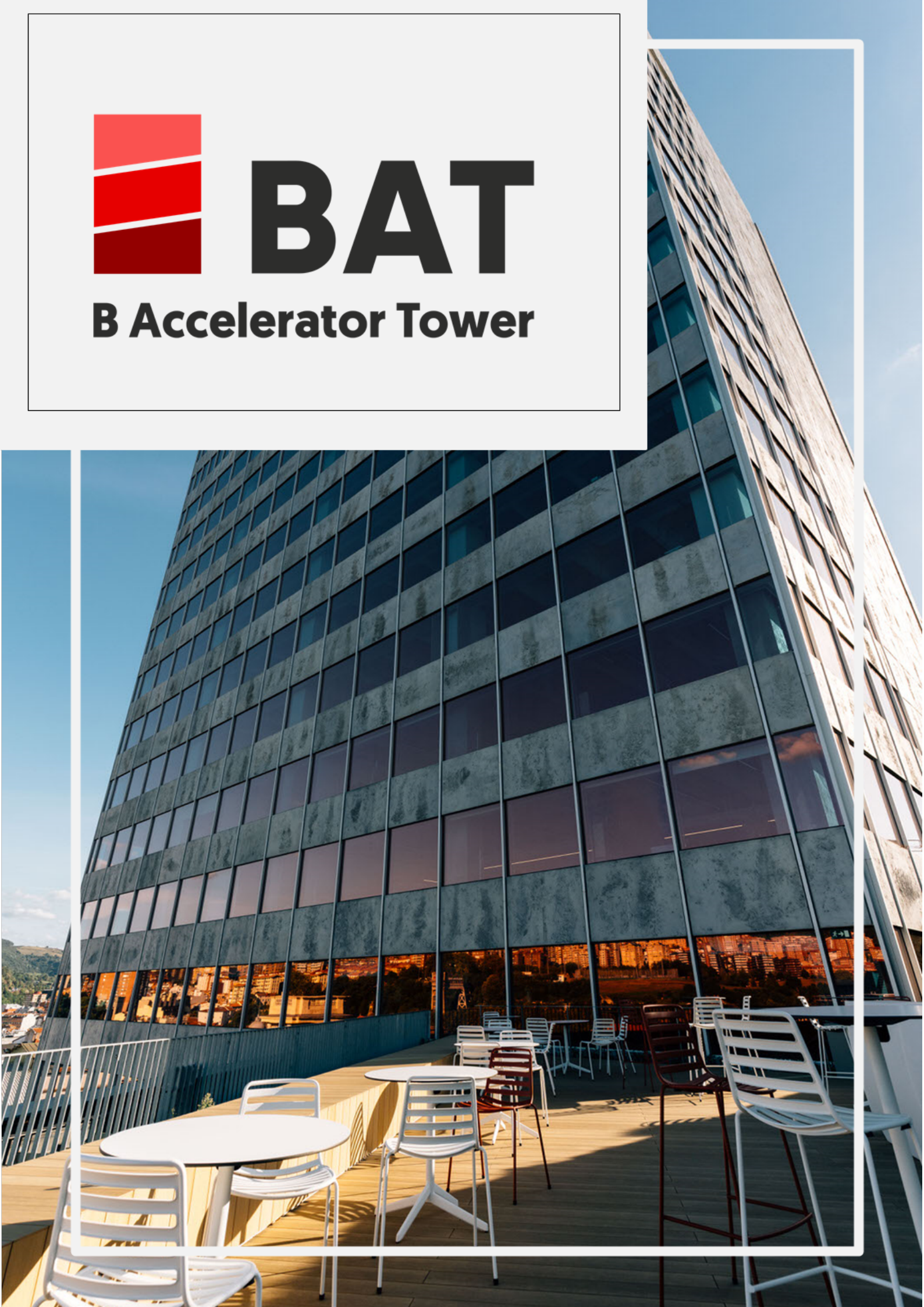
BAT

B Accelerator Tower



Iberdrola Open Innovation Challenge

Sistemas de detección y disuasión de avifauna con parada automática

1. Exposición

Iberdrola es un grupo energético global con actividad en redes eléctricas, energías renovables, almacenamiento y comercialización de energía. Su estrategia está orientada al impulso de un modelo energético más sostenible, apoyado en la innovación, la electrificación y el desarrollo de infraestructuras que contribuyan a la descarbonización de la economía.

