de la documentación generada por la Administración Pública de la CAE, respetando lo dispuesto en la Norma Técnica de Interoperabilidad de gestión de documentos electrónicos.

LA INTEROPERABILIDAD

En base al marco legal actual, cada Administración deberá facilitar, además, el **acceso** de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, haciendo uso para ello de la **interoperabilidad**.

De hecho, esta necesidad ya se recogía en la Agenda Digital para Europa, dentro de las iniciativas emblemáticas de la Estrategia Europa 2020. Es tal su importancia que, en opinión de muchos expertos, «*sin interoperabilidad no hay Administración Electrónica*», y podríamos añadir a su vez que ésta no existiría sin los Documentos y Archivos Electrónicos.

Tanto es así que el **ENI** establece una serie de Normas Técnicas de Interoperabilidad que son de



DICCIONARIO

[5] **País Vasco**: La Universidad del País Vasco-Euskal Herriko Unibertsitatea (UPV-EHU) publicó en abril de 2014 un documento que establecía su «*Política de Gestión Documental y Archivo*», el cual se puede consultar en la siguiente web:

https://www.ehu.eus/es/web/idazkaritza-nagusia/dokumentuak-gestionatu-eta-artxibatzeko-politika

Por otro lado, y como información adicional, indicar que el Gobierno Vasco, por su parte, publicó en 2003 el Decreto 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi.

[BOPV nº 163, de 22 de agosto de 2003]

obligado cumplimiento para las Administraciones Públicas y que desarrollan aspectos concretos de

«La gestión del Documento Electrónico requiere de la colaboración multidisciplinar de especialistas en gestión, archivística y nuevas tecnologías»

la interoperabilidad entre las Administraciones y con la ciudadanía. Estas son las normas:

1. Catálogo de estándares
2. Documento electrónico
3. Digitalización de documentos
4. Expediente electrónico
5. Política de firma electrónica y de certificados de la Administración
6. Protocolos de intermediación de datos
7. Relación de modelos de datos
8. Política de gestión de documentos electrónicos
9. Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas
10. Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos
11. Modelo de Datos para el intercambio de asientos entre las Entidades Registrales
12. Reutilización de recursos de información
13. Reutilización y transferencia de tecnología
14. Declaración de conformidad con el Esquema Nacional de Interoperabilidad
15. URL's de esquemas XML

Como se puede comprobar, muchas de ellas están estrechamente relacionadas con los Documentos, Expedientes y Archivo Electrónico. Elementos todos ellos, por tanto, básicos para la eAdministración. ❑

Legislación

A continuación se recoge una recopilación de la normativa que afecta al funcionamiento de los archivos electrónicos.

- ✓ **Real Decreto 1164/2002**, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.
- ✓ **Ley 11/2007**, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. [Artículo 31, Archivo electrónico de documentos]
- ✓ **Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. [Capítulo X, Artículo 21]
- ✓ **Real Decreto 1708/2011**, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso. [Sección 4.ª Documentos electrónicos y preservación digital]
- ✓ **Decreto 21/2012**, de 21 de febrero, de Administración Electrónica. [BOPV nº 50, 9 de marzo de 2012]
- ✓ **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. [Artículo 17. Archivo de documentos]
- ✓ **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público. [Artículo 46. Archivo electrónico de documentos]

COVASAD

En el ámbito de la administración vasca indicar que existe la denominada Comisión de Valoración, Selección y Acceso a la Documentación de la Administración Pública de la Comunidad Autónoma de Euskadi, también conocida por sus siglas **COVASAD**.

Esta Comisión centra su labor, entre otras cuestiones, en el proceso de determinación de los **calendarios de conservación** de la documentación.

