POLÍTICA CORPORATIVA DE CONTROL Y GESTIÓN DE RIESGOS

El Grupo Euskaltel es el Grupo Empresarial compuesto por aquellas sociedades que, en el sentido de la Ley, forman parte de un Grupo mercantil cuya entidad dominante es Euskaltel S.A. Las referencias que, en esta política, se hacen al Grupo Euskaltel o a Euskaltel, deben entenderse de aplicación a todas y cada una de las sociedades individuales que lo componen.

Este documento, que forma parte del Gobierno Corporativo del Grupo Euskaltel, establece la política de control y gestión de riesgos y de control interno fijada por el Consejo de Administración del Grupo Euskaltel, en adelante, la Política Corporativa de Riesgos.

Objetivo de la Política Corporativa de Riesgos

El objetivo de esta política es establecer los principios básicos que deben regular la actuación del Grupo Euskaltel para el control y la gestión de los Riesgos de todo tipo a los que se enfrenta, o puede enfrentarse en el futuro, y las principales responsabilidades en dicha gestión.

Esta política se desarrolla y complementa por medio del resto del Sistema de Gobierno Corporativo del Grupo, en el que se integra, incluyendo políticas, manuales, instrucciones, y cualesquiera otros documentos.

La Política Corporativa de Riesgos, que conforma en su conjunto el Marco General de Actuación del Grupo en materia de Gestión de Riesgos, se estructura en los apartados siguientes:

- Definiciones y tipos de riesgo,
- Principios Generales de Actuación,
- Sistema de Gestión de Riesgos,
- Roles y Responsabilidades,
- Mapa de Riesgos Corporativos, y
- Nivel de tolerancia al Riesgo.

Definiciones y tipos de riesgos

A los efectos de esta política, un Evento es un incidente o acontecimiento, proveniente de fuentes internas o externas del Grupo Euskaltel, que afecta o puede afectar a la consecución de sus objetivos y que puede tener un impacto positivo, negativo, o de ambos tipos a la vez, sobre el cumplimiento de dichos objetivos. El Riesgo se define como la posibilidad de que un Evento ocurra y afecte desfavorablemente al logro de los objetivos del Grupo.

La gestión de riesgos corporativos es el proceso diseñado para identificar eventos potenciales que puedan afectar al Grupo y gestionar los eventuales riesgos dentro de los umbrales aceptados, con la finalidad de proporcionar un nivel de seguridad razonable sobre el logro de los objetivos del Grupo.

El Control Interno se define como el conjunto de actividades que desarrolla el Grupo con el objetivo de proporcionar seguridad razonable en la consecución de la eficacia y eficiencia de las operaciones, fiabilidad de la información financiera, cumplimiento de normas aplicables y salvaguarda de sus activos, por lo que forma parte íntegra de la Gestión de Riesgos Corporativos.

La Gestión de Riesgos se realiza de manera integrada, aunque cada uno de los Riesgos pueda ser atendido de manera individual, en función de la naturaleza del evento que lo origine, pero teniendo en consideración los posibles efectos en la totalidad de los objetivos del Grupo, sean éstos a corto plazo o a largo plazo. El Riesgo objeto de análisis y gestión se corresponde al Riesgo Inherente, previo a las acciones que se adopten para su gestión, es decir, antes de las acciones que se adopten para alterar o reducir su probabilidad de ocurrencia y/o impacto en los objetivos del Grupo.

A efectos de su gestión, se definen los siguientes tipos de Riesgo del Grupo Euskaltel, en función del posible origen del evento:

- Riesgos Estratégicos: aquellos que afectan a los objetivos estratégicos del Grupo recogidos en su Plan Estratégico y Plan de Negocio vigentes. Son objetivos de alto nivel que reflejan la opción elegida respecto de cómo va a crearse valor para sus Grupos de Interés. Por contraposición, el resto de las tipologías de Riesgos, (los no estratégicos), tienen su origen en la ejecución de la estrategia.

- Riesgos Financieros: por la vía de los instrumentos financieros, tienen incidencia en los resultados financieros del Grupo (tal como vienen definidos en la normativa contable). Se desglosan entre:

    - Riesgo de crédito o contraparte, asociado a que una de las partes del instrumento financiero cause una pérdida financiera a la otra parte por incumplir una obligación,
    - Riesgo de liquidez, asociado a la dificultad para cumplir con obligaciones asociadas con pasivos financieros que se liquiden mediante la entrega de efectivo u otro activo financiero, y
    - Riesgo de mercado o de flujo de efectivo, asociado a que el valor razonable o los flujos de efectivo futuros del instrumento financiero puedan fluctuar como consecuencia de cambios en los precios de mercado, del emisor del instrumento financiero o de factores que afecten a todos los instrumentos financieros de las mismas características.

