Modelo de Gobierno corporativo de protección de datos

Sencillo | Personal | Justo
Simple | Personal | Fair

Santander

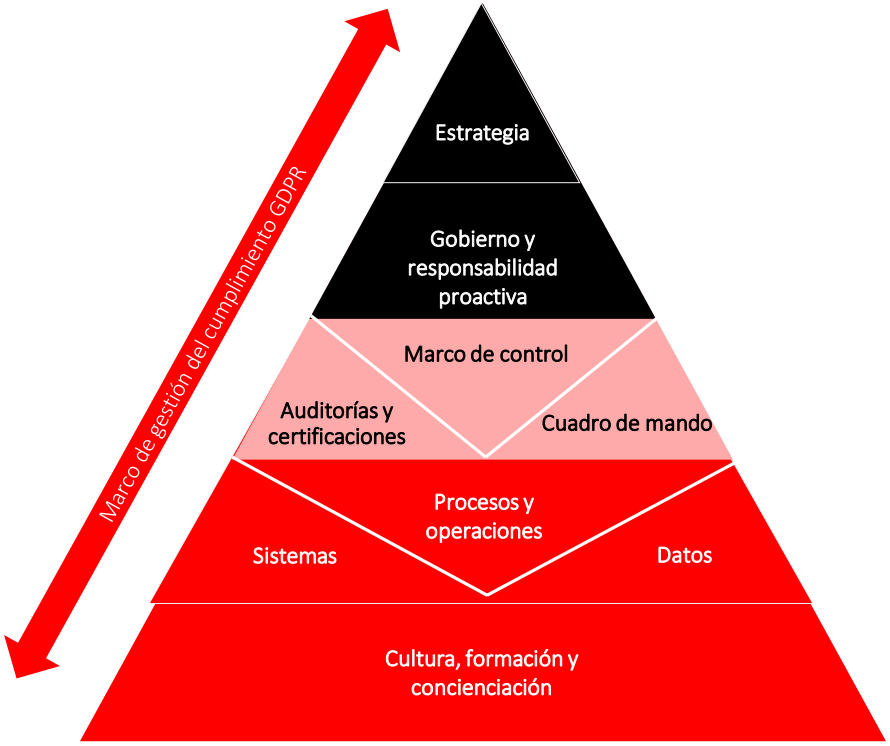
Contenido

1. Marco de referencia.
2. Responsables de protección de datos.
    - Estructura organizativa del modelo.
3. Funciones y responsabilidades.

1.- Marco de referencia.

Estructura del marco de referencia

Para una adecuada gestión del cumplimiento de la normativa de protección de datos, un conjunto de componentes funcionan de manera coordinada y en línea con la estrategia definida de acuerdo con el siguiente marco de referencia, que identifica los elementos clave.



Capa de Gobierno:
- Estructura de *governance* que organice y delimite adecuadamente los roles y responsabilidades.
- Políticas y el marco general de aplicación a todos los componentes del marco de referencia, y que fijará la estrategia de privacy de la entidad.