Más información en el DECRETO 174/2003, de 22 de julio, de organización y funcionamiento del Sistema de Archivo de la Administración Pública de la Comunidad Autónoma de Euskadi. (El artículo 13 y siguientes desarrollan las funciones, composición y demás aspectos relativos a su funcionamiento)

Ransomware: amenaza en auge

Esta clase de *malware*[6] se está convirtiendo en una de las mayores amenazas existentes en Internet hoy en día; se conoce popularmente como «secuestro de ordenador», y con esta acción los cibercriminales tienen como único objetivo conseguir dinero —ilícitamente, por supuesto— a través del pago, por parte de la persona atacada, de un rescate (*ransom*) económico.

DICCIONARIO

[6] **Malware**: software malicioso, cuyo objetivo es dañar o infiltrarse en un sistema de información.

[7] **Scareware:** inducir miedo a la persona usuaria.

¿Qué es un *RANSOMWARE*?

«*Es un programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate*» (fuente: Wikipedia). Este tipo de malware se ha extendido debido a las cantidades de dinero que reporta a los atacantes. A diferencia de otro tipo de *malware*, cuyo objetivo es obtener información, el objetivo del *ransomware* es obtener dinero de una manera rápida.

¿Qué hacer en caso de ser atacados con este tipo de *malware*?

Como norma general, **NUNCA se debe pagar** a los cibercriminales por este tipo de acciones delictivas, ya que, por un lado, nunca se tiene la seguridad de que la restricción que se ha impuesto (en algunos casos el cifrado de los archivos del disco duro de la persona atacada) se vaya a solucionar, y, por otro lado, si se paga, se conseguiría reforzar este tipo de ataques.

Por desgracia, esta amenaza creciente se ha extendido desde Europa Oriental hacia Europa Occidental, Estados Unidos y Canadá; es decir, los criminales suelen ir allá donde hay dinero. Este es un *malware* altamente rentable para los criminales y organizaciones delictivas, ya que casi un 3% de las personas atacadas realiza el pago solicitado.

VARIANTES EN EL TIEMPO

Vamos a explicar, de una forma resumida, como ha variado en el tiempo esta forma de ataque:

Variantes iniciales: SMS Ransomware

Se bloquea el ordenador de la persona usuaria y se muestra una nota la cual indica que se envíe un mensaje SMS (*Short Message Service*, servicios de mensajes cortos o mensajes de texto disponibles en dispositivos móviles) a un número concreto, y, si se realiza esta acción, se recibe un código de desbloqueo, y se consigue liberar el ordenador. El pago consiste en el coste del envío de ese mensaje SMS de tarifa elevada (envío de SMS a números Premium). Las personas autoras de este tipo de *malware* se percataron pronto de que las compañías anti-virus rápidamente ofrecieron soluciones para combatir este problema sin tener que realizar el envío del mensaje Premium, por lo cual pasaron a evolucionar este tipo de ataques a través de servicios de pago electrónico (pago *on-line*).

Primer estadio de evolución: Winlockers

Al igual que SMS Ransomware, se bloquea el ordenador de la persona atacada, pero, en vez de solicitar el pago directamente, utiliza técnicas de ingeniería social, esto es, se engaña a la persona atacada (*scareware*[7]) explicándole que su equipo a infringido alguna Ley, por ejemplo, la Ley de propiedad intelectual, y que a causa de esa infracción debe de pagar una multa utilizando un sistema de pago *on-line.* La cantidad a pagar es mucho mayor que el coste de un SMS Premium, y en muchos casos se requería el envío de un código

de 19 dígitos previamente recibido como el reconocimiento de un pago. Esta variante del ransomware se pudo ver por primera vez en Rusia y en los países en los cuales se habla el idioma ruso, en el año 2009.

El *ransomware* únicamente bloquea la pantalla de la persona usuaria mediante un *banner*[8] a pantalla completa que imposibilita la ejecución de otros programas, y a través del cual se puede visualizar el mensaje de extorsión. Ejemplos de este tipo de malware son los conocidos como «virus de la policía» y «virus del FBI», que tuvieron mucha repercusión hace varios años.

