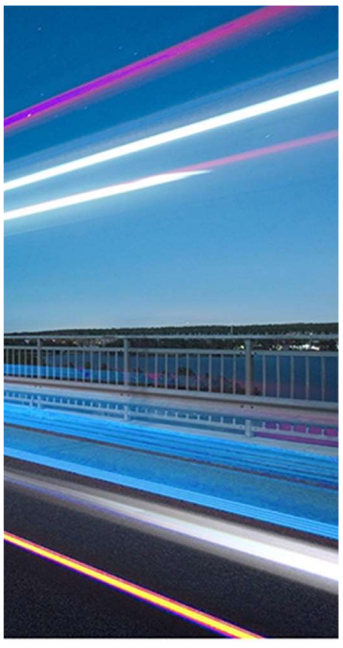
POLÍTICA DE CIBERSEGURIDAD

TRANSPORT SYSTEMS
TRAINS
BUSES
SIGNALLING
COMPONENTS
SERVICES

Your Way
to Future Mobility

ÍNDICE



1. INTRODUCCIÓN Y OBJETO

El Consejo de Administración de CONSTRUCCIONES Y AUXILIAR DE FERROCARRILES, S.A., en el ejercicio de sus funciones indelegables de definición de las estrategias generales de la Sociedad y su Grupo (en adelante **"CAF"** o "Grupo") y teniendo en cuenta los desarrollos normativos impulsados desde la Unión Europea y su proyección en nuestro país, así como las recomendaciones, prácticas y estándares establecidos por las autoridades de supervisión y organismos de reconocido prestigio, ha aprobado en su sesión de 10 de octubre de 2024, la presente Política de Ciberseguridad (la "Política") en la que se establecen los principios y compromisos básicos en materia de seguridad de la información y la ciberseguridad.

De conformidad con lo previsto con carácter general en el Código de Conducta del Grupo y teniendo en cuenta lo dispuesto en la Política de Sostenibilidad y en la Política General de Control y Gestión de Riesgos, los principios básicos establecidos en la presente Política permitirán al Grupo desplegar las estrategias, procedimientos y estándares de Ciberseguridad, alineados con los objetivos de negocio, para la protección de los datos, sistemas y operaciones de CAF. Además, la Política persigue desplegar procesos y tecnologías que permitan al Grupo ofrecer productos y servicios de confianza para los usuarios, los clientes y otros grupos de interés.

2. ALCANCE

La presente Política es de aplicación y obligado cumplimiento para todas las entidades que componen CAF.

Esta Política se aplica a todos los trabajadores, accionistas, directivos o miembros de un órgano de administración de alguna entidad de CAF, independientemente del cargo que ocupen o de su ubicación geográfica.

Así mismo, la presente Política es aplicable a los terceros de la cadena de valor con quien CAF tenga establecido algún tipo de relación comercial (Socios de Negocio) y en especial a los socios de proyecto, agentes, proveedores y clientes.

Para definir las exigencias concretas a las diferentes tipologías de Socios de Negocio se tendrán en cuenta factores objetivos tales como si CAF dispone del control operacional o si tiene una capacidad decisiva de influencia en el tercero, o criterios análogos reconocidos en las principales guías de buenas prácticas a nivel internacional. En el caso de que CAF no asuma dicho control operacional o carezca de influencia significativa, se adoptarán medidas razonables y proporcionales al riesgo, como por ejemplo y entre otras, el análisis de las políticas equivalentes del Socio de Negocio en la materia de la presente Política, para garantizar su compatibilidad y alineamiento con ésta, o cualesquiera otras que puedan ser efectivas para asegurar el respeto por los terceros de los Principios Generales del Código de Conducta de CAF, con carácter general, y el contenido del Código de Conducta de Proveedores, para estos últimos.

Respecto a las sociedades participadas que no pertenezcan a CAF por no disponer de una participación suficiente que asegure el control, se promoverá que sus principios de actuación sean coherentes con lo establecido en esta Política, respetando siempre la legislación aplicable en cada caso.

