EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

60

junio 2017

Boletín divulgativo de Innovación y Nuevas Tecnologías
Publicado por el Gabinete Tecnológico
Dirección de Informática y Telecomunicaciones

ÍNDICE

La única forma que tiene una entidad para mejorar el servicio que ofrece a sus clientes es analizando sus procesos. Para ello, primero es necesario saber qué procedimientos tiene y cómo los tiene organizados. Con ese objetivo, el Gobierno Vasco está implantando en todos los Departamentos y Organismos Autónomos un Modelo de Gestión Pública avanzada, conocido como *Aurrerabide*.

Con esta metodología se pretende que las Direcciones y Servicios departamentales dispongan de una herramienta que les ayude a conocer cuál es su situación, y de esta forma puedan optimizar aquellos aspectos susceptibles de ser perfeccionados. Gracias a ello, se podrá ofrecer un mejor servicio a la ciudadanía. A lo largo del primer tema, por tanto, haremos una introducción de esta metodología.

Dentro del segundo tema, que lleva por título «*Formación desde el punto de vista del ENS*», os adelantaremos los contenidos de la formación que en el ámbito de la seguridad informática está preparando el Gobierno Vasco. Se trata de cursos que van dirigidos a todo el personal y nos permitirá reducir las consecuencias de un ataque informático, así como saber por qué es importante concienciar a todas las personas de los Departamentos y Organismos Autónomos, etc.

El apartado «Alboan» lo hemos dedicado en esta ocasión a los Estándares tecnológicos del Gobierno Vasco, pieza fundamental para definir las características técnicas de la infraestructura horizontal que soporta la Administración Electrónica vasca, los puestos de trabajo, etc.

Por último, y tras los recientes ataques habidos por el malware «*Wanna Cry*», y la gran repercusión que ha tenido tanto para las personas responsables de la ciberseguridad y para la ciudadanía en general, hemos querido dedicar el apartado «*Breves*» a dos temas directamente relacionados con la seguridad informática. En el primero de ellos os presentamos una nueva versión de la aplicación «*CONAN mobile*» y, en el segundo de ellos, os hablamos de un aspecto novedoso de la ciberseguridad y su relación con la mujer, una nueva perspectiva que recientemente ha sido analizada en el «*I Foro Internacional de Género y Ciberseguridad*», organizado por Incibe.

Iniciativa Aurrerabide

Toda organización debe estar constantemente evolucionando sus procesos para poder ofrecer cada día un mejor servicio a su clientela y seguir siendo competitiva frente al resto de empresas. En el caso de las Administraciones Públicas, ocurre exactamente lo mismo, ya que también ellas deben revisar sus procesos internos para mejorar el servicio que se ofrece a la sociedad a la que pertenecen.

En muchas ocasiones, a la hora de describir el funcionamiento de la Administración Pública, se habla de falta de eficacia y eficiencia, de poca flexibilidad y de lentitud para adaptarse a los cambios requeridos por la ciudadanía.

Ya en el Plan de Innovación Pública (PIP) del Gobierno Vasco, elaborado por la Dirección de Atención a la Ciudadanía, Innovación y Mejora de la Administración (DACIMA), se indicaba que «*La Administración Pública es una pieza clave en una sociedad avanzada. Una Administración Pública moderna, ágil y eficiente es determinante para lograr una sociedad con mayores cuotas de bienestar y de calidad de vida. Necesitamos, pues, una Administración Pública capaz de responder con eficacia a las demandas que nuestra sociedad, compleja, cambiante y diversa, le plantea en cada momento*».

Con objeto de mejorar los servicios públicos que se ofrecen a la sociedad vasca, en el PIP se incluyó un Eje cuyo fin era implantar un **Modelo de Gestión Avanzada** en el Gobierno Vasco y sus organismos autónomos, el cual recibió el nombre de «*Aurrerabide*».

Según la planificación inicial, estaba previsto que en un periodo de tres años (entre febrero de 2014 y enero de 2017) todas las Direcciones del Gobierno realizasen la formación-acción correspondiente.

En estos momentos, todos los Departamentos y Organismos Autónomos del Gobierno Vasco están participando.

A modo de referencia, indicar que en las tres convocatorias de 2014, 2015 y 2016 han participado un total de 110 Direcciones, Organismos Autónomos o Delegaciones. Directamente han participado en el proceso 685 directores/ as, delegados/as, las personas responsables de servicio y responsables de área, y más de 1.000 personas están implicadas de forma indirecta.

Esta iniciativa de la Viceconsejería de Función Pública (incluida en el PIP 2014-2016), es un proyecto estratégico para el Gobierno Vasco[1], que tiene su continuidad en el nuevo Plan Estratégico de Gobernanza e Innovación Pública 2020.

¿CÓMO FUNCIONA AURRERABIDE?

Cabe destacar que una de las principales características de Aurrerabide es que es un **modelo propio**, diseñado y desarrollado por personas del Gobierno, pensado para nuestra Administración, que se centra más en la mejora del proceso en sí, que en la parte formal del mismo.