Evolucion avanzada: encriptador de ficheros (*file encryptors*)

En esta variante el *malware* encripta los ficheros de la persona usuaria utilizando algoritmos complejos de encriptación. A esta persona usuaria se le solicita una cantidad de dinero por el «rescate» de su ordenador, lo que supuestamente le permitirá recuperar (mediante una clave de desencriptación) los ficheros encriptados. El pago se debe de realizar a través de medios de pago electrónico, tal y como ocurre en el caso del *ransomware Winlockers*. En estos casos la complejidad con la cual se realizan las operaciones de cifrado varía según el tipo de *ransomware*: unos utilizan herramientas de cifrado incluidas en el propio código, mientras que otros utilizan herramientas de cifrado de terceras partes, como, por ejemplo, GPG, WinRAR...

MECANISMOS DE ENTREGA Y PROPAGACIÓN

Principalmente, los mecanismos de entrega y propagación se basan en las siguientes formas de actuación:

- **Adjuntos a correos *spam***

El *ransomware* llega a través de mensajes de correo electrónico basura (*spam)* que incluyen ficheros adjuntos maliciosos; el correo electrónico puede tener un aspecto legítimo, y solicita a la persona usuaria que abra el fichero adjunto, que puede ser, por ejemplo, un fichero comprimido con extensión .zip; una vez que se abre este fichero adjunto comprimido el binario (fichero con información codificada en ceros y unos) dentro del .zip se ejecuta e instala el *malware* en el sistema, y pone en contacto al equipo con un *C&C server*[9], que es desde donde se baja la imagen de la pantalla de bloqueo (que muchas veces, basándose en sistemas de geo-localización, adapta su lenguaje al idioma del sitio donde se está actuando), y, también, hacia donde se suele enviar la clave de encriptación.

- ***Exploit*[10] *kits* o *exploit pack***

Son conjuntos de herramientas (denominados paquetes) que exploran y, si se da el caso, «explotan» los agujeros de seguridad hallados en el software

Informe de amenazas CCN-CERT IA-01/16

Medidas de seguridad contra *Ransomware*

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. El CCN-CERT tiene responsabilidades en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico; ha publicado el **Informe de Amenazas IA-01/16 - Medidas de seguridad contra *Ransomware***, en el que da a conocer determinadas pautas y recomendaciones de seguridad para ayudar a prevenir y gestionar los incidentes de este tipo, cada día más numerosos y agresivos.

De hecho, sólo en 2015, el Sistema de Alerta Temprana en Internet (SAT-INET) del CERT Nacional Gubernamental gestionó 500 incidentes relacionados con este tipo de ataques (frente a los 200 de 2014).

Acceso al informe:

https://www.ccn-cert.cni.es/informes

Web del CCN-CERT:

www.ccn-cert.cni.es

DICCIONARIO

[8] **Banner:** es un formato publicitario en Internet que se incluye en las páginas Web.

[9] **C&C server:** *Command and Control Server,* servidor de comando y control, , son máquinas centralizadas que son capaces de enviar comandos (instrucciones) y recibir salidas de los equipos que forman parte de una *botnet* (red de robots).

[10] **Exploit**: es un programa de software o código que aprovecha las vulnerabilidades que ofrecen las aplicaciones y sistemas instalados en sistemas de información; suelen ser de dos clases, los conocidos y los desconocidos (también llamados de día cero).

instalado (por ejemplo, en el software Java, software de Adobe —PDF—, los navegadores, los *plugins*[11] instalados...) en las máquinas atacadas en beneficio propio; este tipo de herramientas se pueden comprar por parte de las personas atacantes (cibercriminales) y pueden incluir el *malware* que desean entregar a la persona usuaria final. Se pueden instalar a través de descargas encubiertas, de vulnerabilidades Web, de macros en ficheros ofimáticos...; cuando una persona usuaria navega por un sitio Web comprometido (por ejemplo, contiene un *iFrame*[12] oculto que ha sido instalado por el ciberdelincuente aprovechando alguna vulnerabilidad de esa página Web), el *iFrame* oculto le redirecciona a un segundo sitio Web que tiene un *exploit*, que hará su trabajo en la máquina de la persona usuaria, una vez que esté descargado y se ejecute. Un ejemplo de modo de actuación es a través de los *banners*; normalmente estos anuncios son pagados por los cibercriminales (generalmente incluidos en páginas pornográficas), y a los cuales se les inyecta un código para que redirijan a la persona usuaria a una segunda Web, desde la cual se descarga y ejecuta en el ordenador de dicha persona un *exploit kit*.