PERSEO es el programa de innovación abierta y apoyo a start-ups de Iberdrola, creado para acercar al grupo a tecnologías y modelos de negocio con potencial estratégico para el futuro del sector energético. A través de retos tecnológicos, pilotos, pruebas de concepto, alianzas e inversiones, PERSEO facilita la colaboración entre Iberdrola y empresas emergentes que aportan soluciones tecnológicas que actúan como palanca de transformación dentro del Grupo Iberdrola.

BAT B Accelerator Tower, uno de los ecosistemas de emprendimiento e innovación mejor conectados del mundo, con un espacio colaborativo, emprendedor y de innovación único ubicado en Bilbao, Bizkaia. BAT es la punta de lanza de un proyecto que busca situar Bizkaia en el mapa internacional del emprendimiento y potenciar la competitividad de su economía, impulsando la colaboración entre las grandes empresas locales y las compañías tecnológicas más punteras (startups, scaleups, pymes innovadoras...), polos de innovación e inversores de todo el mundo.

2. Antecedentes

Iberdrola cuenta en España con una potencia eólica cercana a los 7.000 MW, en un contexto en el que la sostenibilidad y la protección de la biodiversidad se han consolidado como ejes prioritarios para el desarrollo y la operación de las instalaciones renovables. En este marco, y en línea con unos requisitos cada vez más exigentes por parte de las Declaraciones de Impacto Ambiental tanto en nuevos proyectos como en activos en operación, la compañía ha venido incorporando sistemas de detección de avifauna y parada automática de aerogeneradores cuando se identifica presencia de aves en las inmediaciones de las máquinas.

No obstante, la experiencia acumulada hasta la fecha pone de manifiesto que la eficacia de las soluciones disponibles puede variar de forma significativa entre tecnologías, lo que, unido al elevado coste de los equipos y a sus necesidades de mantenimiento, condiciona la viabilidad de su despliegue a gran escala. En la actualidad, el mercado se apoya principalmente en soluciones basadas en cámaras en disposición estereoscópica o en combinaciones radar-cámara, mientras que otras alternativas, como los sistemas de disuasión, siguen presentando un grado de desarrollo y validación limitado, con una oferta todavía poco madura para responder de forma robusta a las necesidades operativas del sector.

3. Resumen del reto

A través del presente reto, Iberdrola busca identificar soluciones tecnológicas capaces de mejorar la protección de la avifauna en entornos eólicos, combinando eficacia operativa, viabilidad económica y facilidad de integración en sus instalaciones. El objetivo es avanzar hacia sistemas autónomos y escalables que permitan detectar aves en las proximidades de los aerogeneradores, determinar su posición y trayectoria en tiempo real y, cuando exista riesgo de colisión, activar con la antelación necesaria la orden de parada controlada del aerogenerador a través de la UCC (Unidad de Control) del parque eólico.

Junto a esta primera línea de trabajo, el reto contempla también la identificación de sistemas de disuasión capaces de modificar la trayectoria de riesgo de las aves sin necesidad de detener los aerogeneradores, siempre desde un enfoque respetuoso con la biodiversidad y compatible con la operativa del parque.

En este sentido, se admitirán tanto propuestas centradas en uno solo de los ámbitos descritos como soluciones integradas que combinen detección y disuasión en un mismo planteamiento tecnológico.

4. Descripción del reto

Para la valoración de las propuestas, se plantean un conjunto de condicionantes previos que se deberán cumplir, los cuáles son el resultado de la experiencia adquirida trabajando con sistemas de avifauna durante los últimos años, así como la propia operativa del negocio eólico.

- El sistema debe ser “low-cost” respecto a lo existente en el mercado y el mantenimiento anual debe ser, asimismo, económico.
- Debe ser 3D, posicionando en todo momento las aves en el espacio.
- Sistema fácilmente calibrable y configurable en campo.
- Dispondrá de visor en las propias instalaciones con posibilidad de visualizar trayectorias.
- Incluirá una aplicación web de uso privado para almacenar las diferentes trayectorias de aves, fotografías, videos, y poder realizar tanto búsqueda como un posible análisis forense en caso de colisión de aves.
- Podrá incluir un reconocimiento de especies en base a las imágenes o videos obtenidos en el caso de sistemas basados en cámaras. El reconocimiento se llevará a cabo a nivel de especie (milano real, por ejemplo) y no a nivel de género (milano)
- Los sistemas deberán ser capaces de detectar las aves a una distancia de los aerogeneradores que permita la parada controlada de los mismos, que nunca se realizará haciendo uso del freno de emergencia.
- Las aves a detectar partirán de una envergadura alar de 0,60 metros hasta 2,50 metros aproximadamente. En caso de no llegar a detectar 0,60 metros se indicarán los límites de detección.
- Los equipos estarán diseñados para estar colocados permanentemente a la intemperie.
- Se incluirá la conexión a las instalaciones de Iberdrola. Todas las señales cumplirán con los protocolos de ciberseguridad de Iberdrola.
- Cualquier parada se realizará a través de la UCC de Iberdrola.