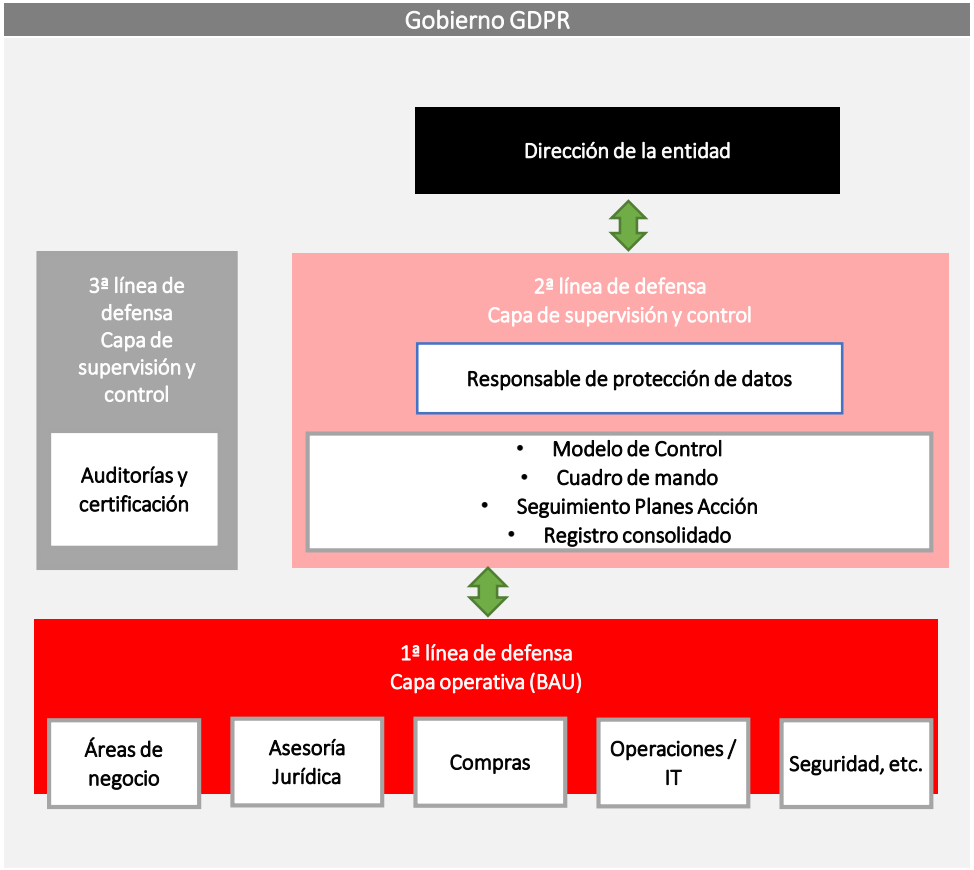
Capa de supervisión y control:
- Modelo de control basado en tres líneas de defensa
- Modelo de gestión/cuadro de mando que permitan la toma decisiones
- Seguimiento de Planes de acciones mitigantes y registro consolidado de información de gestión GDPR (inventarios, DPIA,..)

Capa operativa:
- Conjunto de procesos, procedimientos y operaciones que dan soporte operativo al cumplimiento de GDPR. Deberán estar adecuadamente coordinados con la Capa de supervisión y control, y de acuerdo con la Capa de Gobierno.

1.- Marco de referencia.

Líneas de defensa del marco de referencia

El modelo de gobierno de protección de datos a nivel entidad se encuadra en el modelo de gobierno corporativo/grupo.



3ª línea de defensa:

Visión independiente sobre el grado de cumplimiento de la gestión de la privacidad en la organización, tomando como referencia la regulación vigente, así como las políticas y procedimientos existentes.

2ª línea de defensa:

Supervisión de la gestión de las actividades en materia de privacidad realizadas por la primera línea de defensa. Esta segunda línea de defensa debe asegurarse de que los riesgos de privacidad se gestionan de acuerdo con el apetito de riesgo formulado por la alta dirección y promoverá una sólida cultura de riesgos y cumplimiento en toda la organización.