Al igual que otras muchas Direcciones, la Dirección de Informática y Telecomunicaciones (DIT) ha participado en la iniciativa Aurrerabide. A lo largo de los próximos apartados, y por si puede ser de utilidad, contaremos la experiencia y tareas llevadas a cabo por la DIT dentro de esta iniciativa.

[1] **Proyecto estratégico**: El Gobierno Vasco ha publicado la siguiente normativa relacionada con Aurrerabide:

- Acuerdo de Consejo de Gobierno sobre el PIP 2014-2016 (17/junio/2014)
- Acuerdo de Consejo de Gobierno sobre Aurrerabide (14/octubre/2014)
- Acuerdo de Consejo de Gobierno sobre Evaluaciones, Planes de Consolidación y Mejora y Red de Colaboradores (7/junio/2016)
- Proyecto de Ley de Organización y Funcionamiento del Sector Público Vasco

El primer paso, tal y como ocurre en cualquier proceso de mejora continua del tipo PDCA[2], ha consistido en realizar una

autoevaluación para conocer cuál es nuestra situación respecto al Modelo de Gestión Avanzada que sirve de base: identificando los puntos fuertes, las debilidades, posibles oportunidades, así como las amenazas a las que tendremos que hacer frente. Asimismo, se ha ido elaborando, entre otros documentos, el Catálogo de Servicios de nuestra Dirección. Todo ello para concretar en compromisos específicos que deberán ser desarrollados posteriormente.

Una vez aprobado, el proyecto se ejecutaría por fases.

¿PARA QUÉ SIRVE?

Si se llevan a cabo los temas expuestos en las distintas sesiones que incluye la Metodología, ello nos permitirá transformarnos en una administración tal y como nos quiere la ciudadanía: más transparentes, cercanos, flexibles, corresponsables, participativos, innovadores, que trabajemos con objetivos que se evalúen, y que seamos más eficientes, esto es, que hagamos un mejor uso de los recursos públicos.

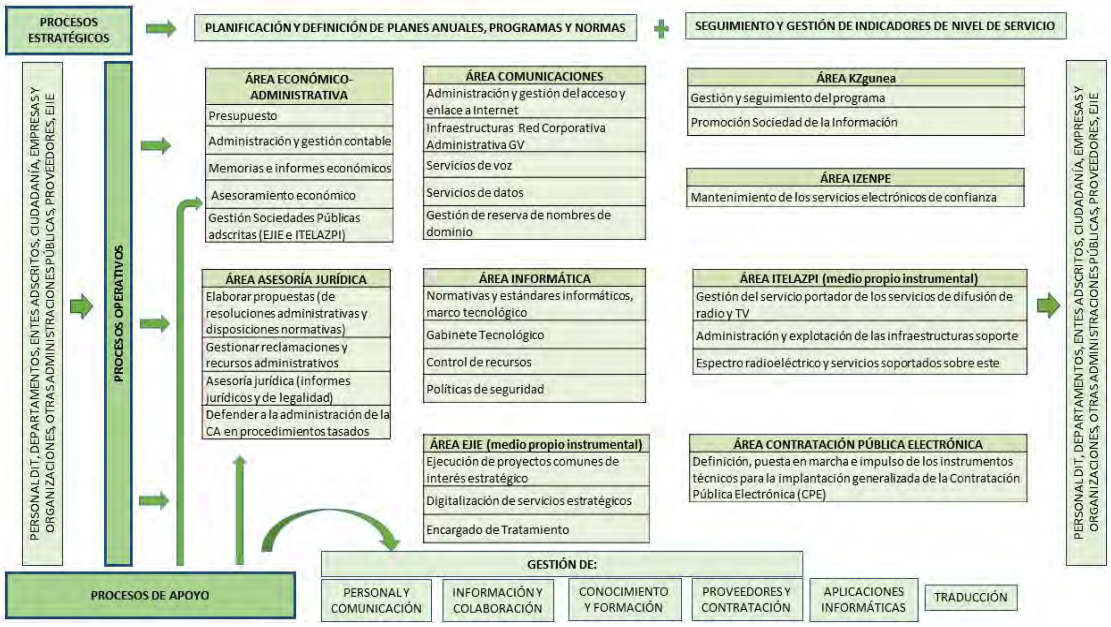
Para ello, el Modelo presta una atención especial a temas relacionados con:

1. **Estrategia**: planificación de objetivos, alineados con estrategia global del Gobierno.
2. **Servicios**: gestión de servicios para que respondan a lo que la ciudadanía demanda.
3. **Personas**: gestión de personas en condiciones que potencien su compromiso.
4. **Innovación**: creación de contexto para innovar y gestionar las ideas y proyectos innovadores.
5. **Sociedad**: promoción del buen gobierno y la ética pública, del trabajo colaborativo y asunción de la responsabilidad con la

[2] **PDCA:** el Ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés *Plan-Do-Check-Act*, es decir, Planificar-Hacer-Verificar-Actuar) o **espiral de mejora continua**, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.