- Preferentemente los equipos se instalarán en infraestructuras existentes (por ejemplo, en torres de aerogeneradores, y nunca soldados a las mismas). Se evitarán en la medida de lo posible postes o torres exteriores porque suponen mayores rutados de cables y nuevas afecciones a propietarios de terrenos.
- Los sistemas de disuasión propuestos serán respetuosos tanto con la avifauna como con las condiciones locales de los lugares de instalación de los parques eólicos, y cumplirán con la legislación vigente.
- El sistema debe venir avalado por una calibración en paralelo, a definir por el ofertante, que permita definir el porcentaje de detección de aves a distintas distancias, la eficacia de la disuasión, así como (si aplica) el % de acierto en la detección de la especie.

Entre las propuestas a considerar será esencial contar con los siguientes atributos:

- La madurez y fiabilidad de la solución.
- Optimización de los costes de inversión y operación.
- Costes de implementación y personal necesario.
- Facilidad de implementación, uso y mínima capacitación.
- Minimización del número de paradas por avifauna
- Respeto a la avifauna.
- Cumplimiento con las normas de salud, seguridad y medio ambiente (HSE, por sus siglas en inglés).

5. Tipología de empresas candidatas

El principal objetivo buscado es identificar soluciones innovadoras en el ámbito previamente descrito y promover proyectos colaborativos entre Startup/Empresa tecnológicas y la entidad promotora del reto.

Podrán participar en el reto, cualquier persona emprendedora, startup, pyme o empresa tecnológica con una propuesta que pudiera contribuir a la resolución parcial o total del reto planteado. Para aquellas organizaciones interesadas en ofrecer su solución al reto planteado, no será necesario estar ubicadas en el territorio de Bizkaia o ser parte activa de la comunidad empresarial de BAT B Accelerator Tower.

El reto planteado está principalmente orientado a:

- Empresas legalmente constituidas (sin limitación en la antigüedad de la creación empresarial).
- Empresas de perfil innovador con soluciones basadas en desarrollos tecnológicos y capacidad de acometer proyectos de I+D para abordar las necesidades descritas.
- Empresas con producto ya en mercado o con desarrollos tecnológicos equivalentes a TRL 7 en adelante, los cuales pueden ser probados en entornos reales.
- Empresas con capacidades y solvencia para colaborar con grandes empresas.
- Empresas con capacidad para desarrollar el piloto en España

Una misma startup, pyme u organización solo podrá participar con un proyecto, ya sea de forma individual o de forma conjunta con terceros.

6. Fases, fechas e hitos principales

FASE	FECHA	HITO
Periodo de recepción de candidaturas	Desde 25/06/2026 a 21/08/2026	Apertura y Cierre de la "Call"
Evaluación de candidaturas	Desde 31/08/2026 a 11/09/2026	Evaluación interna
Anuncio de candidaturas seleccionadas	14/09/2026	Notificación a las candidaturas seleccionadas
Reuniones entre empresas seleccionadas e Iberdrola	A partir del 15/09/2026	Reuniones presenciales

7. Proceso de aplicación

El periodo de recepción de candidaturas estará abierto entre el 25/06/2026 y el 21/08/2026 a través de la web de BAT B Accelerator Tower en el apartado "Oportunidades Abiertas". Las organizaciones interesadas en participar en esta iniciativa cumplimentarán el correspondiente formulario de solicitud, anexando a su inscripción, cuanta información se le requiera o vea de interés.

- Las candidaturas deberán cumplimentarse en Castellano o inglés.
- Se evaluará una única candidatura por empresa, evaluándose la última candidatura recibida en el caso de realizar más de una aplicación.
- Una vez recibida la candidatura, un mensaje de confirmación de recepción de la candidatura será enviado automáticamente.
- El formulario de solicitud contendrá la siguiente información:
  - Información de contacto.
  - Información general de la empresa.
  - Solución propuesta.
  - URL – video explicativo de la solución propuesta (opcional)
  - Elementos de innovación (producto, proceso, marketing y organización) o resultados de I+D relacionados con la solución propuesta
  - Tecnologías asociadas a la solución propuesta (en caso de que las hubiera).
  - Equipo que participará en el desarrollo de la solución.
  - Beneficios.
  - Riesgos.
  - Colaboradores.
  - Estado de desarrollo.
  - Coste.