- Riesgos Regulatorios: son los derivados de requerimientos y limitaciones establecidos por la legislación y regulaciones específicas que afectan a la práctica de los negocios del Grupo, e incluyen los riesgos derivados del incumplimiento de obligaciones contractuales, cualquiera que sea su naturaleza, tanto por el propio Grupo como por la contraparte (cualquiera que sea ésta: cliente, proveedor, empleado, institución financiera, etc.).

  A los efectos de la Gestión de Riesgos del Grupo, se estructuran en Riesgos penales, de Protección de Datos, Fiscales, Sectoriales, de Entidad de Interés Público y Otros Riesgos regulatorios y de cumplimiento normativo.

- Riesgos asociados a la Sostenibilidad: los vinculados a los objetivos medioambientales, sociales, éticos y de gobierno corporativo que tiene establecidos el Grupo.

- Ciberriesgos: los derivados de amenazas y vulnerabilidades que puedan afectar a los sistemas de control, información y comunicación del Grupo y a los servicios que ofrece a sus clientes, así como a cualquier activo que forme parte de su infraestructura. Incluye aquellos riesgos derivados del engaño a las personas para acceder a los sistemas que operan y, en su caso, la falta de diligencia por su parte. Su gestión se estructura en base a cuatro tipologías:

    - Ciberriesgos asociados a la Red / Servicios, derivados de amenazas y vulnerabilidades que puedan afectar a los sistemas de control y comunicación del Grupo, con incidencia en los servicios de telecomunicaciones que presta a sus clientes,

- Ciberriesgos asociados a los sistemas / procesos, donde la posible afección son los sistemas de control e información del Grupo, con incidencia en sus procesos,
- Ciberriesgos asociados a los servicios digitales, donde la incidencia de las posibles afecciones son los servicios digitales que el Grupo presta a sus clientes, y
- Riesgos de Contingencias y Continuidad de Negocio: los derivados de eventuales situaciones de desastre, con afección muy grave sobre servicios y procesos.

- Riesgos Operativos u Operacionales: aquellos que afectan a la eficacia y eficiencia de los procesos operativos y a la prestación de los servicios (excluidos los ciberriesgos) y a la satisfacción de los clientes.

  Estos Riesgos se estructuran en Riesgos de suministros básicos (contenidos de TV y tráfico de otros operadores), Tecnológicos (de Red y Sistemas), de dependencia de terceros, de Recursos Humanos, y otros.

- Riesgos Reputacionales: aquellos que pueden impactar de manera negativa en el valor de la Sociedad, resultado de comportamientos por parte del Grupo por debajo de las expectativas creadas en los distintos grupos de interés, incluyendo los comportamientos o conductas relacionadas con la corrupción.

- Riesgos de Información, asociados al objetivo de disponer y facilitar al destinatario datos e información segura, completa, elaborada de acuerdo con la normativa aplicable, en su caso, adecuada a la finalidad que se pretende con ella, y para que sirva de apoyo a la toma de decisiones y al seguimiento de las actividades y rendimientos del Grupo.

  Estos Riesgos se desglosan en Riesgos de la Información Financiera Oficial, Riesgos de la Información No Financiera Oficial y Riesgos de la Información Operativa (no oficial).

El Riesgo de fraude, en sus distintas acepciones, se incluye en la gestión de cada uno de los tipos de Riesgo.

Principios Generales de Actuación

Los Principios Generales de actuación en el marco de la Política Corporativa de Riesgos del Grupo son los siguientes:

- Cumplimiento de la legalidad, de la normativa interna y de las relaciones contractuales

  La Gestión de Riesgos se desarrolla con estricto cumplimiento de la legalidad vigente, de la normativa interna que el Grupo haya establecido voluntariamente, de las obligaciones contractuales asumidas con terceros, y de las resoluciones administrativas y judiciales firmes, rechazando expresamente cualquier conducta deshonesta o fraudulenta, y cualquier acto dirigido contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes de telecomunicaciones y de los datos informáticos, así como el abuso en la utilización de dichos sistemas, redes y datos.