3. PRINCIPIOS BÁSICOS Y COMPROMISOS EN MATERIA DE CIBERSEGURIDAD

Parar lograr la puesta en marcha de los compromisos, CAF se guiará por los principios básicos de la seguridad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, que presiden la presente Política sobre Ciberseguridad.

En este sentido:

- La confidencialidad garantiza que la información solo sea accesible para los usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización.
- La integridad asegura que los datos se mantengan libres de modificaciones no autorizadas y que la información existente no haya sido alterada por personas o procesos no autorizados.
- La disponibilidad garantiza que la información y los sistemas de información estén accesibles y utilizables cuando los usuarios autorizados lo requieran.
- La autenticidad es la capacidad de garantizar que el origen y las identidades asociadas a la información sean realmente los que aparecen en los atributos de ésta. Ello va unido al principio de no repudio, que asegura que el usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos.
- La trazabilidad garantiza la posibilidad de determinar en cada momento la identidad de las personas que acceden a la información y la actividad que desarrollan en relación con la misma, así como los distintos estados y rutas que ha seguido la información.

Sobre estas bases, la presente Política responde a los siguientes compromisos:

Compromiso 1: Impulsar y mejorar continuamente la gestión de la ciberseguridad, de forma que nos permita cumplir con las obligaciones legales y contractuales incorporando asimismo buenas prácticas de seguridad y el uso ético de los recursos de la organización, satisfaciendo las necesidades y expectativas de nuestros clientes y demás grupos de interés.

Se entiende por gestión de la ciberseguridad el conjunto de actividades, controles y medidas técnicas y organizativas para una gestión efectiva de los riesgos de ciberseguridad, que garanticen la seguridad integral de los sistemas de información, las redes y la información almacenada en dichos sistemas, incluyendo la prevención, detección, respuesta y recuperación ante incidentes.

El presente compromiso se extiende al cumplimiento, tanto de las obligaciones legales y contractuales, como de las mejores prácticas de seguridad y al uso ético de los recursos de la organización, satisfaciendo las necesidades y expectativas de los clientes y demás grupos de interés.

El modelo de gestión de la ciberseguridad en CAF se basa en referentes y estándares reconocidos, y en las regulaciones y normativas nacionales e internacionales. Esto permite tanto el despliegue de controles y medidas, como una gestión de riesgos adecuada a cada ámbito, teniendo en cuenta el entorno y amenazas actuales, y las que surjan en el desarrollo de los negocios y como resultado de nuevas exigencias normativas.

En todo caso se llevará a cabo una continua supervisión y monitorización que garantice la eficacia y mejora continua del modelo.

Compromiso 2: Promocionar una cultura de ciberseguridad entre nuestras personas y colaboradores externos, implicándolos en la consecución de los objetivos.

Una cultura de ciberseguridad para las personas implica:

El establecimiento, despliegue, mantenimiento y comunicación de las políticas, normas y procedimientos de ciberseguridad que son fundamentales para definir los principios, objetivos y responsabilidades en esta materia.

Estos elementos proporcionan directrices claras para el uso de la tecnología, la gestión de datos y la respuesta ante incidentes, promoviendo así la integración de la ciberseguridad en todos los ámbitos de la organización y estableciendo la ciberseguridad por diseño, tal y como se definirá más adelante, como base de nuestras actividades. Además, es esencial definir planes de formación que capaciten a toda la organización en ciberseguridad, adaptándolos a sus áreas de actividad y responsabilidad. Para complementar esto, la concienciación en materia de ciberseguridad es crucial, implicando la educación y sensibilización de todas las personas de la organización sobre los riesgos de ciberseguridad, las amenazas actuales y las mejores prácticas para prevenir incidentes.

Por otro lado, supervisar el cumplimiento de las buenas prácticas requiere establecer acuerdos claros sobre los estándares de seguridad esperados, realizar evaluaciones periódicas de los controles implementados y monitorizar continuamente el desempeño en ciberseguridad. En este contexto, es fundamental mantener una comunicación fluida y transparente con los Socios de Negocio para abordar cualquier vulnerabilidad o incidente de seguridad de manera rápida y eficiente. Integrar todos estos componentes asegura una ciberseguridad robusta y efectiva, protegiendo a la organización de posibles amenazas y garantizando la continuidad de sus operaciones.