- Plazos.
- Otras observaciones.
- Confirmación de que la solución cumple las especificaciones de ciberseguridad de Iberdrola.

8. Proceso de selección

Con el fin de elegir los mejores proyectos, se constituirá un equipo de evaluación con personas pertenecientes a Iberdrola y BAT, que llevarán a cabo el proceso de selección.

Finalizado el plazo de presentación de las solicitudes, BAT realizará una primera revisión de calidad de las solicitudes presentadas, descartando todas aquellas que no hayan cumplimentado adecuadamente la información requerida. Las personas asignadas de Iberdrola analizarán las solicitudes presentadas y valorarán desde un punto de vista técnico cada una de ellas, hasta tener una preselección de proyectos.

El equipo de evaluación valorará los siguientes aspectos de cada una de las propuestas finalistas:

- Innovación: se valorará el grado de innovación en la solución propuesta
- Grado de construcción del proyecto: el grado de desarrollo de la solución propuesta.
- Equipo de proyecto: se valorará el equipo de la/s organización/es participante/s, su experiencia, dedicación, conocimiento de mercado, contactos, etc
- Plazos: los tiempos en que la solución pudiera estar operativa en el mercado.
- Viabilidad: la viabilidad del proyecto y el coste de la solución y su mantenimiento en un entorno real.
- Alcance del proyecto: se valorará el grado de respuesta de la solución propuesta y de qué manera aborda la problemática planteada.

El cumplimiento de los requisitos anteriores deberá acreditarse en el momento de la presentación de la candidatura mediante el formulario diseñado a tal efecto, al que podrá añadirse la documentación adicional correspondiente, aportando los anexos necesarios, con el fin de verificar el cumplimiento de los requisitos exigidos.

9. Relación entre la empresa promotora del reto y las empresas candidatas

El objetivo de Iberdrola en este proceso es identificar empresas con las que poder iniciar un proyecto piloto de máximo tres meses tras el anuncio del ganador. El pilotaje propuesto permitirá a la empresa seleccionada colaborar con Iberdrola en un parque eólico ubicado en España, con posibilidad de un contrato de seguimiento y escalado o colaboración a largo plazo en caso de éxito del piloto

Durante todo el proceso la startup/ empresa tecnológica candidata se compromete a dedicar los recursos humanos y materiales necesarios para llevar a cabo las actividades planteadas, incluyendo a las personas capacitadas para tomar decisiones sobre el desarrollo tecnológico y del negocio, así como para responder a las comunicaciones oficiales.

El representante deberá ser mayor de 18 años, ostentar un cargo “C-Level” en la empresa y ser capaz de comunicarse en idioma inglés o castellano con fluidez en todos los niveles, actuando como representante de la empresa.

Esta persona deberá cumplir las condiciones legales necesarias para residir y permanecer en España. Asimismo, el candidato deberá estar al corriente de sus obligaciones fiscales, tributarias y con la seguridad social.

Todas las notificaciones relativas al desarrollo del reto se realizarán por correo electrónico directamente al representante. Las empresas candidatas deberán proporcionar un número de teléfono para atender aquellas comunicaciones que así lo requieran.

10. Aceptación de Términos y Condiciones

Los siguientes términos y condiciones tienen por objeto establecer las normas de participación en este proceso. La participación en esta convocatoria implica la aceptación plena e incondicional de estos Términos y Condiciones sin excepción.

11. Política de confidencialidad y protección de datos

La participación en esta convocatoria es voluntaria. El contenido de las candidaturas enviadas a través del formulario de solicitud, así como toda la documentación e información de cualquier tipo que se aporte, será confidencial y privada, y será tratada como tal por la empresa promotora del reto.

Las empresas candidatas aceptan, como norma general, el uso por la empresa promotora del reto de los datos básicos del proyecto durante los procesos de evaluación y selección descritos en estos Términos y Condiciones.