En todo momento se deben cumplir las normas del Sistema de Gobierno Corporativo y los procedimientos que regulan la actividad del Grupo, evitando conductas que contravengan los valores, principios y comportamientos éticos establecidos en el Código Ético y sus Instrucciones de Conducta., bajo el principio de "tolerancia cero" hacia la comisión de actos ilícitos y situaciones de fraude.

- Organización y segregación de funciones

  La estructura organizativa del Grupo debe ser eficaz y adecuada para la aplicación del Sistema de Gestión de Riesgos y Control Interno, incluyendo las políticas y procedimientos necesarios, y garantiza una suficiente segregación de funciones operativas entre los tomadores de los riesgos y los responsables de su análisis, control y supervisión.

- Transparencia

  La Gestión de Riesgos y el Control Interno del Grupo garantiza información fiable a todos sus grupos de interés sobre los riesgos inherentes del Grupo y los sistemas desarrollados para su prevención y mitigación.

  El Control y la información relevante sobre los Riesgos y el funcionamiento del Sistema de Gestión de Riesgos y Control Interno debe ser tratada de manera transparente dentro del Sistema de Gestión de Riesgos entre los tomadores de los riesgos y los responsables de su análisis, control y supervisión.

- Continuidad

  La Gestión de Riesgos y el Control Interno del Grupo se desarrolla de manera continua en el tiempo, y se diseña y actualiza regularmente para garantizar en lo posible, y permitir, la identificación preventiva de los riesgos y la adopción de medidas mitigadoras en su gestión.

- Supervisión

  El Sistema de Gestión de Riesgos y Control Interno del Grupo incorpora y ejecuta suficientes medidas de supervisión y seguimiento de los riesgos que evidencien el cumplimiento de la presente Política Corporativa de Riesgos.

Sistema de Gestión de Riesgos

El Sistema de Gestión de Riesgos del Grupo se fundamenta en estándares internacionales reconocidos (Marco COSO y Normas ISO), desarrollando un proceso continuo e iterativo con cuatro principales fases:

1. Identificación de Riesgos de forma continuada
2. Análisis y evaluación
3. Tratamiento
4. Supervisión y revisión del Sistema

Las principales herramientas del Sistema de Gestión de Riesgos, que se aplican en función de la valoración del riesgo, se estructuran con arreglo al siguiente esquema:

- Normas internas, incluida la presente Política Corporativa, otras políticas adicionales que la desarrollan y los procesos de elaboración del Mapa de Riesgos del Grupo, que incluyen todos los tipos de riesgo definidos,

- Información y Reporting, donde se incluyen el Plan Estratégico, el Plan de Negocio, los Cuadros de Mando, los Informes Oficiales y las reuniones periódicas de los Órganos de Control y Supervisión de Riesgos,

- Gestión específica de los Riesgos, que incluye la gestión automatizada de Riesgos a través de herramientas informáticas, Mapas de Riesgos y controles específicos, y escalado de actuación en función de las operaciones o tipologías de riesgo,

- Intervención de terceros especialistas, que prestan servicios de aseguramiento en materia de gestión de Riesgos.

Roles y Responsabilidades

Todos los integrantes del grupo son responsables de que el Sistema de Gestión de Riesgos funcione de acuerdo con la presente Política Corporativa de Riesgos, en función de los roles que desempeñan en la organización. Específicamente destacan, entre otras, las siguientes responsabilidades:

- Consejo de Administración: aprueba las políticas y estrategias generales del Grupo y, en particular, la política de control y gestión de riesgos, incluidos los fiscales, así como realiza el seguimiento periódico de los sistemas internos de información y control. Adicionalmente, aprueba operaciones concretas cuando por su cuantía o características, tienen especial riesgo.

- Comisión de Auditoría y Control: supervisa, dentro de sus competencias básicas sobre sistemas de información y gestión de riesgos, la eficacia del control interno del Grupo, así como sus sistemas de gestión de riesgos y evalúa, periódicamente, los sistemas de control interno y gestión de riesgos, para que los principales riesgos se identifiquen, gestionen y den a conocer adecuadamente.

  En relación con la política y la gestión de riesgos, identifica los distintos tipos de riesgo a los que se enfrenta el Grupo incluyendo los pasivos contingentes y otros riesgos fuera de balance; determina un modelo de control y gestión de riesgos basado en diferentes niveles, identifica los niveles de riesgo que el Grupo considera aceptables y las medidas previstas para mitigar el impacto de los riesgos identificados, en caso de que llegaran a materializarse, así como los sistemas de información y control interno que se utilizan para controlar y gestionar los citados riesgos.