Por ello, tal y como comentaremos más adelante, entre las medidas preventivas más importantes está el **mantener el sistema actualizado con los últimos parches de seguridad**.

- **Servicios de escritorio remoto (RDP, *Remote Desktop Protocol*)**

Estos servicios muchas veces no están lo suficientemente securizados en lo que respecta a las contraseñas de acceso, por lo que son vulnerables a ataques por diccionario (utilizar de forma automatizada una colección de palabras de acceso para poder acceder de manera ilegal).

- **A través de otro *malware***

Un sistema infectado por un software malicioso concreto se puede utilizar para descargar y ejecutar *ransomware*.

MEDIDAS PARA PREVENIR UN ATAQUE A TRAVÉS DEL RANSOMWARE

Las medidas preventivas son las citadas en el **Informe de Amenazas CCN-CERT IA-01/16** denominado «**Medidas de seguridad contra Ransomware**» (ver recuadro «*Informe de amenazas*»):

1. Mantener **copias de seguridad periódicas** (*backups*) de los datos considerados importantes: las copias se deben mantener **aisladas y sin conectividad** con otros sistemas (el *ransomware* puede afectar a todos los sistemas conectados al equipo afectado; por ejemplo, el *ransomware* conocido como **CryptoLocker** tiene la capacidad de recorrer y listar las unidades montadas en el equipo, sean USBs o sean unidades de red). También se recomienda utilizar VPN (*Virtual Private Network*) como método de acceso a servicios concretos, ya que muchas infecciones de *ransomware* se producen, como hemos comentado anteriormente, por el acceso a través de los servicios de escritorio remoto.

DICCIONARIO

[11] **Plugins**: conectores, extensiones, aplicaciones o programas que se relacionan con otra aplicación o programa para proporcionarle una funcionalidad determinada, generalmente muy específica.

[12] **iFrame**: marco incorporado, permite insertar un documento HTML (*HyperText Markup Language*, lenguaje de marcas de hipertexto, hace referencia al lenguaje de marcado para la elaboración de páginas web) dentro de otro documento HTML.

Herramientas EMET de Microsoft

EMET (*Enhanced Mitigation Experience Toolkit*) es un conjunto de herramientas que se utilizan para prevenir que se exploten vulnerabilidades de seguridad en el software.

EMET logra esto mediante el uso de tecnologías de mitigación de seguridad. Estas tecnologías funcionan como obstáculos y protecciones especiales que deben sortear la persona autora de un ataque para aprovechar las vulnerabilidades de software. Estas tecnologías de mitigación de seguridad no garantizan que no se puedan explotar las vulnerabilidades de seguridad. Sin embargo, su misión es **dificultar al máximo** dicha explotación.

EMET también ofrece una característica configurable de fijación de certificados SSL/TLS denominada *Certificate Trust* (Certificados de confianza). Esta característica está diseñada para detectar (y detener, con EMET 5.0) ataques de intermediarios que aprovechan la infraestructura de clave pública (PKI).

