BANCO DE ESPAÑA
Eurosistema

PÚBLICO

DISTINTAS INICIATIVAS DESARROLLADAS POR EL BANCO DE ESPAÑA EN EL MARCO DE LA GOBERNANZA: PROCEDIMIENTO DE EVALUACIONES EXTERNAS SOBRE DETERMINADAS ACTIVIDADES Y ESTRUCTURA Y MEDIDAS EN EL TRATAMIENTO Y GESTIÓN DE LOS DATOS DE CARÁCTER PERSONAL

ENCUENTRO DE EXPERTOS SOBRE BUEN GOBIERNO Y TRANSPARENCIA: AUTONOMÍA DE LOS BANCOS CENTRALES

PONENTES:

- Cristina Hijosa, Jefa de la División de Secretaría Institucional
- Marisa Boronat, Jefa de la División de Gobernanza y Transparencia y, Delegada de Protección de Datos

14 de julio de 2022

VICESECRETARIA GENERAL

SUMARIO

- Iniciativa del **Plan Estratégico 2020-2024**: programa de **evaluaciones objetivas**, para impulsar la **modernización** del Banco y aumentar la **eficacia** de sus actuaciones, promoviendo un proceso de **mejora continua**, centrado en:

  - **Cometidos** de la institución (Programa de evaluaciones)
  - Funcionamiento de **órganos de gobierno y dirección** (Autoevaluación Consejo de Gobierno)

- Ejercicio de **sistematización y planificación:** experiencias puntuales previas y *benchmarking* de modelos internacionales

- Gobernanza del **Programa de evaluaciones**:

  - **Directrices** de evaluación: rigen la implementación del programa y establecen los principios básicos de funcionamiento
  - **Plan anual de evaluaciones**: aprobado por el Consejo de Gobierno a propuesta del Gobernador

- Misión: **examen y mejora de actuaciones**; **transparencia** y **rendición de cuentas**; uso racional de **recursos públicos** e impulso de la gestión de la **calidad**

- Objeto: actividades de ámbito operativo o de gestión del Banco en ejercicio de sus funciones
  - Se excluye el cumplimiento o control financiero o normativo, así como, aquellas actuaciones que correspondan a la Auditoría Interna del Banco o a otros organismos fiscalizadores o de control

- Resultado: valoración total o parcial de las actuaciones del Banco mediante (i) **indicadores** de eficacia, eficiencia y calidad, y (ii) establecimiento de **mecanismos de seguimiento y control** de objetivos

- **Principios** de actuación:

- ✓ Independencia de criterio, dictamen y juicio
- ✓ Transparencia
- ✓ Calidad y mejora continua
- ✓ Planificación de los trabajos


Planificación de las evaluaciones
Selección y contratación del equipo evaluador
Ejecución de la evaluación
Presentación de los resultados de la evaluación
Seguimiento de las recomendaciones
Difusión y comunicación (transparencia)

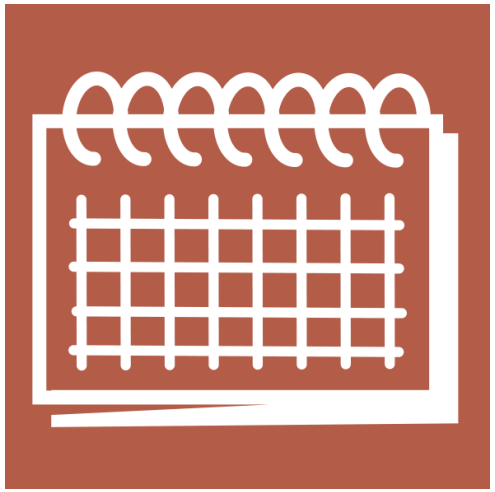
Coordinación del Programa de Evaluaciones

- En una primera etapa (dos primeros años de vigencia del programa anual de evaluaciones), se designará al efecto un **Coordinador,** dependiente del departamento de Gabinete del Gobernador.
  - ➢ *Futuro: ¿Oficina de evaluaciones?*

- **En cada evaluación*:***
  - Equipo evaluador: seleccionado para cada una de las evaluaciones (conocimiento más especializado e independencia).
  - *Adviser* seleccionado para cada evaluación, como enlace entre el equipo evaluador y el área sujeta a evaluación.

- **Órganos decisorios**

- El **Plan de Evaluaciones del Banco de España 2022-2023** contempla la realización de 3 ejercicios:



i. Evaluación de la **investigación** en el Banco de España

ii. Evaluación de la actividad de **proyección económica** del Banco de España

iii. Evaluación del **proceso de autorización de entidades de pago y dinero electrónico** del Banco de España

- El **Portal de Transparencia** del Banco de España recoge toda la información sobre el Programa de Evaluaciones, incluyendo el Plan anual.