- Alta Dirección: asegura el buen funcionamiento del Sistema de Gestión de Riesgos y Control Interno, garantizando que todos los riesgos relevantes que afectan al Grupo se identifican, gestionan, cuantifican e informan adecuadamente. Supervisa y coordina el trabajo de los Gestores de Riesgos de su Área de responsabilidad, identifica eventos en el ámbito de su responsabilidad, informa al Área de coordinación de riesgos y a Auditoría Interna, y valida, impulsa y realiza un seguimiento de los planes de acción y de trabajo derivados del proceso de gestión de riesgos.

- Gestores (o propietarios) de los Riesgos: definen y ejecutan los planes de acción, velan por la eficiencia y eficacia de las medidas adoptadas, informan periódicamente sobre sus actuaciones e identifican posibles eventos en el ámbito de su responsabilidad.

- Auditoría Interna del Grupo vela por el buen funcionamiento de los sistemas de información y control internos, contribuyendo a la mejora de los procesos de gestión de riesgos, control y gobierno, garantizando a la Comisión de Auditoría y Control del Grupo la supervisión eficaz e independiente del sistema de control interno y aportando al Grupo recomendaciones que contribuyan a reducir a niveles razonables el impacto potencial de los riesgos que dificultan la consecución de sus objetivos. Así mismo, coordina y unifica la información sobre Riesgos que elaboran la Alta Dirección y los gestores de los riesgos y la información necesaria para que la Comisión de Auditoría y Control pueda desarrollar su labor de supervisión, incluido el Mapa de Riesgos Corporativo y sus actualizaciones.

  Auditoría Interna debe salvaguardar, en todo momento, su independencia frente al Sistema de Gestión de Riesgos, sin responsabilizarse de la toma de decisiones clave para su funcionamiento.

Mapa de Riesgos Corporativos

El Grupo recoge la lista de sus principales riesgos en un Mapa de Riesgos Corporativos que se elabora por integración de los Mapas de Riesgos de cada una de las tipologías definidas previamente y que se gestionan por parte de los responsables correspondientes.

Su finalidad principal es la de permitir a los Órganos de Gobierno la reevaluación periódica de los riesgos existentes, hacer un seguimiento de las medidas adoptadas para su gestión, incluida la mitigación del impacto en caso de materializarse, y establecer y actualizar, en su caso, el nivel de tolerancia para cada uno de ellos, partiendo de la información proporcionada por los integrantes del Grupo, en función de sus roles y responsabilidades. El Mapa de Riesgos sirve, así mismo, para homogeneizar y comparar riesgos de distinta naturaleza. El Mapa de Riesgos se reevaluará al menos anualmente, sin perjuicio de la actualización que fuera necesaria realizar debido a otras circunstancias.

Nivel de tolerancia al Riesgo

El Sistema de Gestión de Riesgos del Grupo Euskaltel está orientado a lograr un perfil medio de riesgo moderado, a través de una gestión prudente de los mismos. El nivel de tolerancia al riesgo del Grupo se determina en función del valor asignado a cada uno de los riesgos identificados en el Mapa de Riesgos aplicando criterios de probabilidad, impacto y velocidad de ocurrencia.

Para la determinación del impacto esperado, se atiende, al menos, a los siguientes factores:

- Necesidades de Tiempo y Recursos para su resolución,
- Impacto en el Resultado después de Impuestos,
- Afección a corto y medio plazo a la facturación,
- Repercusión mediática, definida como tiempo de exposición pública,
- Impacto en la reputación del Grupo,
- Eventual efecto sancionador por parte de las Administraciones Públicas, y
- Necesidad de implicación de los distintos niveles organizativos para su gestión.

La gestión de los riesgos atiende al principio de Materialidad o importancia relativa del valor asignado a los riesgos identificados en el Mapa de Riesgos.

Entrada en vigor

El Consejo de Administración de Euskaltel aprobó, en su sesión celebrada el 24 de mayo de 2016, la Política Corporativa de Control y Gestión de Riesgos. Con la finalidad de adoptar las novedades y tendencias en esta materia previstas en el Código de Buen Gobierno de sociedades cotizadas revisado en junio de 2020, completando así el proceso de actualización iniciado en el ejercicio 2019, la Política Corporativa de Control y Gestión de Riesgos ha sido actualizada y aprobada por el Consejo de Administración de Euskaltel en su sesión celebrada el 15 de diciembre de 2020.

* * * * * * * * *