EMET requiere Microsoft .NET Framework 4.0.

https://support.microsoft.com/es-es/kb/2458544

2. Mantener el **sistema actualizado** (sistema operativo más programas instalados) con los últimos parches de seguridad: algunas de las principales vías de infección suelen ser versiones no actualizadas de la máquina virtual JAVA, de Flash o de Adobe (los *exploit kits*, como hemos dicho antes, explotan los agujeros de seguridad del software instalado).
3. Mantener **programas antivirus actualizados** (con las últimas firmas de código dañino) y configurar correctamente el cortafuegos a nivel de aplicación (basado en aplicaciones de lista blanca —*white listing*—, que protegen el sistema operativo de programas no autorizados y dañinos).
4. Que **el servicio de correo electrónico disponga de sistemas anti *spam*** (anti correo basura), dado que una de las vías de infección más comunes son los adjuntos asociados al correo basura.
5. **Establecer políticas de seguridad** de tal modo que sea imposible ejecutar ficheros desde directorios utilizados por el *ransomware*, como pueden ser: App Data, Local App, etc. Existen herramientas que posibilitan establecer estas políticas, como, por ejemplo, CryptoLocker Prevention Kit y AppLocker.
6. **Evitar la comunicación entre el código dañino y C&C Server** (del servidor de comando y control ya hemos explicado su función dentro de los mecanismos de entrega y propagación), a través del bloqueo de tráfico con dominios y servidores mediante la utilización de IDS/IPS[13].
7. Se recomienda **utilizar herramientas del tipo EMET** (ver recuadro «*Herramientas EMET de Microsoft*») o similares para proteger el navegador y las aplicaciones ofimáticas.
8. **No utilizar cuentas que tengan privilegios de administrador** si no es estrictamente necesario, para, de ese modo, reducir el impacto de una acción de *ransomware*, ya que desde una cuenta de administrador se puede llevar a cabo todo tipo de acciones dañinas.
9. **Mantener listas de control de acceso para unidades mapeadas en red**. De este modo evitaremos que, en caso de infección, se puedan cifrar las unidades de red (mediante la restricción de los privilegios de escritura en estas unidades).
10. **Emplear bloqueadores de Javascript[14] para el navegador**.
11. **Mostrar las extensiones para los tipos de fichero conocidos**. Esta medida es debido a que algunos *ransomware* utilizan ficheros dañinos con doble extensión para ocultar que son ficheros ejecutables dañinos (por ejemplo: .PDF.EXE, con lo cual la persona usuaria sólo ve un nombre de fichero que acaba en .PDF).
12. **Se recomienda la instalación de la herramienta «Anti Ransom»**[15], que puede mitigar el impacto producido por una infección del tipo *ransomware*; es una herramienta que se basa en el concepto de *honeypot* (*tarro de miel*), esto es, atrae y analiza los ataques que se producen utilizando un entorno controlado: se crea una carpeta de usuario, en la cual deja documentos no útiles susceptibles de ser cifrados por *ransomware* (que se conocen como *honeyfiles*), y se dedica a analizar posibles cambios dentro de los ficheros de esta carpeta; si estos cambios se producen, detecta el proceso que es culpable de estas modificaciones, vuelca la memoria del proceso para encontrar la clave de cifrado, y «mata» al proceso.
13. **Utilizar máquinas virtuales**. Ya que técnicamente, en un entorno virtualizado es más difícil que se materialice un ataque por *ransomware*.

QUÉ HACER ANTE UN ATAQUE

Muchos de los ataque de *ransomware* se basan en la ingeniería social (basada en el engaño), utilizando correos electrónicos, que tratan de que la persona usuaria que recibe ese correo electrónico abra una determinada página Web o ejecute un fichero concreto; por ello, la **concienciación** y **formación** que se realice con las personas usuarias finales es muy importante para prevenir este tipo de ataques.

Si se es consciente de que hemos sido atacados por *ransomware*, lo primero que hay que hacer es, en un entorno de red, desenchufar el cable de red o deshabilitar la red inalámbrica (Wi-Fi), e inmediatamente comunicar la incidencia al equipo de respuesta ante emergencias informáticas, a nuestro centro de atención al usuario (en el caso de una persona usuaria de la Red Corporativa del Gobierno Vasco se deberá llamar al Centro de Atención a Usuarios —CAU—), etc., ya que son quienes realizarán una valoración de los escenarios y soluciones posibles en función de la información aportada por la persona atacada. ❑

DICCIONARIO

[13] **IDS/IPS**: del inglés *Intrusion Detection System* (IDS) e *Intrusion Prevention System* (IPS), sistemas de detección y prevención de intrusiones. Una intrusión es una secuencia de acciones realizadas por un usuario o proceso deshonesto, con el objetivo final de provocar un acceso no autorizado sobre un equipo o sistema.

