ÍNDICE

DISTRIBUIDO A:					
Presidente	**Director General**	**Director de Operaciones, Comercial, Logística y Vigilancia Estratégica**	**Secretario General**	**Directora de Talento, Organización y Marketing**	**Director Económico-Financiero y Coordinador Fondos Europeos**
Jefes/as de Departamento	**Jefe/as de División**	**Jefes/as de Unidad**			
REALIZADO POR: **Responsable de Ciberseguridad**		**REVISADO POR:** **Jefe de Transformación Digital**		**APROBADO POR:** **Jefe de Sistemas y Control de Gestión**	

1.- OBJETO Y ALCANCE

El objeto de este procedimiento es garantizar el cumplimiento de la normativa vigente en materia de seguridad de la información y, complementariamente a lo anterior, implementar los mecanismos necesarios para asegurar la calidad de la información gestionada por la APB y la prestación continuada de los servicios ofrecidos.

Se entenderá la seguridad de la información como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, por tanto, esta instrucción aplica a:

- Todos los sistemas de información y de telecomunicaciones de la APB.
- Todos los procesos de la administración electrónica.
- Todos los procesos que presten servicio a los ciudadanos, instituciones o empresas.
- Todo el personal de la APB y todo el personal de terceros que tenga relación con los procesos antes mencionados.

Regulaciones y estándares de seguridad de la información incluidos:

- Ley de Protección de Datos Personales.
- Norma ISO/IEC 27001.
- Norma ISO/IEC 27002.
- Reglamento General de Protección de Datos (GDPR).

2.- DESARROLLO

2.1.- DEFINICIONES

- Soportes informáticos: Medios de grabación de datos que se usan para realizar copias o pasos intermedios en los procesos que gestionan los ficheros (discos, disquetes, CD-ROM's, DVD's, cintas, memorias extraíbles, portátiles, etc.).
  Se considerarán soportes a efectos de transferencia de datos, los mensajes enviados o recibidos a través de cualquier red telemática y sus posibles anexos.

- Comité de Seguridad Corporativo: Grupo de personas, cuya composición y funciones se describen en la instrucción IGI 01.02/04 "Funciones y obligaciones en seguridad de la información".

- Responsable de Seguridad de la Información (CISO): (Chief Information Security Officer: 'Oficial principal de seguridad de la información'. Es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

- Responsable de la Información: Personas que determinan los niveles de seguridad de la información dentro del marco establecido en la legislación vigente por la que se regula el Esquema Nacional de Seguridad (ENS) y Reglamento General de Protección de Datos (RGPD).

- Responsable del Servicio: Personas que determinan los niveles de seguridad de los servicios dentro del marco establecido en la legislación vigente.

- Responsable del Sistema de Información: (En adelante, Responsable del Sistema). Son las personas responsables de mantener los sistemas de información permanentemente adaptados a las directrices de la Política de Seguridad.

- Administradores de la Seguridad de los Sistemas de Información: (En adelante Administradores de Seguridad). Son las personas designadas para administrar la seguridad del sistema.

- Usuarios: Todos los trabajadores/as de la **APB.**

- Fichero: Todo conjunto organizado de datos, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables.

- Tratamiento de la información: Cualquier operación o procedimiento técnico, automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, bloque o supresión de datos.

- Cambio: La adición, modificación o eliminación de hardware, red, software, entorno, sistema, estación de trabajo o documentación asociada que sea aprobado, soportado o tenga una línea de referencia.

- Control de cambios: Asegurar que todos los cambios sean controlados, incluyendo el sometimiento, análisis, proceso de decidir, aprobación, implementación y post-implementación del cambio.

- Lista de cambios planificados: Lista con los detalles de todos los cambios aprobados para implementación y las fechas propuestas.

- Registro de cambios: Registro que contiene los detalles de los elementos de configuración que han sido afectados por un cambio, los detalles de ese cambio y la autorización.

- Solicitud de Cambio: Registro con los detalles de una solicitud de cambio en cualquier elemento de configuración perteneciente a un servicio o infraestructura.

- Incidente de seguridad de la información. Evento que afecta a uno o más de los componentes cuya preservación constituye el objetivo de la seguridad de la información: Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.

- Afectado o interesado: Persona física titular de los datos que sean objeto de tratamiento.

- Procedimiento de disociación**:** Método por el cual la información que se obtenga no pueda asociarse a persona identificada o identificable.

- Bloqueo de datos**:** La identificación y reserva de los datos con el fin de impedir su tratamiento.

- Consentimiento del interesado**:** Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

2.2.- PRINCIPIOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

Los principios de la Política de Seguridad de la APB son los siguientes:

- La información y los servicios estarán protegidos contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información y los servicios deben estar disponibles, permitiendo su uso y acceso siempre que sea necesario, con las debidas autorizaciones.
- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tienen acceso a la información de la APB deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.
- Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.
- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad.
- Los incidentes de seguridad serán comunicados y tratados apropiadamente.
- La Seguridad de la Información deberá ser constantemente controlada y periódicamente revisada.
- Adicionalmente, el tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento y con las instrucciones y procedimientos de la APB.