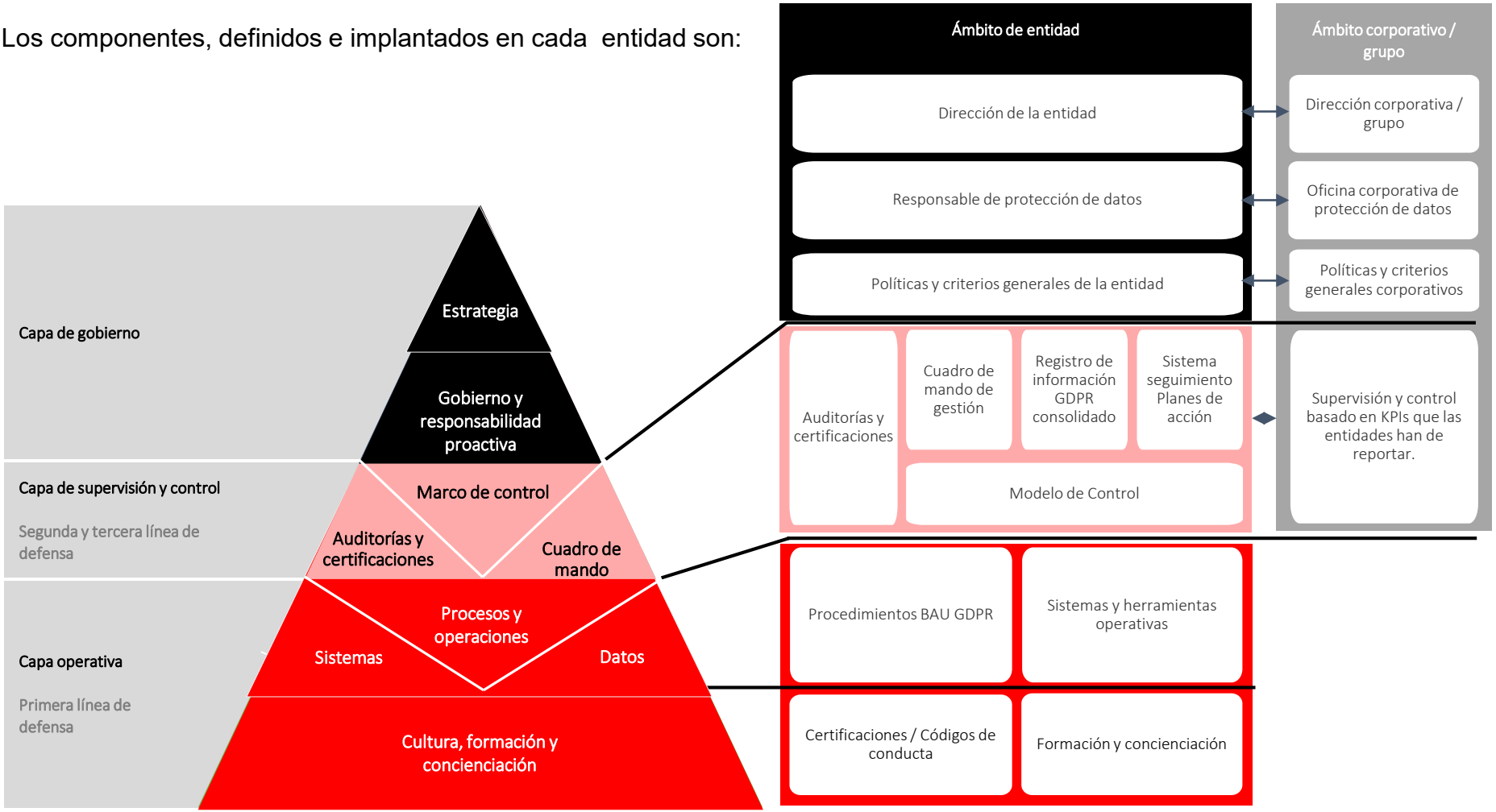
1ª línea de defensa:

Las unidades de negocio y de apoyo son la primera línea de defensa responsables de identificar, evaluar y controlar los riesgos en materia de privacidad. Deben conocer y llevar a cabo las políticas y procedimientos, y estar dotados con los recursos suficientes para hacerlo de forma eficaz.

1.- Marco de referencia.

Líneas de defensa del marco de referencia

Los componentes, definidos e implantados en cada entidad son:



Contenido

1. Marco de referencia.
2. **Responsables de protección de datos.**
    - Estructura organizativa del modelo
3. Funciones y responsabilidades.

2.- Responsables de protección de datos.

Existen tres figuras principales que ostentan el máximo nivel de responsabilidad en el cumplimiento de protección de datos, diferenciando entre el ámbito local y el corporativo.

Ámbito local

DPO/Head

Máxima autoridad en protección de datos

1. Punto de contacto con la Autoridad de Control y con los Interesados
2. Cooperación con la Autoridad de Control
3. Asesoramiento en materia de protección de datos
4. Control y supervisión
5. Formación
6. Asesoramiento en los DPIAs
7. Realización de las Consultas Previas ante la Autoridad de Control
8. Supervisar el Registro de tratamientos
9. Asesoramiento en la comunicación de las Brechas de Seguridad
10. Asesoramiento en la gestión de terceros
11. Supervisar el ejercicio de derechos de los interesados

Champion

SME en la unidad o sociedad

1. Punto de contacto interno como función de soporte de primer nivel
2. Canalizador de dudas y solicitudes de soporte:
    a) A la Oficina corporativa de protección de datos, en el caso de unidades y sociedades corporativas
    b) Al DPO/Head de la jurisdicción, en el caso del resto de sociedades
3. Encargado de la distribución interna de criterios, procedimientos y otras instrucciones.