La participación en el reto no otorga ningún derecho sobre la propiedad intelectual de las candidaturas por el mero hecho de participar en esta convocatoria. Las empresas candidatas deberán garantizar que el trabajo y el contenido aportados de manera voluntaria al formulario vinculado al reto (incluyendo resúmenes o presentaciones) no infringen derechos de terceros y que cuentan con todas las autorizaciones necesarias para participar en este reto.

Asimismo, dichos contenidos no deberán ser ofensivos ni vejatorios, ni incitar a la violencia o al racismo, ni vulnerar los derechos fundamentales o las libertades públicas reconocidas por la normativa vigente, incluidas las leyes de protección de la infancia y juventud.

Tampoco deberán constituir o implicar intrusiones en la intimidad personal o familiar de individuos, ni vulnerar el derecho al honor o al secreto de las comunicaciones de terceros, ni contravenir cualquier regulación vigente. Además, los proyectos presentados deberán garantizar un uso no sexista del lenguaje y las imágenes.

Por último, cada Startup/Empresa tecnológica participante autoriza a la empresa promotora del reto a utilizar su nombre e imagen en materiales de difusión relacionados con el reto, incluidos aquellos publicados en Internet, sin recibir por ello compensación alguna.

12. Derechos de propiedad intelectual

La empresa candidata garantiza que es titular de los derechos de explotación adecuados sobre los productos, servicios, patentes, modelos de utilidad y demás contenidos que formen parte de su candidatura. Las empresas participantes eximirán a la empresa promotora del reto de cualquier reclamación por infracción de derechos de terceros, incluidas las infracciones de derechos de propiedad intelectual e industrial.

El candidato participante no tendrá que otorgar ningún derecho de propiedad intelectual o industrial a la empresa promotora del reto, salvo en las excepciones indicadas en estas bases. Si la empresa candidata y la empresa promotora del reto acuerdan llevar a cabo trabajos colaborativos para diseñar o cocrear soluciones de manera conjunta, ambas partes establecerán en un documento privado y por separado los términos relativos a la propiedad intelectual e industrial y a la comercialización de la solución resultante.

13. Declaración responsable

Al presentar su candidatura, las empresas candidatas declaran y garantizan ante la empresa promotora del reto:

- Que las candidaturas presentadas son obras originales de sus autores y/o que disponen libremente de cualquier idea, imagen u otros elementos incorporados en su presentación.
- Que cuentan con el consentimiento de todos los terceros cuyos datos personales hayan sido incluidos en su candidatura.
- Que la información facilitada no contiene información confidencial propia o de terceros ni secretos industriales o, en su caso, que disponen de las autorizaciones y licencias que permiten su comunicación en el marco de esta convocatoria.
- Que disponen de plena capacidad legal y facultades para participar en la convocatoria, y que dicha participación no vulnera ninguna normativa de cualquier índole.
- Que asumirán cualquier impuesto derivado de la participación en esta convocatoria, así como de la eventual recepción de cualquiera de las aportaciones económicas previstas en el reto.
- Que la empresa promotora del reto no será responsable de los daños, pérdidas, costes y/o reclamaciones que los candidatos pudieran sufrir o en los que pudieran incurrir como consecuencia de la presentación de sus candidaturas.
- Que la solución planteada cubre los requisitos de ciberseguridad de Iberdrola (ver Anexo 1).

14. Contacto y resolución de dudas.

Ante cualquier duda, se puede contactar con el equipo de gestión de BAT B Accelerator Tower a través del siguiente mail de contacto: [info@bacceleratortower.com]

Web oficial: [BAT B Accelerator Tower website].

Anexo 1 - CIBERSEGURIDAD

Se buscará garantizar la protección de la infraestructura tecnológica, la disponibilidad de los sistemas de generación, la integridad y confidencialidad de los datos, así como el cumplimiento normativo en materia de ciberseguridad conforme a los estándares ISO 27001, IEC 62443 y la Directiva NIS2.

El Contratista deberá garantizar que todas las comunicaciones del sistema se realicen a través de protocolos seguros, evitando el uso de protocolos sin cifrado.

Todo dato en tránsito deberá ser cifrado mediante TLS 1.2 o superior, mientras que los datos en reposo deberán contar con cifrado AES-256.

El Contratista se compromete a garantizar que todos los aplicativos software desarrollados e implementados en el servicio cumplan con los principios de desarrollo seguro y hayan pasado un análisis de seguridad DAST y SAST antes de su puesta en producción.

La arquitectura deberá contemplar una segmentación adecuada de red, con la implementación de firewalls perimetrales que aseguren el aislamiento de los distintos componentes del sistema, incluyendo infraestructura de procesamiento y almacenamiento de datos, así como su integración con los sistemas de control.