[14] **Javascript:** Es un lenguaje de programación interpretado (se ejecuta en el navegador web de la persona usuaria), orientado a objetos, se utiliza para crear páginas Web dinámicas, donde aparecen texto, animaciones... Permite crear funcionalidades específicas en las páginas Web.

[15] **Herramienta Anti Ransom:** herramienta basada en el concepto «tarro de miel» (*honeypot*), ver más información y acceso a la herramienta:

http://www.security-projects.com/?Anti_Ransom

ALBOAN:

Eustat obtiene la certificación ISO9001 para su área de Sistemas de Información

«La obtención del certificado no es un punto final para Eustat, sino que constituye un hito más dentro de la mejora continua de sus procesos»

A lo largo de este artículo os explicaremos cuál ha sido el camino recorrido por nuestros compañeros y compañeras de Eustat hasta conseguir la **certificación ISO9001** para su área de Sistemas de Información (en concreto para el Sistema de Gestión de la Calidad).

Sin duda alguna, un hito importante cuyo objetivo es la **mejora continua de los servicios** que ofrecen desde el área de Sistemas de Información al resto de Eustat, así como mejorar los procesos y sistemas de gestión internos ya implantados.

ANTECEDENTES

Instaurar el Sistema de Calidad (y su posterior Certificación) ha sido consecuencia de un trabajo de varios años, que se ha logrado mediante la consolidación de diferentes iniciativas comenzadas años atrás, relativas todas ellas a la sistematización y mejora continua de los procesos informáticos: impulso de «Besaide» (Metodología de gestión y desarrollo de sistemas de información basada en Métrica 3 y adaptada para Eustat), Proceso de Gestión de proyectos, y Catálogo de actividades gestionadas con indicadores.

Años antes de tomar la decisión de abordar este proyecto, Eustat ya poseía una cultura de trabajo basada en la **calidad y mejora continua**, habiéndose implantado hasta ese momento elementos como el Mapa de procesos y la Carta de Servicios, entre otros.

En 2009, tras un análisis sobre las metodologías y modelos de Calidad utilizados en organizaciones del sector TIC, se consideró que la certificación ISO ayudaría a impulsar todas las iniciativas en curso.

Así pues, en 2010 se comenzó a trabajar en medidas para sistematizar y alinear las iniciativas con objeto de abordar el proceso de certificación dentro del marco del «*Plan de Informática y Telecomunicaciones 2013-2016*» de Eustat.

En 2013, definitivamente, se toma la decisión de acometer el proyecto de certificación ISO9001, para el **área informática** de Eustat y sus procesos de trabajo asociados. Trabajo que se desarrolló en distintas fases entre los años 2014 y 2015.

En 2014, por ejemplo, se definió el alcance del proyecto, se asignaron las personas responsables del mismo y se impartió la formación correspondiente sobre el sistema de Calidad ISO9001.

Posteriormente, se realizó la definición del Sistema de Calidad en cada una de las áreas afectadas: Gestión de la Documentación, Gestión de proyectos (Desarrollo de aplicaciones), Gestión de Sistemas Informáticos (Comunicaciones, Seguridad), Contratación y Recursos Humanos.

En esa fase se revisó la coherencia de la Misión, Visión y Valores con el sistema de Calidad y se ajustó el Mapa del Proceso de Informática.

El sistema se implantó definitivamente a finales de 2014. Se realizaron tutorizaciones en la gestión de proyectos y en el cumplimiento de la normativa Besaide definida.