El responsable del tratamiento debe ser capaz de **CUMPLIR** y **DEMOSTRAR** que teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, ha aplicado las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que trata los datos personales de forma licita, transparente, limitada a su finalidad, minimizando datos, con exactitud, conservándolos estrictamente el tiempo necesario, con integridad y confidencialidad.

Cambio de esquema mental: del cumplimiento pasivo al cumplimiento activo

Por "**mejores prácticas en materia de protección de datos**", entendemos aquellas experiencias o intervenciones implementadas en el marco de la gestión de datos personales, con resultados positivos en términos de eficiencia interna, transparencia frente a los interesados, resolución de problemas y, especialmente, de cumplimiento normativo.

¿Cuáles?

- ✓ DPD
- ✓ Registro de actividades de tratamiento
- ✓ Bases legitimadoras
- ✓ Transparencia
- ✓ Ejercicio de derechos
- ✓ Encargos de tratamiento
- ✓ Transferencias internacionales de datos personales
- ✓ Privacidad desde el diseño y por defecto
- ✓ Análisis de riesgos y evaluaciones de impacto
- ✓ Brechas de seguridad
- ✓ Otras

- ✓ **Nombrar a un DPD con la suficiente formación.**
- ✓ **Diseñar un mecanismo de información que confiera al DPD suficiente autoridad y evite conflictos de intereses.**
- ✓ **Nombrar un equipo de apoyo con expertos jurídicos e informáticos especializados.**
- ✓ **Informar a la autoridad de protección de datos del nombramiento del DPD.**
- ✓ **Creación de canales de consulta para las áreas involucradas en el tratamiento de datos.**
- ✓ **Nombrar "amigos de la protección de datos" que actúen como puntos de contacto en todas las áreas implicadas en el tratamiento de datos (responsables funcionales).**

- ✓ **Aprobación de un procedimiento interno de para realizar el registro de actividades de tratamiento.**
- ✓ **Redacción de un cuestionario para ayudar a las áreas a reconocer las actividades de tratamiento de datos. El cuestionario debería cubrir al menos las siguientes áreas:**
  - Fuentes de datos;
  - Objetivo;
  - Categorías de interesados y datos personales tratados;
  - Fundamentos jurídicos del tratamiento;
  - Flujos de información;
  - Periodos de conservación;
  - Cláusulas de información;
  - Destinatarios y posibles procesadores de datos;
  - Transferencias internacionales de datos;
  - Procedimiento para abordar los derechos de protección de datos;
  - Herramientas informáticas o aplicaciones aplicables.
- ✓ **Organizar reuniones con todas las áreas implicadas para resolver cuestiones y abordar incoherencias.**
- ✓ **Agrupación de las actividades de tratamiento por finalidad.**
- ✓ **Crear políticas y canales de comunicación para que las áreas puedan informar de nuevas actividades de tratamiento o de modificaciones de las existentes.**

- ✓ **Diseñar estrategias específicas de regularización.**
- ✓ **Cuando la base legitimadora es cumplimiento de una obligación legal o misión realizada en interés público, identificar correctamente la norma que establece la obligación o atribuye la competencia.**
- ✓ **En el caso de Administraciones Públicas no aplica el interés legítimo.**
- ✓ **No utilizar los datos personales para otra finalidad diferente de aquella para la que fueron recogidos e informada al titular de los datos.**
- ✓ **Establecer una metodología para la gestión de los consentimientos (conservación y retirada).**

- ✓ **Redactar una política general de privacidad detallada y una breve descripción de las políticas vinculadas a la misma.**
- ✓ **Establecer un mecanismo de revisión de la política de privacidad.**
- ✓ **Cláusulas informativas de doble capa: remisión al Registro de Actividades de Tratamiento.**
- ✓ **Establecer modelos de cláusulas informativas y ponerlos a disposición de todos los empleados a través de intranet.**
- ✓ **Establecer un mecanismo de revisión de las cláusulas informativas utilizadas.**

- ✓ **Aprobación de un procedimiento interno de gestión de ejercicio de derechos.**
- ✓ **Implementar en la oficina virtual un procedimiento especifico con un formulario *ad hoc*.**
- ✓ **Gestionar todas las peticiones de forma centralizada a través del DPD.**
- ✓ **Creación de modelos de respuesta: la mayoría de las peticiones son estándar.**

- ✓ **Aprobación de un procedimiento interno de gestión de encargos de tratamiento.**
- ✓ **Sensibilización para que los gestores de contratos identifiquen cuando hay un encargo de tratamiento.**
- ✓ **Revisión por parte del DPD de todos los contratos que implican un encargo de tratamiento.**
- ✓ **Mecanismos para supervisor el cumplimiento de RGPD por parte del proveedor encargado de tratamiento.**
- ✓ **Especial atención al almacenamiento en nube por parte del proveedor encargado de tratamiento (transferencias internacionales de datos).**