Ámbito corporativo

Oficina corporativa de protección de datos

Supervisor global del cumplimiento

1. Supervisar el cumplimiento del Grupo en materia de protección de datos
2. Reporting consolidado a la Alta dirección del Grupo
3. Punto de interlocución con las Autoridades competentes a nivel global
4. Análisis de impacto a nivel global de los incidentes de seguridad
5. Análisis de riesgos globales en materia de protección de datos
6. Facilitar criterios corporativas y ser punto de contacto en la corporación para los DPOs/Heads de las entidades

Soporte al DPO/Head y champions de las unidades y sociedades corporativas

1. Asesoramiento especializado en la regulación y apoyo en el desempeño de las funciones propias del DPO/Head.

2.- Responsables de protección de datos.

Cada entidad o unidad corporativa sujeta a la normativa de protección de datos cuenta con un responsable en protección de datos, que podrá ser un DPO/Head o un "*champion*" en función de los siguientes criterios.

1. Entidades del Grupo.

De acuerdo a los requerimientos del GDPR, los siguientes supuestos obligan a una entidad jurídica al nombramiento formal de un DPO ante la autoridad local:

Supuesto
Observación habitual y sistemática de interesados a gran escala.
Categorías especiales de datos personales (p.e. origen étnico o racial, opiniones políticas, afiliación sindical, datos de salud, condenas e infracciones penales, etc.)
En los casos que lo exija el Derecho de la Unión o de los Estados miembros.

- Adicionalmente, según la Ley Orgánica de Protección de datos, será necesario nombrar DPO para entidades de crédito y sociedades que ofrezcan servicios de inversión.

Las entidades del Grupo que cumplen alguno de los supuestos cuentan con un ***DPO*** que responde directamente ante la autoridad de control competente local y sus interesados.
En el resto de los casos se cuenta con un ***champion de protección de datos***.

Para el resto (fuera del ámbito de aplicación GDPR), todas las unidades cuentan con un responsable de protección de datos.

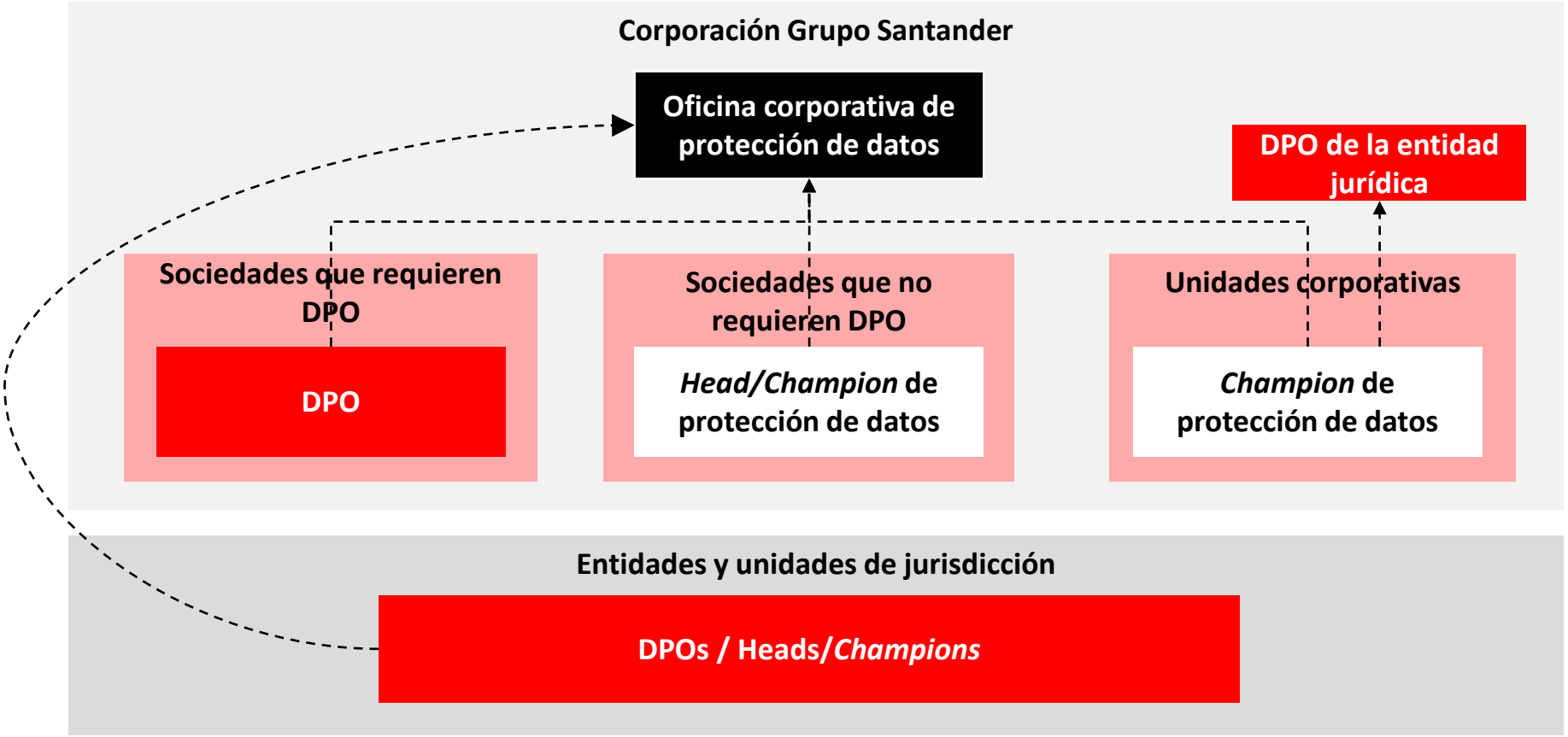
2. Unidades y áreas corporativas:

Las unidades que tratan datos de carácter personal cuentan con un ***champion*** que depende del responsable de protección de datos de la entidad a la que pertenecen.

2.- Responsables de protección de datos.

Estructura organizativa del modelo

El modelo de gobierno presenta la siguiente estructura organizativa y de relación entres las figuras responsables de protección de datos:



Contenido.

1. Marco de referencia para el cumplimento de la normativa GDPR
2. Responsables de protección de datos
   - Estructura organizativa del modelo
3. **Funciones y responsabilidades**

3.- Funciones y responsabilidades.

- **R - Responsible**: Responsable de realizar la tarea.
- **A - Accountable**: Responsable de que la tarea se cumpla.
- **C - Consulted**: Figura que debe ser consultada para la realización de la tarea.
- **I - Informed**: Figura que debe ser informada sobre la realización de la tarea.

Componentes / Roles		Dirección corporativa / grupo	Oficina corporativa de protección de datos	Dirección de la entidad	DPO/Head	Champion, en caso de existir	Área Responsable tratamiento	Encargado de tratamiento tercero	Otras áreas
Modelo de gobierno	Definición del Modelo de gobierno	I	I	C, I	R, A	C, I	I	I	I
Aspectos institucionales y representación	Punto de contacto con la Autoridad de Control y con los Interesados	I*	I	I*	R, A	C	C		
	Cooperación con la Autoridad de Control	I*	I	I*	R, A	C	C		
Aspectos operativos	Definición de la política local	I*	C, I	A, C	R	C, I	I	I	I
	Identificación cambios normativos y fijación criterios	I*	C, I	C	R, A	C, I	I	I	I
	Asesoramiento en materia de protección de datos		C		R, A	R**	C, I	I	I
	Adaptación de procedimientos BAU	I*	I	I*	A, C	C	I	C	R
	Identificación y evaluación de posibles nuevos tratamientos				A, C	A, C**	R	C	
	Definición de metodología de riesgos a emplear (incluye fijación apetito de riesgo)	I*	I	I*	A, R	I	I		C (p.e. Riesgos)
	Realización de análisis de riesgos pre-DPIA y DPIAs		I	I*	A, C	A, C**	R	C	C (p.e. CISO, Riesgos,Legal)
	Consultas previas ante Autoridad de control		I	C, I	A, R	C	C, I		
	Mantenimiento actualizado del registro de tratamientos		I	I*	A, I	C, I	R	C	C (p.e. CISO, Legal, etc.)