Y a primeros de 2015 se implanta completamente el sistema. Se continuó con la tutorización de proyectos y se realizó la primera auditoría del Sistema. Posteriormente, y una vez consolidados todos los procesos desarrollados, la auditoría se llevó a cabo el 19 de mayo de 2015, donde Eustat consiguió el **Certificado de Calidad**.

LOGROS CONSEGUIDOS

El proyecto de certificación ISO ha permitido al área informática de Eustat conseguir, entre otros

temas:

- ✓ Definir e implantar una metodología de Gestión de Proyectos y Planificación uniforme para todas las actividades y proyectos realizados.
- ✓ Planificar la actividad, controlando los posibles desvíos existentes entre la planificación inicial y la actividad realizada.
- ✓ Integrar las actividades de gestión de proyecto con las actividades técnicas y documentación establecidas por la metodología Besaide.
- ✓ Mejorar el análisis de necesidades de recursos y su previsión para gestión interna o de subcontrataciones.
- ✓ Implantar un cuadro de mando integral de indicadores alineado con la estrategia de la organización y los compromisos de la Carta de servicios de Eustat, y que enfoque a la organización hacia la mejora continua.
- ✓ Sistematizar los servicios a los clientes internos (producción estadística) mediante Acuerdos de Nivel de Servicio o ANS.
- ✓ Obtener conclusiones, determinar acciones de mejora y difundir lecciones aprendidas en el cierre de proyectos.
- ✓ Dotar a la organización de métodos y herramientas que permitan una más fácil formación e integración de nuevas personas que se incorporen a la misma.
- ✓ Certificación ISO9001 basada en gestión por procesos y la mejora continua y, por tanto, que esté alineada con el modelo de excelencia empresarial EFQM

FACTORES DE ÉXITO

Para conseguir la certificación han sido clave los siguientes factores:

- El liderazgo y la priorización de las actividades necesarias por parte de la Dirección
- La definición de una persona responsable del Sistema de Gestión de Calidad (RSGC) y de diferentes responsables para el resto de procesos, que han intervenido activamente en la definición e implantación del sistema.
- La definición de un Comité de Calidad compuesto por personas de responsabilidad, Subdirección, jefatura de área y responsable de calidad.
- Involucrar al personal del área Informática en la consolidación del Sistema de Calidad.
- Contraste de experiencias previas de implantaciones de sistemas similares en organizaciones externas del sector TIC y, más concretamente, de desarrollo de software.
- Formación previa a las personas participantes en la definición del Sistema: Comité de Calidad y coordinadores.
- Y en las diferentes áreas-procesos a trabajar:
  - Reunión para la recopilación de información con intervención del Responsable del Proceso y el RSGC donde se define el funcionamiento básico del proceso, los documentos involucrados y generar así los indicadores que permitan la gestión y ajuste del mismo.
  - Validación e implantación de procesos por personal de Eustat a todos los niveles: responsable de proceso, RSGC y confirmación con responsables superiores o colaboradores.
  - Tutorización del Sistema: reuniones con responsables de procesos para llevar a cabo el seguimiento.

PRÓXIMOS PASOS

El Sistema de Calidad implantado en Eustat es un sistema vivo y está inmerso en un proceso de mejora y mantenimiento. La obtención del certificado no es un punto final sino que **constituye un hito más dentro de la mejora continua de sus procesos**.

En la actualidad, de hecho, se está valorando avanzar en mejoras asociadas a metodologías de desarrollo ágiles, seguimiento continuo de proyectos, integración de metodologías y modelos específicos TIC (CMMi, ISO27000, ITIL, PMP...) y la automatización de la gestión de indicadores y registros de calidad, entre otros. ❑

«La norma ISO9001 tiene como objetivo fundamental la mejora continua de los servicios que ofrece el área de Sistemas de Información al resto de áreas de Eustat»

[+info]:

Web de Eustat

www.eustat.eus

Eustat

ALBOAN

¡¡BREVES!!

nº 55

Marzo de 2016

eSIM

Se estima que para el año 2020 el número de dispositivos móviles conectados en el mundo alcanzarán los 10.500 millones. Liberar a todos estos dispositivos de una tarjeta física como es la actual SIM (*Subscriber Identity Module*, módulo de identificación de abonado) supondrá una oportunidad, sobre todo para las comunicaciones entre máquinas remotas (M2M) y la electrónica de consumo.