[fuente: Wikipedia]

Mapa de Procesos de la Dirección de Informática y Telecomunicaciones (DIT)



sostenibilidad, la igualdad y la normalización del uso del euskera.

6. **Resultados**: seguimiento de resultados en relación con cada uno de los ejes.

«Aurrerabide pretende ser un modelo o programa para gestionar mejor los servicios que ofrece el Gobierno Vasco a la ciudadanía.»

[3] **Euskalit**: es la Fundación Vasca para el Fomento de la Calidad, que fue creada el 15 de diciembre de 1992.

Es una fundación, propiciada por el Gobierno Vasco, cuyo objetivo es promover la Gestión Avanzada en las organizaciones vascas y contribuir a mejorar su competitividad.

EUSKALIT

http://www.euskalit.net

EGITEN IKASI

Tal y como hemos comentado, Aurrerabide pretende ser lo más práctico posible. Para ello se basa en un proceso de formación-acción y acompañamiento continuo a la hora de implantar los elementos básicos del Modelo de Gestión en cada una de las Direcciones o Servicios participantes, y lo hace a través del proyecto conocido como «*Egiten Ikasi*» («*Aprender haciendo*», en castellano).

Este proceso se centra en ayudar a pensar y escribir en grupo sobre buenas formas de hacer que se puedan aplicar con el resto de compañeros y compañeras. Con ello, se impulsa el diseño colaborativo.

Tal es así que para trabajar en el diseño de «*Egiten Ikasi*» se constituyó en su momento un Grupo de Trabajo con la participación de representantes de la Dirección de Atención a la Ciudadanía e Innovación y Mejora de la Administración (DACIMA), del Instituto Vasco de Administración Pública (IVAP), y de la Dirección de Función Pública. EUSKALIT[3], por su parte, aportó su experiencia en la organización y desarrollo de los cursos *KnowInn* de formación-acción.

Posteriormente, se contrastó la estructura y el contenido en sesiones con Direcciones de Servicio, Responsables de Servicio y personal técnico, que hicieron aportaciones que sirvieron para mejorar la propuesta inicial.

AURRERABIDE

EGITENIKASI

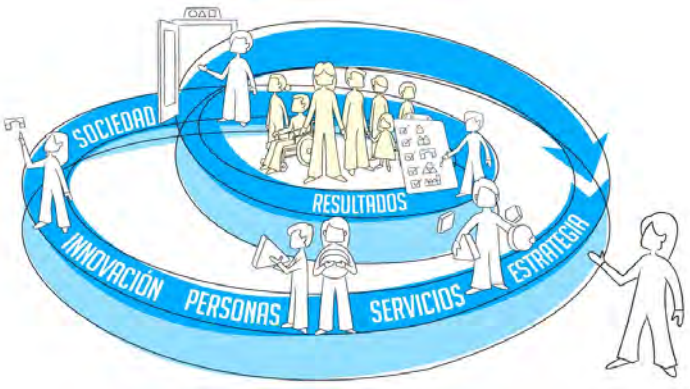
En el caso de la Dirección de Informática y Telecomunicaciones, al igual que el resto de Direcciones participantes, ha participado en una formación basada en el aprendizaje compartido y en talleres prácticos. Así, durante un año se han organizado 10 sesiones (de 5 horas de duración cada una de ellas) con los Directores/as y con las personas responsables de cada Servicio,

RED DE COLABORADORES Y COLABORADORAS

Las personas que actúan como «*colaboradoras*» son una de las piezas clave de este Modelo de Gestión, ya que se trata del agente activo que permitirá impulsar el cambio cultural necesario para alcanzar el éxito de esta iniciativa.

Es importante destacar que este colectivo está compuesto por personas del propio Gobierno Vasco que, coordinadas por el Equipo Aurrerabide de la Viceconsejería de Función Pública, trabajan en red para apoyar y extender esta nueva cultura de gestionar los procesos en sus unidades organizativas (Servicios, Direcciones...) y en el resto del Gobierno Vasco. Así mismo, colaboran con otros compañeros/as en la realización y contraste de evaluaciones de gestión en otras unidades organizativas de otros Departamentos y Organismos Autónomos.

acompañadas por una persona especialista, que ha actuado como «*entrenadora*».



En esas sesiones...

- Se ha explicado las características del modelo
- Se ha formado en herramientas relacionadas con la buena gestión.
- Se han comentado experiencias de éxito.
- Se ha facilitado estándares
- Se les ha tutorizado para que elaboren, ya dentro de sus direcciones y entre sesiones, la documentación básica que les deberá servir en su trabajo posterior. Como pueden ser, entre otros, los siguientes «*entregables*»: el Catálogo de servicios, el Mapa de procesos, las Fichas de los procesos operativos y la Planificación básica a dos años.

Asimismo, la DIT ha hecho uso de una plataforma informática (conocida con el nombre de «*Txoko de Aurrerabide*») para facilitar la carga y descarga de los distintos contenidos (documentos), la resolución de dudas por parte de la persona que actuado como facilitador/a y la relación con el resto de personas participantes.