La infraestructura de seguridad deberá incluir firewalls de nueva generación con capacidades IDS/IPS, aprobados por los responsables de Comunicaciones del CORE y Ciberseguridad del negocio, tales como Palo Alto u otras soluciones equivalentes que permitan la detección y bloqueo de amenazas en tiempo real.

El Contratista deberá establecer políticas de gestión de identidades y accesos que apliquen el principio de mínimo privilegio, asegurando que cada usuario cuente solo con los permisos estrictamente necesarios para su función.

Todas las conexiones remotas para la administración de sistemas o equipos que presten servicio a El Cliente o interactúen con su infraestructura deberán realizarse mediante mecanismos que incorporen autenticación multifactor.

Las conexiones remotas deberán realizarse exclusivamente a través de redes privadas virtuales (VPN) que cumplan con los estándares de seguridad definidos por la organización. Este requisito aplica tanto a accesos puntuales como a conexiones continuas de monitorización.

Todos los dispositivos destinados al acceso a la red, incluyendo, entre otros, routers 4G/5G, deberán ser propiedad exclusiva de El Cliente, quien mantendrá en todo momento control y capacidad plena de gobierno, administración y configuración sobre los mismos. Queda prohibida la utilización de equipos que no estén bajo dicho control directo.

Se prohíbe la exposición de routers con direcciones IP públicas, debiendo garantizarse la aplicación de mecanismos de filtrado de tráfico para restringir accesos no autorizados.

El Contratista deberá garantizar que todos los dispositivos utilizados en el servicio, incluyendo routers y servidores, cuenten con medidas de protección adecuadas.

La seguridad física de los dispositivos deberá gestionarse adecuadamente con armarios con cerradura o elementos de protección similares, para restringir el acceso a los equipos solo al personal autorizado.

Se deberá garantizar que todos los servidores y dispositivos de comunicación utilizados para prestar el servicio cuenten con configuraciones de bastionado (hardening) conforme a las mejores prácticas de la industria y estándares como CIS.

Se deberá implementar un plan de mantenimiento preventivo que contemple la actualización periódica del firmware y software, y la verificación del estado de los dispositivos en operación.

El Contratista podrá visualizar y consumir los datos generados por el sistema una vez sean almacenados en una infraestructura segura y propiedad de El Cliente, ya sea en entornos cloud previamente autorizados (como AWS, GitHub o plataformas privadas de El Cliente) o en instalaciones locales bajo control estricto.

Deberá implementarse una política de clasificación y retención de datos que contemple la confidencialidad de la información generada por el sistema, especialmente aquellos registros cuya exposición pública podría implicar un impacto para El Cliente. En este sentido, se deberá evaluar la necesidad de anonimización de los datos antes de su tratamiento o almacenamiento.

La infraestructura de procesamiento deberá incorporar mecanismos de supervisión para detectar alteraciones en la información (parametrización de umbrales) capturada por el sistema, evitando así falsos positivos derivados de ataques externos.

El sistema deberá contar con capacidades de registro y auditoría, asegurando que todas las conexiones, accesos y eventos críticos queden documentados en el sistema con una retención mínima de seis meses.

El Contratista deberá contar con un plan de respuesta a incidentes que contemple procedimientos específicos para la gestión de ataques cibernéticos dirigidos contra la infraestructura del servicio. Dicho plan deberá incluir mecanismos de notificación inmediata al equipo de ciberseguridad de Iberdrola IESE (ciberseguridad_iese_ren@iberdrola.es) y al equipo de respuesta a incidentes (srv-icsirt@iberdrola.es).

El Contratista deberá garantizar que todos los terceros y subcontratistas involucrados en el suministro, mantenimiento o soporte del sistema cumplan con los mismos controles de seguridad comprometidos por el Contratista.

El Cliente podrá solicitar evidencias que acrediten la aplicación de medidas de seguridad mediante auditorías externas o ejercicios de pentest.

Todo contrato con terceros deberá incluir cláusulas específicas de ciberseguridad que contemplen la adopción de buenas prácticas en la gestión de accesos, protección de datos y notificación de incidentes.

Se cumplirá con todos los requisitos de Ciberseguridad anexos a esta especificación técnica.

Cualquier desviación respecto a los requisitos indicados deberá ser aprobada por escrito por El Cliente y durante un plazo temporal definido por El Cliente en dicha comunicación.