POLÍTICA DE CIBERSEGURIDAD

El Consejo de Administración de Sacyr, S.A. ("**Sacyr**"), en el marco de su competencia general e indelegable de determinar las políticas y estrategias generales de la sociedad, y previa revisión y propuesta por parte de la Comisión competente, ha aprobado la presente *Política de Ciberseguridad* (en adelante, la "**Política**").

El objetivo de esta Política, dirigida a todos los grupos de interés, es definir y establecer los principios, criterios y objetivos que rigen las actuaciones en materia de ciberseguridad.

1. Finalidad

Sacyr y su grupo de sociedades ("**Grupo Sacyr**") asumen la ciberseguridad asociada a sus servicios como uno de los factores clave en la realización de sus actividades que aseguren en Sacyr la salvaguarda de la confidencialidad, la integridad, la disponibilidad, la trazabilidad, la autenticidad y privacidad de la información y de los activos tecnológicos que la soportan, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad.

Asimismo, estos principios deberán estar alineados con los requerimientos normativos y regulatorios vigentes y prevenir los impactos relativos, entre otros, a:

- la imagen y reputación de Sacyr,
- interrupción de los procesos críticos que soportan el negocio,
- uso indebido de los activos de información,
- pérdida o exfiltración de datos.

Forma parte de la estratégica del Grupo Sacyr la implantación y el desarrollo de un Sistema de Gestion de Ciberseguridad basado en normativas y mejores prácticas nacionales e internacionales y sustentado en las capacidades de identificación, protección, detección, respuesta y recuperación de los sistemas de información, aportando para ello la Alta Dirección, los recursos necesarios para su consecución.

Sacyr entiende que esta finalidad debe nacer desde el interior del equipo humano que integra Sacyr, como seña de identidad, por lo que anima a todas estas personas a incorporarlo en su forma de trabajo, y hacerlo extensivo a todas sus partes interesadas.

2. Ámbito de aplicación

Esta política de ciberseguridad es de aplicación a todas las entidades pertenecientes al Grupo Sacyr, atendiendo a sus características propias. A efectos del presente documento, el Grupo Sacyr se considera integrado por (i) todas las sociedades filiales o participadas mayoritariamente respecto de las que, de forma directa o indirecta, se ejerza un control efectivo por parte de Sacyr, S.A. independientemente de su localización geográfica, (ii) así como por la Fundación Sacyr. Por lo tanto, en todas las referencias que esta *Política* haga al Grupo Sacyr, se entenderán incluidas todas las sociedades detalladas anteriormente y la Fundación.

No están incluidas en su ámbito de aplicación las sociedades filiales o participadas minoritariamente respecto de las que no se ejerza, ni de forma directa ni indirecta, un control efectivo por parte de Sacyr, S.A, que dispondrán, en su caso, de sus propias políticas o normativa interna que regule la materia, no pudiendo en ningún caso, éstas ser contrarias a lo establecido en la presente *Política*.

3. Principios Generales

Mediante esta *Política*, Sacyr y las demás sociedades del Grupo asumen y promueven los siguientes principios generales que deben guiar todas sus actividades:

I. Proteger la información soportada sobre los sistemas de información de Sacyr.
II. Garantizar que los activos de las sociedades del Grupo poseen un nivel de ciberseguridad y ciber-resiliencia adecuados y aplicar los estándares más avanzados en aquellos que soporten la operación de infraestructuras críticas.
III. Dotar de procedimientos y herramientas que permitan adaptarse con agilidad a las condiciones cambiantes del entorno tecnológico y a las nuevas amenazas que surjan.
IV. Sensibilizar a todos los empleados, proveedores y otras partes interesadas acerca de los riesgos de ciberseguridad, promoviendo una cultura de la ciberseguridad mediante acciones de formación y concienciación. Así mismo, se garantizará que el personal implicado en las tareas relativas a la ciberseguridad dispondrá de los conocimientos, experiencia y capacidades tecnológicas necesarias para cumplir con los objetivos de ciberseguridad de Sacyr.
V. Requerir la existencia de mecanismos de ciberseguridad y resiliencia adecuados para los sistemas de información de terceros que presten servicios al Grupo.
VI. Tener en cuenta criterios de eficiencia y sostenibilidad en la implementación de las medidas de ciberseguridad aplicables.

VII. Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las amenazas de ciberterrorismo y ciberdelincuencia, para evitar que éstas lleguen a impactar a Sacyr, o en caso de que lo hagan, se puedan minimizar sus efectos sobre el negocio.

VIII. Colaborar con los organismos y agencias gubernamentales relevantes para contribuir a la mejora de la ciberseguridad en el ámbito nacional e internacional.

IX. Actuar de acuerdo con la legislación vigente, el Código ético y demás normativa interna de la Sociedad.

X. Mantener y promover desde la Alta Dirección de la organización los principios de la presente política.

Esta *Política de Seguridad de ciberseguridad* fue aprobada por el Consejo de Administración el día 18 de diciembre de 2023.