FASES Y DESARROLLO

Dado que se trata de un proceso continuo, la metodología incluye una serie de fases y tareas que hay que ir realizando, como son las siguientes:

- ✓ Elaboración o actualización de la **Memoria «*Eginez Gara*»** («*Haciendo somos*», en castellano), que reúne todos los documentos finales del trabajo realizado.
- ✓ Autoevaluación (por personal de la unidad organizativa)
- ✓ Cumplimentación de los cuestionarios de evaluación
- ✓ Priorización para concretar áreas de consolidación y mejora
- ✓ Elaborar el Plan de Consolidación y Mejora

DE CARA A FUTURO

Con vistas al futuro, Aurrerabide plantea, entre otros objetivos, extender su Modelo de Gestión a la administración del sector educativo, sanitario y al resto de la administración institucional y del sector público, así como a todas aquellas administraciones públicas que lo soliciten.

En la actualidad, los responsables de Aurrerabide y el equipo de personas colaboradoras están en contacto con otras entidades[4] (Diputaciones Forales de Gipuzkoa y Bizkaia, Asociación de Municipios Vascos [EUDEL], Ayuntamiento de Vitoria-Gasteiz y Q-epea) para seguir extendiendo el Modelo.

En definitiva, Aurrerabide pretende ser un modelo o programa para gestionar mejor los servicios que ofrece el Gobierno Vasco a la ciudadanía y, como cualquier otro Modelo de mejora, requiere de un proceso continuo para seguir mejorando nuestros procesos internos. ❑

[4] **Entidades**:

- Diputación Foral de Gipuzkoa www.gipuzkoa.eus
- Diputación Foral de Bizkaia www.bizkaia.eus
- Asociación de Municipios Vascos (EUDEL) www.eudel.eus
- Ayto. de Vitoria-Gasteiz www.vitoria-gasteiz.org

Para más información podéis poneros en contacto con el Equipo Aurrerabide de la Viceconsejería de Función Pública en el siguiente correo electrónico: aurrerabide@euskadi.eus

O consultando la información que publican en la página web del proyecto: http://www.euskadi.eus/gobierno-vasco/innovacion-publica-mejora-administracion/gestion-avanzada-aurrerabide/inicio/

Formación desde el punto de vista del ENS

El Esquema Nacional de Seguridad (ENS) es un Real Decreto (RD 3/2010, de 8 de enero) que obliga a que el personal de las Administraciones Públicas reciba una formación adecuada de tal modo que se garantice la seguridad de las tecnologías de la información que manejan los Sistemas de Información, para que estos últimos estén protegidos.

El artículo 15. «*Profesionalidad*» del ENS, en su apartado segundo, dice que «*el personal de las Administraciones Públicas recibirá la* ***formación específica necesaria*** *para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración*».

CONCIENCIACIÓN Y FORMACIÓN

Está claro que la **concienciación y formación** del personal que trabaja en las Administraciones Públicas es de vital importancia para garantizar la seguridad de los sistemas, servicios, y de los datos que se manejan, y, por ende, crear la confianza necesaria para con la ciudadanía y empresas, de tal modo que se incentive el uso de los medios telemáticos en sus gestiones con las Administraciones.

Todas las personas expertas coinciden en que las protecciones en el campo de la seguridad (cortafuegos, software antivirus, filtros *antiSpam*, sistemas de detección y prevención de intrusiones…) son insuficientes ante los errores humanos. Como ya se apuntó en el anterior boletín Aurrera! (nº 59, de marzo de 2017) «*la* ***concienciación****, la* ***utilización de buenas prácticas de uso****, y* ***el sentido común*** *son las mejores armas para defenderse ante los ataques que recibimos (las personas delincuentes cibernéticas utilizan técnicas de ingeniería social para perpetrar sus ataques)*», a todo esto hay que añadir, junto con las «armas» mencionadas, la **formación** adecuada, y, de este modo, conseguiremos una protección también adecuada.

Un caso real: el de la persona que recibe en su buzón de correo corporativo un mensaje, de un remitente que desconoce, sobre un asunto con el que no tiene relación alguna, y que incluye un enlace (*link*) o archivos adjuntos, dentro de un mensaje que puede estar mal redactado o con faltas de ortografía, con un asunto como, por ejemplo, «*usted es el ganador de un premio…*», «*tiene una factura, pinche el siguiente enlace…*», «*ha recibido un paquete de correos…*», etc.; nuestro sentido común **desaconseja** que este tipo de correos sean abiertos, y mucho menos que vayamos a los enlaces que se indican, o abramos los archivos adjuntos. Siempre que recibamos este tipo de correos u otros que sean sospechosos, lo más adecuado es avisar a nuestro servicio informático, o al servicio de Centro de Atención a personas Usuarias (CAU[5]), para que tomen cartas en el asunto, y este sea tratado como un incidente de seguridad. Los ataques de *ransomware*[6] suelen iniciarse en las organizaciones a través de correos electrónicos como el que hemos explicado en las líneas anteriores.

