La actividad de Riesgos en CACEIS Bank Spain SAU se rige por los siguientes principios, los cuales están alineados con marcos y políticas de Caceis S.A. y tienen en cuenta las recomendaciones de los supervisores, reguladores y las mejores prácticas del mercado:

- Una cultura de Riesgos integrada en la organización.
- Independencia de la función de riesgos.
- Enfoque integral de todos los riesgos como objetivo para su adecuada gestión y control.
- Un modelo de organización y gobierno que asigna a todos los riesgos responsables su control y gestión.

CACEIS Bank Spain SAU cumple con el Marco general de riesgos, donde se recogen los principios básicos aplicables en la gestión de los riesgos que están establecidos en el mapa de riesgos (financieros, no financieros y transversales).

Gobierno de los riesgos

Además de las funciones indelegables en materia de riesgos que desempeña el Consejo de Administración, en la actualidad celebra con carácter recurrente el Comité Control de Riesgos, presidido por el director general de la sociedad, y el Comité de Riesgos y Cumplimiento, presidido por el Chief Risk Officer, que es el órgano encargado del control efectivo de todos los riesgos.

Estructura organizativa de la función de riesgos

El Chief Risk Officer es el responsable de la función de Riesgos. Reporta tanto al Director General como al Consejo de Administración, realizando la labor de asesoramiento, control y challenge a la línea ejecutiva de la entidad.

Riesgo Operacional y Tecnológico; modelos de identificación, medición y evaluación

Dado el negocio de CACEIS Bank Spain SAU, el riesgo operacional y tecnológico constituye un foco muy relevante de gestión, que sigue en todo momento los marcos y políticas de la entidad. Así, se han definido una serie de técnicas/ herramientas cuantitativas y cualitativas a nivel para medir y evaluar el riesgo tecnológico y operacional, que se combinan para hacer un diagnóstico (sobre la base de los riesgos identificados) y obtener una evaluación (a través de la medición/evaluación) de cada unidad.

El análisis cuantitativo se realiza principalmente con herramientas que registran y cuantifican el nivel de pérdidas asociadas con los eventos de riesgo operacional:

- Base de datos interna de los eventos, cuyo objetivo es capturar todas las pérdidas por riesgo operacional de la Unidad. La captura de eventos relacionados con el riesgo operacional no se restringe por establecer umbrales (es decir, no hay exclusiones por razones de cantidad) y se consideran todos los eventos con impacto contable (incluyendo los de impacto positivo), así como los no contables. Hay procesos de conciliación contable para garantizar la calidad de la información recogida en las bases de datos. Los principales eventos de riesgo operacional son documentados y revisados de forma individual.
- Base de datos externa de los acontecimientos. El uso de bases de datos externas permite un análisis más detallado y estructurado de los eventos que se producen en el sector.

- Análisis de escenarios de riesgos operacionales. Se obtiene una opinión de expertos de las líneas de negocio y de los gestores de control de riesgos cuyo propósito es identificar eventos potenciales con una muy baja probabilidad de ocurrencia, pero que podrían significar una gran pérdida para la entidad. Se evalúan sus posibles efectos y se establecen controles adicionales y medidas de mitigación para reducir la eventualidad de un alto impacto económico.

Las herramientas definidas para el análisis cualitativo tratan de evaluar aspectos (cobertura/exposición) vinculados al perfil de riesgos, lo que permite la existencia de un entorno de control. Estas herramientas son principalmente:

- Mapa de procesos y riesgos y cuestionarios de autoevaluación. Una evaluación adecuada de los riesgos, sobre la base del criterio experto de sus gestores, permite una visión cualitativa de los principales focos de riesgos de la Unidad, independientemente de haberse materializado antes.
- La metodología empleada estima la pérdida inherente y residual de acuerdo con el mapa de procesos y riesgos. En concreto, los expertos de las distintas áreas de negocio y de soporte evalúan los riesgos asociados a los procesos y actividades, estimando la frecuencia media de ocurrencia en la materialización de los riesgos, así como la severidad media. El ejercicio también incorpora la evaluación de la pérdida mayor, la evaluación del entorno de control y la vinculación con el riesgo reputacional y regulatorio. La información obtenida se analiza a nivel local y corporativo y se incorpora dentro de la estrategia de reducción del riesgo operacional a través de medidas para mitigar los principales riesgos.
- Sistema de indicadores de riesgo operacional, en continua evolución y en coordinación con el Área de Control Interno. Son diversos tipos de estadísticas o parámetros que proporcionan información sobre la exposición de una entidad al riesgo. Estos indicadores son revisados periódicamente con el fin de alertar ante cambios que podrían revelar problemas con los riesgos.
- Recomendaciones de auditoría. Proporcionan información relevante sobre el riesgo inherente debido a factores internos y externos, que permiten identificar debilidades en los controles.
- Otros instrumentos específicos que permiten un análisis más detallado del riesgo tecnológico, tal como, por ejemplo, el control de incidentes críticos en los sistemas y eventos de ciber-seguridad.

También se han definido protocolos para escalar incidencias relevantes, dando visibilidad a ciertos eventos de riesgo.

Además de los procesos regulares de identificación y evaluación de riesgos, CACEIS Bank Spain SAU ha desarrollado un plan de contingencia y de continuidad del negocio para completar los instrumentos de gestión esenciales que, junto con el resto de los instrumentos y principios, constituyen los componentes de gestión global de riesgos de la entidad.