Compromiso 3: Velar por la protección de las personas frente a accidentes e incidentes originados o relacionados con nuestros productos y servicios.

Se establece la obligación de proteger a las personas de cualquier daño o incidente relacionado con nuestros productos y servicios digitales. Esto implica establecer la ciberseguridad por diseño, es decir, diseñar, desarrollar y suministrar productos y servicios con medidas de seguridad robustas, alineadas con las necesidades de los clientes, normativas y amenazas existentes, e integrando la ciberseguridad en todo el ciclo de vida de los desarrollos. El objetivo no es otro que identificar y corregir las vulnerabilidades durante todo el proceso. Adicionalmente, CAF extiende la gestión de vulnerabilidades y la monitorización de incidentes a las fases de operación y mantenimiento, protegiendo a las personas y reduciendo los riesgos asociados a los posibles incidentes.

Compromiso 4: Adoptar un criterio de tolerancia cero frente a las acciones o actitudes que vayan en detrimento de la ciberseguridad y, en caso de conflicto entre intereses contrapuestos, dar prioridad a la seguridad.

Se establece una política de tolerancia cero ante cualquier acción o actitud que pueda comprometer la Ciberseguridad de los sistemas y datos. Esto implica mitigar y gestionar los riesgos, aplicar de medidas correctivas inmediatas ante cualquier incumplimiento, y priorizar la seguridad en todas las decisiones y asignación de recursos. En caso de conflicto entre la seguridad y otros intereses, como la funcionalidad o la eficiencia, la seguridad siempre deberá prevalecer. Este enfoque requiere un liderazgo comprometido, comunicación clara, formación continua y evaluación constante para garantizar un entorno digital seguro y protegido.

Compromiso 5: Proteger los datos de toda índole relativos a CAF y a sus grupos de interés, en materia de propiedad intelectual, industrial, secretos comerciales, de carácter personal u otros ámbitos.

Se establece la salvaguarda integral de los datos que conciernen a CAF y a sus grupos de interés. Esto abarca la protección rigurosa de la propiedad intelectual, industrial, los secretos comerciales y los datos de carácter personal, entre otros ámbitos sensibles. La implementación de medidas de seguridad robustas, como el cifrado, el control de acceso y la formación del personal, resulta esencial para prevenir el acceso no autorizado, la divulgación o el uso indebido de esta información. De igual modo, es necesario implantar medidas que abarquen la seguridad física y del entorno de los sistemas de información y redes, tendentes a la protección de dichos sistemas frente a fallos inesperados del sistema, errores humanos, actos malintencionados o fenómenos naturales para garantizar la continuidad de las actividades.

Al proteger estos activos intangibles, CAF no solo preserva su ventaja competitiva y su reputación, sino que también cumple con sus responsabilidades legales y éticas para con sus distintos grupos de interés. Además, implica establecer canales de comunicación claros para que los usuarios puedan reportar incidentes y recibir asistencia, así como contar con planes de respuesta a incidentes para mitigar cualquier impacto negativo en la seguridad y privacidad de los usuarios.

Compromiso 6: Promover la Ciberseguridad en toda la cadena de valor.

Se fomenta activamente la ciberseguridad en todos los niveles de la cadena de valor, promoviendo la implementación y cumplimiento de estándares globales de ciberseguridad y de seguridad de la información y protección de datos entre proveedores, subcontratistas y clientes. Se establecen alianzas estratégicas con actores comprometidos con la ciberseguridad, promoviendo prácticas responsables que minimicen el riesgo de incidentes y protejan la integridad de los sistemas y datos.

4. MÉTRICAS Y OBJETIVOS

Para garantizar el cumplimiento de los principios y compromisos establecidos en la Política de Ciberseguridad, CAF ha definido un robusto sistema de monitorización y control basado en indicadores de rendimiento y objetivos claramente definidos a corto, medio y largo plazo.