PROGRAMA DE FORMACIÓN PROPIO

Desde GureSeK[7] (*Gure Segurtasun Kudeaketa*, proceso de gestión de seguridad de la información del Gobierno Vasco) se está definiendo y redactando un programa

[5] **CAU:** Centro de Atención a personas Usuarias de los Sistemas de Información del Gobierno Vasco, accesible a través del teléfono 440.

[6] **Ransomware:** (del inglés *ransom*, «*rescate*», y *ware*, por software). Es un software o programa informático (del tipo *malware*) que cifra determinados archivos o carpetas impidiendo que se puedan volver a usar. El fin último de este *malware* es conseguir dinero a través de un pago electrónico, generalmente en *Bitcoins* (moneda virtual), aunque realizando esta acción no hay garantías de que podamos recuperar dichos archivos.

[7] **GureSeK:** Sistema de Gestión de la Seguridad de la Información (SGSI) del Gobierno Vasco. Un SGSI «*es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización*». («*Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*», AENOR ediciones)

denominado *Programa de formación del Sistema de Gestión de la Seguridad de la Información del Gobierno Vasco*, a través de un documento, entroncado con la formación reglada que se realiza desde el IVAP[8], que establece las directrices a seguir para regular las acciones formativas y de capacitación del personal del Gobierno Vasco con respecto al proceso de gestión de la seguridad corporativa.

A continuación, vamos a tratar de explicar las características principales de esta formación (**las acciones formativas deberán ser aprobadas formalmente en los Comités** que se han creado en el Acuerdo de Consejo de Gobierno sobre la organización de la seguridad del Gobierno Vasco[9], aprobado el 30 de junio de 2015: «*Acuerdo por el que se aprueba la estructura organizativa y asignación de roles de seguridad para la administración electrónica del Gobierno Vasco*»).

ALCANCE Y OBJETIVOS DE LA FORMACIÓN GURESEK

La formación que se establece en este programa compete a todas las personas que trabajan en los Departamentos y Organismos Autónomos del Gobierno Vasco.

Los objetivos específicos de este programa de formación son los siguientes:

- Dar a conocer todos los aspectos relacionados con las políticas de seguridad en la utilización de medios electrónicos recogidas en el ENS.
- Dar a conocer y concienciar sobre las obligaciones generales para las personas usuarias del Gobierno Vasco.
- Aprender a identificar los riesgos a los que puede estar sometido un sistema de información (ya se han realizado, por parte de las personas responsables, las valoraciones de los servicios electrónicos)
- Reconocer los aspectos básicos relacionados con la gestión de la seguridad y la respuesta a incidentes de seguridad.
- Conocer los roles de seguridad asociados a nuestro ámbito de actuación.

MÓDULOS DE FORMACIÓN OFERTADOS

Dispondremos de tres módulos de formación:

- Introducción a la seguridad.
- Formación básica en seguridad.
- Formación avanzada en seguridad.

MÓDULO DE INTRODUCCIÓN A LA SEGURIDAD

Este módulo de introducción a la seguridad tiene como objetivos:

- Conocer el marco regulatorio en materia de seguridad.
- Conocer los principios generales (normas) que se deben respetar y asumir en el puesto de trabajo como persona usuaria respecto a la seguridad de la información. (recogidos en el documento «*Obligaciones generales para las personas usuarias—Gobierno Vasco*», estas normas vienen derivadas de las obligaciones legales aplicables en materia de protección de datos de carácter personal —RDLOPD— y de seguridad de los servicios electrónicos —ENS y MSPLATEA—).

Los contenidos de este curso serán los siguientes:

- Introducción a la seguridad: seguridad de la información, garantías de seguridad

[8] **IVAP:** es el Instituto Vasco de Administración Pública, es un organismo autónomo adscrito al actual Departamento de Gobernanza Pública y Autogobierno del Gobierno Vasco, cuya creación, estructura y funciones se establecen en la Ley de 16/1983, de 27 de julio. Uno de los tres grandes ámbitos de actuación del Instituto es la selección y formación del personal de la Administración vasca.

Más información en: www.ivap.euskadi.eus

[9] **Acuerdo de Consejo de Gobierno sobre la organización de la seguridad del Gobierno Vasco:** si queréis saber las obligaciones que tenemos como entidad en el ámbito de la seguridad de la información, documentación que debemos preparar y cómo está organizada la seguridad en el Gobierno Vasco, entre otros aspectos, podéis consultar el boletín Aurrera nº 56 (publicado en junio de 2016), y en concreto el artículo titulado «*Política de Seguridad de la Información (PSI)*».

DICAT (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad), Esquema Nacional de Seguridad, legislación respecto a la protección de datos de carácter personal, amenazas, etc.

«La formación de este programa compete a todas las personas que trabajan en el Gobierno Vasco.»

- Política de seguridad de la información.
- Soportes externos de información: dispositivos USB, otros dispositivos externos, utilización del papel, dispositivos multifunción.
- El puesto de trabajo: política de contraseñas (SARgune[10]), política de escritorio limpio, limpieza de metadatos...