La tarjeta SIM física será sustituida por lo que se conoce como eSIM, o SIM integrada (embebida o incrustada) o SIM electrónica o tarjeta SIM virtual o SIM GSMA *Embedded*; **se instalará de fábrica en el dispositivo como un elemento hardware más** (pequeño *chip* implantado en la placa). Para los teléfonos móviles va a simplificar y agilizar el cambio de operadora, aunque no comenzarán a instalarse en estos dispositivos hasta finales de 2017.

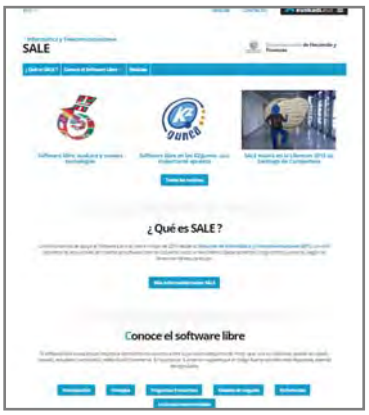
Operadoras y fabricantes se han puesto de acuerdo para lanzar un estándar común para crear una tarjeta virtual preinstalada en el hardware, que se podrá cargar con la información de cualquier compañía operadora (perfil de interoperabilidad), prescindiendo de la actual tarjeta SIM. En el *Mobile World Congress* (MWC) de 2016 la asociación mundial de operadores de telecomunicaciones (GSMA) presentó las especificaciones técnicas de la eSIM.

Las primeras experiencia o pruebas piloto se van a realizar con equipos máquina a máquina (M2M) instalados en coches o sistemas de seguridad, y en relojes inteligentes.

Una de las ventajas del nuevo tipo de SIM para dispositivos móviles inteligentes es que se van a poder **administrar varios SIM desde un único dispositivo** (dispositivos multiSIM). Asimismo, la eSIM facilitará el proceso para darse de alta en operadores extranjeros cuando salgamos fuera del país, lo que ayudará a mitigar los costes del «*roaming*».

Nueva web de SALE

SALE (*Software Askea/Libre en Euskadi*) es la marca que identifica a la Oficina Técnica de apoyo al Software Libre en el Gobierno Vasco. Se trata de una iniciativa puesta en marcha por el Gobierno en 2010, a través de la Dirección de Informática y Telecomunicaciones.



Esta iniciativa disponía de una página web cuyo entorno tecnológico estaba soportado en una arquitectura tipo LAMP (Linux, Apache, MySQL, PHP).

Este año, con objeto de actualizar su diseño y aprovechar la infraestructura del portal corporativo euskadi.eus, se ha llevado a cabo recientemente la migración de todos los contenidos (información, artículos/*post*, imágenes, enlaces...) de la antigua web al gestor de contenidos corporativos del Gobierno Vasco.

La nueva web, que ya se encuentra disponible, se caracteriza por ser *responsive design*, es decir, su contenido se adapta al dispositivo desde el cual estamos accediendo, bien sea un móvil, un ordenador o una *tablet*.

La nueva web consta de varios apartados:

- **Destacados**: en la parte superior de la web se destacan los 3 últimos artículos o noticias que ha elaborado y publicado SALE.
- **Descripción**: se incluye una breve reseña sobre qué es SALE, cuáles son sus objetivos, así como los enlaces de las redes sociales en las que SALE tiene perfil (*facebook*, *twitter*...)
- **Software Libre**: en este apartado se detalla la historia y características principales del Software Libre, su filosofía y las referencias más importantes, entre otros aspectos.

Web de SALE: http://www.euskadi.eus/sale