- ✓ **Registrar todas las transferencias internacionales en el RAT, indicando los motivos legales en los que se basa la transferencia.**
- ✓ **Sensibilización para que los empleados reconozcan los posibles comunicaciones internacionales**
- ✓ **Controlar la frecuencia de las transferencias con un determinado país.**
- ✓ **Especial atención a la posible realización de transferencias internacionales por parte del proveedor encargado de tratamiento.**

CUESTIONARIO VALORACIÓN PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO	
INTRUCCIONES: MARCAR CON UNA X O CON SI/NO CADA A UNA DE LAS OPCIONES DE LAS PREGUNTAS	
[En caso de duda y para cumplimentar la Parte II, contacte con #VCSG_DIV.Gobernanza y Transparencia]	
1. PARTE I. CUESTIONARIO A CUMPLIMENTAR POR EL GESTOR DEL PROYECTO Y EL DEPARTAMENTO PROPIETARIO	
1.1. ¿El sistema va a incluir datos personales, esto es, información que permita identificar, directa o indirectamente, a personas físicas (como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea, etc.)?	
	Sí.
	No (en ese caso, no es necesario que cumplimentes más preguntas).
Nota: Si la respuesta es NO, no cumplimetar nada más. SI la respuesta es SI, continuar con el cuestionario	
1.2. ¿Qué categorías de datos personales van a incluirse en el sistema? [Dentro de la categoría que se marque deberán eliminarse los ejemplos de datos no tratados, enumerándose solo aquellos datos que se incluirán en el sistema]	
	Datos identificativos: Nombre, apellidos, NIF, etc.
	Datos de contacto: Correo electrónico (personal o profesional), dirección postal, teléfono, etc.
	Datos profesionales y académicos: Formación, cargo, nº empleado, código de usuario, etc.
	Datos económicos y financieros: Salario, cuentas, transacciones, información financiera, etc.
	Datos de características personales: Nacionalidad, fecha y lugar de nacimiento, etc.
	Datos tecnológicos: Dirección IP, etc.
	Datos relativos a la comisión de infracciones penales.
	Datos de categoría especial: Datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o a la orientación sexual.
	Datos de sujetos vulnerables: Datos de menores de 14 años, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes.
	Otros: *[incluir detalle].*
1.3. Describir brevemente para que y como se utilizan los datos de las categorías indicadas en la pregunta anterior	
[Incluir descripción]	
1.4. ¿Quiénes son los colectivos titulares de los datos personales que van a incluirse en el sistema?	
	Empleados y subcontratados.
	Ciudadanos.
	Otros: *[incluir detalle].*

- ✓ **Sensibilización sobre la necesidad de notificar las nuevas actividades de tratamiento de datos al DPD antes de diseñarlas: cuestionario de privacidad.**
- ✓ **Elaboración de plantillas fácilmente comprensibles para informar de las nuevas actividades de procesamiento de datos.**
- ✓ **Seguimiento especial de las aplicaciones informáticas.**
- ✓ **Nombrar "mejores amigos de la protección de datos" en los ámbitos en los que se tratan los datos personales para que actúen como puntos de contacto con el DPD.**

- ✓ **Aprobación de un procedimiento interno de análisis de riesgo y evaluaciones de impacto.**
- ✓ **Determinar los criterios de análisis de riesgo y los niveles y categorías de riesgo.**
- ✓ **Aplicar criterios a todas las actividades de procesamiento para detectar las necesidades de evaluación de impacto.**
- ✓ **Disponer de plantillas para realizar análisis de riesgo y, en su caso, evaluación de impacto.**
- ✓ **Medidas de seguridad preestablecidas para cada nivel de riesgo.**
- ✓ **Medidas mitigadoras preestablecidas.**
- ✓ **Aplicación del Esquema Nacional de Seguridad.**

- ✓ **Aprobación de un procedimiento interno de gestión de brechas.**
- ✓ **Mecanismos que garanticen la notificación inmediata al DPD.**
- ✓ **Campañas de sensibilización para todos los empleados.**
- ✓ **Modelo de informes de evaluación de la brecha y de notificación.**
- ✓ **Informes de seguimiento.**
- ✓ **Obligaciones de notificación específicas para los proveedores encargados de tratamiento.**

- ✓ **Elaboración de informes de tratamiento.**
- ✓ **Aprobación de normativa interna: circular interna 5/2020.**
- ✓ **Elaboración de procedimientos respecto de las materias más sensibles: notas internas.**
- ✓ **Sección específica de protección de datos en intranet.**
- ✓ **Memoria como rendición de cuentas al más alto nivel.**
- ✓ **Auditorías de cumplimiento internas o externas.**
- ✓ **Participación activa en *networks* de expertos.**

BANCO DE ESPAÑA
Eurosistema

MUCHAS GRACIAS POR SU ATENCIÓN

VICESECRETARÍA GENERAL