MÓDULO DE FORMACIÓN BÁSICA EN SEGURIDAD

Los objetivos de este módulo, respecto al personal, son los siguientes:

- Dar a conocer unas nociones básicas del marco regulatorio aplicable en materia de Seguridad de la información.
- Asumir, por parte del personal, unas mínimas funciones relacionadas con la seguridad como una parte más de las tareas habituales.
- Conocer la estructura y el funcionamiento de GureSeK.
- Ser conscientes de las repercusiones de GureSeK en el puesto de trabajo.

[10] **SARgune**: es el sistema de acceso a los servicios de la Red Corporativa, cuyo objetivo es mejorar la seguridad y la calidad, a la vez que facilitar el acceso a los servicios de la Red Corporativa (correo electrónico, aplicaciones, sistemas...). Lleva implícito una política de contraseñas fuerte de acceso a los equipos.

Módulo de introducción a la seguridad: dimensiones de Seguridad DICAT

Las dimensiones de seguridad, también llamadas garantías de seguridad, suelen ser las siguientes:

- **Disponibilidad**: las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Integridad**: la información no ha sido alterada de manera no autorizada.
- **Confidencialidad**: la información ni se pone a disposición, ni se revela a personas, entidades o procesos no autorizados.
- **Autenticidad**: una entidad es quien dice ser o garantiza la fuente de la que proceden los datos.
- **Trazabilidad**: Las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Para cada servicio se analizan todas las dimensiones de seguridad que hemos citado, asignándoles a cada una de estas dimensiones un nivel **BAJO**, **MEDIO** o **ALTO**.

- **BAJO**. Si el incidente de seguridad tiene un perjuicio **LIMITADO** (reducción apreciable de la capacidad operativa para atender las obligaciones corrientes, daño menor a los activos de la organización, incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable, perjuicio menor a alguna persona...)
- **MEDIO**. Si el incidente de seguridad tiene un perjuicio **GRAVE** (reducción SIGNIFICATIVA de la capacidad operativa para atender las obligaciones corrientes, daño SIGNIFICATIVO a los activos de la organización, incumplimiento MATERIAL de alguna ley o regulación, o incumplimiento formal NO SUBSANABLE, perjuicio SIGNIFICATIVO a alguna persona, de difícil reparación...)
- **ALTO**. Si el incidente de seguridad tiene un perjuicio **MUY GRAVE** (ANULACIÓN de la capacidad operativa para atender las obligaciones FUNDAMENTALES, daño MUY GRAVE O IRREPARABLE a los activos de la organización, incumplimiento GRAVE de alguna ley o regulación, perjuicio GRAVE a alguna persona, de difícil o imposible reparación...)

Las personas destinatarias de este módulo de formación básica, y del primer módulo de introducción, son TODAS las que trabajan en el Gobierno Vasco, siendo obligatorio la realización de ambos; para ello, el IVAP pondrá a disposición de las personas adscritas a los Departamentos y Organismos Autónomos del Gobierno Vasco, a través de su catálogo general de cursos de formación anual, y con la periodicidad que dicho Organismo estime oportuno, una formación *on-line* para que todo el personal del Gobierno Vasco tenga la oportunidad y obligación de realizar. Si este módulo de formación básica ya se hubiese cursado, y los contenidos del curso hubiesen cambiado significativamente, se deberá volver a realizar.

MÓDULO DE FORMACIÓN AVANZADA EN SEGURIDAD

Los contenidos de este módulo avanzado serán los siguientes:

- ✓ Introducción. Resumen de los contenidos del módulo básico de seguridad.
- ✓ GureSeK. El proceso de seguridad del Gobierno Vasco: roles, funciones y responsabilidades del proceso; actividades del proceso; evaluación y seguimiento del proceso.
- ✓ GureSeK. Aplicación práctica: gestión de la seguridad (programa de mantenimiento GureSeK, metodología de análisis y gestión de riesgos, procedimiento de gestión documental, procedimiento de gestión de incidentes de seguridad, procedimiento de auditoría, sistemática de mejora continua...) y seguridad tecnológica (requisitos mínimos de arquitectura de seguridad, política de actualización de infraestructuras, política de detección y prevención de intrusiones, plan de continuidad...)

Este módulo de formación se desarrollará de manera presencial, a partir de una explicación teórico-práctica con soporte audiovisual.

Las personas que deben asistir a este módulo formativo son aquellas cuyo trabajo está en relación directa con la seguridad de la información en el ámbito de la administración electrónica. ❑

[11] **SCORM**: *Sharable Content Object Reference Model*, es un conjunto de especificaciones técnicas en el ámbito de aprendizaje a través de Internet (*e-learning*) que definen la estructura de los contenidos, su comportamiento y el de las plataformas de aprendizaje a la hora de alojar dichos contenidos y de ejecutarlos.