* A criterio del DPO/Oficina corporativa de protección de datos

** Responsabilidad en primera instancia, compartida con el DPO en caso de no poder asumirse

*** Unidades sin DPO

3.- Funciones y responsabilidades.

- **R - Responsible**: Responsable de realizar la tarea.
- **A - Accountable**: Responsable de que la tarea se cumpla.
- **C - Consulted**: Figura que debe ser consultada para la realización de la tarea.
- **I - Informed**: Figura que debe ser informada sobre la realización de la tarea.

Componentes / Roles		Dirección corporativa / grupo	Oficina corporativa de protección de datos	Dirección de la entidad	DPO/Head	Champion, en caso de existir	Área Responsable tratamiento	Encargado de tratamiento tercero	Otras áreas
Aspectos operativos	Obtención de consentimientos y cumplimiento de deber de información				A	A, I	R	R	R (p.e. negocio, operaciones)
	Identificación de incidentes de seguridad				A	A, I	R	R	R (p.e. CISO)
	Evaluación y comunicación de incidentes de seguridad	I	I	I	R, A	R***, A, C	C	C	C (p.e. CISO, negocio, etc.)
	Homologación proveedores		I, C	I*	A, I	I	C	C	R (p.e. Costes, Gestor servicio, gestión proveedores)
	Gestión de contratos de terceros			I*	A, I	I	C	C	R (p.e. Aquanima, Legal)
	Seguimiento del cumplimiento por parte de proveedores			I*	A, I	I	C	C	R (p.e. Aquanima, gestión proveedores)
	Atención a las solicitudes de ejercicio de derechos de los interesados		I	I*	A	A	C	C*	R (p.e. operaciones, Legal)
	Realización de cambios operativos e IT (acorde a procedimientos y DPIAs)			I*	A, C	A, C**	R	I	R (p.e. IT)
	Ejecución de operaciones BAU según procedimientos y criterios			I*	A	A	R	I	R
	Ejecución acciones formativas y de concienciación		C	I*	A	A	C		R (p.e. Formación)

* A criterio del DPO/Oficina corporativa de protección de datos

** Responsabilidad en primera instancia, compartida con el DPO en caso de no poder asumirse

*** Unidades sin DPO

3.- Funciones y responsabilidades.

- **R - Responsible**: Responsable de realizar la tarea.
- **A - Accountable**: Responsable de que la tarea se cumpla.
- **C - Consulted**: Figura que debe ser consultada para la realización de la tarea.
- **I - Informed**: Figura que debe ser informada sobre la realización de la tarea.

Componentes / Roles		Dirección corporativa / grupo	Oficina corporativa de protección de datos	Dirección de la entidad	DPO/Head	**Champion, en caso de existir**	Área Responsable tratamiento	Encargado de tratamiento tercero	Otras áreas
Modelo de Control interno de cada entidad/unidad	Definición del Modelo de Control		I	I	A, C	A, C**	C	C	R (Cumplimiento y áreas en 1 LOD)
	Ejecución de controles				A, I	A, I	I		R (responsables de controles)
	Seguimiento del cumplimiento	I*	I	I*	A, R	A, C, I	I	C	C (responsables de controles)
Cuadro de mandos (modelo de relación Corporación-subsidiaria)	Definición del sistema de indicadores de gestión		A, R		C, I	C, I			
	Reporting de indicadores		I	I*	A, R	A, R**			
	Análisis de indicadores	I*	A, R		A, C, I	A, C, I			
Gestión de aspectos relevantes e incidencias críticas	Gestión de aspectos relevantes e incidencias críticas	I*	C, I	C, I	A, R	A, C	C	C	C

* A criterio del DPO/Oficina corporativa de protección de datos

** Responsabilidad en primera instancia, compartida con el DPO en caso de no poder asumirse

*** Unidades sin DPO

Our purpose is to help people and businesses prosper.

Our culture is based on the belief that everything we do should be

Simple | Personal | Fair

Santander

MEMBER OF
Dow Jones
Sustainability Indices
In Collaboration with RobecoSAM

FTSE4Good