- Se establecerán las operativas necesarias para cumplir con esta Política.
- La política será puesta a disposición de las partes interesadas que lo requieran mediante un correo electrónico.

2.3.- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La seguridad de la información estará gestionada por el **Comité de Seguridad Corporativo**.

Se dispone de un sistema que define y asigna las funciones y responsabilidades relacionadas con la seguridad de la información en las instrucciones:

- IGI 01.02/04 "Funciones y obligaciones en Seguridad de la Información"
- IGI 01.02/05 "Funciones de los usuarios de los Sistemas de Información"

Este comité se encargará de realizar el seguimiento de la seguridad de la información y de esta forma mejorar el sistema de gestión.

El Responsable de Ciberseguridad dispondrá de los medios, recursos y capacidades técnicas necesarios para el adecuado desempeño de sus funciones de supervisión, verificación, análisis de riesgos, auditoría técnica y respuesta a incidentes, garantizando su independencia operativa conforme a lo establecido en el Esquema Nacional de Seguridad y en el Sistema de Gestión de Seguridad de la Información.
La organización asegurará que este rol cuenta con el nivel de acceso, información y herramientas técnicas necesarias para realizar dichas funciones, sin perjuicio de los controles, supervisión y trazabilidad establecidos por el SGSI.

2.4.- PROCESOS INCLUIDOS EN LA POLITICA DE SEGURIDAD DE LA INFORMACION.

Estos procesos deberán ser comunicados, entendidos y cumplidos por toda la organización, ya que son requisitos aplicables a la seguridad de la información.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deben someterse a un proceso de análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

El **Responsable de Seguridad de la Información (RSI)** elabora el "Informe de análisis y gestión de riesgos" que deberá ser aprobado por el **Comité de Seguridad Corporativo** y asumido por los Responsables de la Información y los Responsables del Servicio.

CLASIFICACIÓN DE LA INFORMACIÓN

Se dispone de un sistema que clasifica la información gestionada por la APB en función de su sensibilidad en la instrucción IGI 01.02/06 "Clasificación de la información".

CONTROL DE ACCESO A LA INFORMACIÓN

Los usuarios de los sistemas de información únicamente tienen acceso a la información y funcionalidades necesarias para el desarrollo de su actividad profesional según se regula en la instrucción IGI 01.02/07 "Control de acceso a la información".

PLANIFICACIÓN DE LA SEGURIDAD

Se regula en las instrucciones:

- IGI 01.02/08 "Seguridad física de los Sistemas de Información"
- IGI 01.02/09 "Seguridad lógica de los Sistemas de Información"
- IGI 01.02/14 "Copias de seguridad y gestión de soportes".

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Se regula en las instrucciones:

- IGI 01.02/11 "Gestión de ficheros de carácter personal"
- IGI 01.02/12 "Protección de datos de control de acceso y videovigilancia"
- IGI 01.02/13 "Derechos en Protección de Datos"

DESARROLLO DE SOFTWARE

Se establecerá una operativa de desarrollo de software tendente a minimizar los riesgos durante el desarrollo, pruebas e implantación de programas y aplicaciones informáticas.

Se regula en la instrucción IGI 01.02/10 "Desarrollo de software".

GESTIÓN DE INCIDENTES DE SEGURIDAD

Se establecerá una operativa para la detección, análisis y respuesta a incidentes de seguridad de la información (ciberincidentes), según la instrucción IGI 01.02/15 "Gestión de incidentes de seguridad".

GESTIÓN DE LA CONTINUIDAD

Según la instrucción IGI 01.02/16 "Gestión de la continuidad".

2.5.- CONTROL, REVISIÓN Y AUDITORÍA

El Sistema de Gestión de Seguridad de la Información está sometido a auditoría interna de acuerdo con el PGI 03.03 "Auditorías internas y externas".

2.6.- ESTABLECIMIENTO DE OBJETIVOS Y MEJORA CONTINUA

El Sistema de Gestión de Seguridad de la Información (SGSI) se gestiona bajo un enfoque de mejora continua, basado en la definición, seguimiento y evaluación periódica de objetivos orientados a garantizar la eficacia y evolución del sistema, conforme a lo establecido en el PGI 01.03 "Establecimiento de objetivos". Asimismo, la identificación, gestión y seguimiento de acciones de mejora se realiza de acuerdo con el PGI 04.01 "Gestión de acciones de mejora", con el fin de reforzar el desempeño del sistema y asegurar su adecuación permanente a las necesidades de la organización y a los requisitos aplicables.

3.- REGISTRO Y ARCHIVO

CÓDIGO	DENOMINACIÓN	RESPONSABLE REGISTRO	MÉTODO DE ARCHIVO	LUGAR	TIEMPO DE CONSER-VACIÓN
----------	Informe de análisis y gestión de riesgos	CISO	Ultimo en vigor	Sistema informático	Permanente

4.- DOCUMENTOS DE REFERENCIA

No procede.