Formación a través del CCN-CERT

El CCN (Centro Criptológico Nacional), a través de su web, pone a disposición de cualquier persona, **en su parte pública**, dos cursos:

- **Esquema Nacional de Seguridad**: consta de nueve unidades o módulos con documentación de referencia:
  1. La Administración Electrónica y la Seguridad de la Información.
  2. Introducción al Esquema Nacional de Seguridad.
  3. Los requisitos mínimos de Seguridad de Información.
  4. Infraestructura y Herramientas de Seguridad.
  5. Auditorías de seguridad y Respuesta a incidentes
  6. Órganos y Organismos de referencia.
  7. Categorización de Sistemas y Medidas de Seguridad.
  8. Ejercicio práctico.
  9. Las Guías CCN-STIC del ENS e Información complementaria.
- **Análisis y Gestión de Riesgos de los Sistemas de Información**: cuyo objetivo es tratar todos los aspectos teóricos relacionados con la gestión y el análisis de riesgos en los sistemas de información (Introducción, Proceso de gestión de riesgos, Elementos de un análisis de riesgos, Activos, Amenazas, Impacto y riesgo, Salvaguardas, Tratamiento de los riesgos, Continuidad de las operaciones, y Conclusiones)

También han creado una serie de cursos relacionados con la seguridad en su parte privada.

Los cursos del CCN-CERT están desarrollados sobre el conjunto de especificaciones técnicas denominado SCORM[11].

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

ALBOAN:

Revisión y actualización de los Estándares tecnológicos del Gobierno Vasco

«La definición de estándares es considerada una iniciativa estratégica y necesaria para el Gobierno Vasco»

La Dirección de Informática y Telecomunicaciones (DIT) del Gobierno Vasco tiene entre sus competencias la de actuar como autoridad central encargada de la «*observancia, control y seguimiento de los estándares*», tal y como se indica en el Decreto 35/1997, de 18 de febrero, por el que se regula la planificación, organización, distribución de funciones y modalidades de gestión en materia de sistemas de información y telecomunicaciones.

La definición de estándares es considerada una **iniciativa estratégica y necesaria** para el Gobierno Vasco, por cuanto contribuye de forma directa a la consecución de los objetivos estratégicos de nuestra Administración, como son, por ejemplo:

- ✓ Incrementar y garantizar la máxima calidad en los servicios destinados a la ciudadanía y empresas
- ✓ Tender a la máxima eficacia y eficiencia en los procesos internos de la Administración
- ✓ Facilitar el despliegue de un entorno y red colaborativos entre Instituciones y Organismos Públicos relacionados con el Gobierno Vasco

El denominado Documento de Estándares Tecnológicos del Gobierno Vasco recoge las especificaciones y requisitos técnicos que dan soporte a los servicios desplegados por la Administración vasca en el ámbito de las nuevas tecnologías, de acuerdo siempre con los objetivos estratégicos establecidos por el propio Gobierno Vasco a través de sus diferentes planes, y que son gestionados por la Sociedad Informática del Gobierno Vasco, **EJIE**, S.A.

Para ello, el Documento de Estándares tecnológicos define una serie de estándares o productos, considerados corporativos o troncales, que darán soporte a los distintos Sistemas de Información de los Departamentos / Organismos Autónomos del propio Gobierno Vasco.

Dada la continua evolución de los distintos entornos tecnológicos que soportan la infraestructura de la Administración Electrónica vasca, así como las diferentes iniciativas que van surgiendo en los Departamentos y Organismos Autónomos que la componen, se ha considerado necesario abordar las tareas necesarias para revisar y actualizar el contenido de los Estándares tecnológicos del Gobierno Vasco, siempre con la idea de dar una adecuada respuesta (desde el punto de vista de la integración, calidad y seguridad) a todas las necesidades que se plantean, así como poder establecer el marco tecnológico que debe ser soportado en los próximos años.

Por todo ello, y con objeto de cumplir lo establecido en el Decreto 35/1997, la DIT ha lanzado una iniciativa para proceder a la

revisión y actualización de los Estándares tecnológicos del Gobierno Vasco.

DEL DOCUMENTO A LA WEB

Hasta ahora, toda la información referida a los Estándares tecnológicos estaba incluida en un documento denominado «*Documento de Estándares tecnológicos*», el cual se estructuraba en un documento principal y una serie de Anexos que lo complementan, todo ello accesible en la web de la DIT. Dichos anexos eran los siguientes:

1. Modelo de Interconexión con JASO y SARA
2. Estándares tecnológicos PLATEA
3. Catálogo de Estándares en el ámbito de la eAdministración
4. Política de Firma y Certificados
5. Metodología de gestión del cambio
6. Directrices de desarrollo
7. Formatos admitidos de documentos
8. Versiones actualizadas de los productos / tecnologías definidas
9. Estándares en el ámbito FLOSS

Mediante la iniciativa anteriormente mencionada, se han llevado a cabo los trabajos necesarios para revisar y actualizar la información recogida a día de hoy como Estándares tecnológicos, así como adaptarlo a un formato web.

Para ello, y a lo largo de las últimas semanas, la DIT, con la colaboración de las personas responsables de cada tema en EJIE, se ha encargado de revisar y actualizar los contenidos del documento principal y sus anexos.

Una de las novedades que van a incorporar en esta nueva edición los Estándares tecnológicos es que vamos a dejar de lado la idea de «*DOCUMENTO*» y pasaremos todos los contenidos a un formato de «***FICHAS***» que estarán accesibles también en la web, lo cual permitirá adoptar un diseño «*web responsive*», facilitando de esta forma el acceso y consulta desde cualquier dispositivo (ordenador, tableta, *smartphone*…). Además, gracias a los «*links*» o enlaces que se incluirán en cada ficha, podremos ver la relación existente entre un estándar y otro, así como su equivalente con las normas internacionales (ISO...), fecha en la que ha sido actualizada la información, etc.

LOGOTIPO

Una vez actualizada la información o contenido de las fichas, se abordó también la tarea de diseñar un logotipo que identificase a los Estándares Tecnológicos y a toda la documentación relacionada con ellos.

El logotipo finalmente seleccionado tiene las siguientes características:

- ✓ La letra «**E**» haría referencia a «*Euskadi*» y a los propios «*Estándares*».
- ✓ Simboliza la integración y conexión existente entre los distintos contenidos (estándares y productos)
- ✓ Representa la seguridad, robustez y unión de los contenidos.
- ✓ El color oscuro (gris oscuro) es el color asociado habitualmente a la tecnología
- ✓ El color azul, por su parte, representa la seguridad y la fiabilidad, y se asimila además con el azul de la web corporativa actual.

Si bien el trabajo de actualización ha finalizado, esto no significa que la información que se publique sea fija o estática, ya que gracias a la estructura que se le ha dado (mediante fichas), se podrá actualizar cualquier dato de una manera rápida y flexible. ❑

«Una de las novedades de esta edición es que se ha pasado del formato DOCUMENTO al formato FICHA»

[+info]:

Web de los Estándares Tecnológicos del Gobierno Vasco

http://www.euskadi.eus/informatica

(apartado «*Estándares tecnológicos*»)

Estandar teknologikoak
Estándares tecnológicos

60
junio 2017

¡¡BREVES!!

CONAN mobile

La Oficina de Seguridad del Internauta (OSI) de Incibe (Instituto Nacional de Ciberseguridad), uno de cuyos objetivos es reforzar la confianza de las personas en el ámbito digital a través de la formación en ciberseguridad, pone a disposición del público en general una herramienta gratuita para analizar y proteger dispositivos móviles (*smartphone*, *tablet*...) que tengan instalado el sistema operativo Android (versión 2.2 o superior).

Esta herramienta o aplicación (de cuya primera versión ya os informamos en el boletín Aurrera nº 49) se puede descargar desde la tienda de *GooglePlay* y te permite conocer el nivel de seguridad de tu dispositivo Android a través de un análisis del mismo (se requiere tener acceso a Internet).

El resultado del análisis indica el estado global de seguridad del equipo analizado: **EN RIESGO**, **REQUIERE ATENCIÓN**, **CORRECTO** y **PENDIENTE**; y se divide a su vez en cinco apartados:

1. Configuración (si tiene problemas o requiere atención, en función de los resultados del análisis del sistema operativo)
2. Aplicaciones (análisis de peligrosidad de las aplicaciones instaladas)
3. Permisos (categorizados por altos, medios y bajos; asociados a los permisos que se han concedido a las aplicaciones instaladas)
4. Servicio proactivo (alerta sobre eventos y conexiones que realizan las aplicaciones instaladas: conexiones WiFi inseguras, llamadas y mensajes a números de tarificación especial...)
5. Consejos OSI (para mejorar la seguridad del terminal móvil, se conecta directamente con la página web de Incibe).

Web: https://www.osi.es/es/conan-mobile

Género y Ciberseguridad

Al hilo de la gran repercusión que ha tenido recientemente el ataque masivo sufrido por muchas compañías e instituciones de distintos países a manos del ya famoso *malware* «*Wanna Cry*», mucha gente se ha dado cuenta de la importancia que tiene la ciberseguridad.

Son muchos los aspectos relacionados con la seguridad informática que hay que tener en cuenta frente a estas amenazas, como pueden ser, entre otros, la labor de concienciación que hay que hacer con los usuarios y usuarias de una entidad para evitar los ataques, y tener en cuenta las pérdidas económicas que nos puede ocasionar un virus o *malware* de este tipo, por ejemplo.

Sin embargo, existe otra vertiente o punto de vista que también conviene tener en cuenta, se trata de la relación que existe entre Ciberseguridad y la perspectiva de Género.

A este respecto, **Incibe** (Instituto Nacional de Ciberseguridad) acaba de organizar en León (los días 5 y 6 de junio) el «*I Foro Internacional de Género y Ciberseguridad*», donde se han analizado varias vertientes de la seguridad informática y el tema de género, como pueden ser: la importancia de la diversidad de género en el ámbito tecnológico y la ciberseguridad, o las acciones contra la violencia de género en el ámbito digital, así como los delitos de género en la red.

Podéis consultar la relación de participantes y las ponencias en la web de Incibe.

Página web: https://www.incibe.es