El seguimiento periódico de los indicadores de rendimiento permite evaluar el progreso hacia el logro de los objetivos a corto, medio y largo plazo que han sido previamente definidos. Esta práctica facilita la identificación de áreas que requieren atención y mejora, posibilitando la correcta toma de decisiones y la implementación de medidas correctivas adecuadas. De esta manera, se asegura un ciclo continuo de mejora continua, y se optimiza el rendimiento y la eficiencia en todos los niveles de la organización.

Para garantizar su eficacia, los indicadores de rendimiento deben ajustarse a los siguientes criterios:

- Relevancia: Los indicadores deben medir y reflejar de manera precisa y significativa el progreso hacia el logro de un objetivo específico, proporcionando información que pueda ser utilizada para la toma de decisiones y acciones.
- Representación fiel: Las fuentes de los datos deben ser confiables, y los métodos de medición deben ser estandarizados. La información presentada a través de los indicadores debe ser completa, neutral y precisa.
- Oportunidad: La frecuencia de medición de los indicadores debe ser adecuada para la oportuna toma de decisiones.
- Facilidad de uso: Deben ser fácilmente comprensibles e interpretables tanto para quienes los recopilan como para quienes se encargan de su análisis.
- Comunicación efectiva: Los resultados de los indicadores deben ser comunicados de forma clara y concisa a todos los niveles de la organización.

Los indicadores más relevantes formarán parte del reporte de información no financiera de conformidad con las mejores prácticas de sostenibilidad asumidas por el Grupo.

El propósito que se persigue con este enfoque es que el buen gobierno corporativo, la ética y la sostenibilidad sean ejes transversales en la toma de decisiones a todos los niveles de CAF y en especial en la gestión de los riesgos, con el fin de que sus actividades generen valor tanto para sus accionistas como para sus restantes grupos de interés.

5. GOBERNANZA Y SUPERVISIÓN EN MATERIA DE CIBERSEGURIDAD

La gobernanza de CAF en materia de seguridad de la información y, en particular, sobre ciberseguridad, se estructura a través de los siguientes niveles:

a) Consejo de Administración

El Consejo de Administración fija las bases de la gobernanza interna del Grupo sobre ciberseguridad mediante la definición de los objetivos estratégicos en esta materia, y en particular mediante las competencias siguientes:

- Aprobar esta Política de ámbito corporativo.
- Llevar a cabo un seguimiento regular de la ciberseguridad en la organización.

- Fomentar, junto con la dirección, una cultura de ciberseguridad en toda la organización, con el objetivo de concienciar sobre las prácticas recomendables para prevenir y mitigar riesgos en el ámbito de la ciberseguridad.
- Atribuir a la Comisión de Auditoría la supervisión directa en materia de ciberseguridad.
- Asegurar la disponibilidad de las capacidades y recursos, materiales y humanos, necesarios para la consecución de los objetivos de la Función de Ciberseguridad.
- Actualizar, a instancias de la Comisión de Auditoría, la presente Política, de conformidad con lo previsto en el apartado 7 de la misma.

b) Comisión de Auditoría

La Comisión de Auditoría tiene atribuidas las facultades de supervisión y evaluación de los sistemas de gestión y control de los riesgos financieros y no financieros del Grupo, incluidos los tecnológicos.

Asimismo, corresponden a la Comisión de Auditoría las siguientes competencias.

- Supervisar la aplicación de la presente Política, así como la Función de Ciberseguridad.
- Recabar regular y periódicamente del Responsable Corporativo de la Función de Ciberseguridad, informes sobre la gestión de la misma, como mínimo una vez al año.

  Dichos informes contendrán, al menos, el estado de la ciberseguridad y los incidentes significativos gestionados, si los hubiera.
- Proponer al Consejo la actualización de la presente Política, de conformidad con lo previsto en el apartado 7 de la misma.

c) Director de Tecnología Corporativo

El Director de Tecnología Corporativo:

- Fijará las directrices en materia de Tecnología del Grupo y, en particular, para la gestión de la ciberseguridad, coordinando esta Función con los restantes ámbitos tecnológicos del Grupo.
- Recibirá el reporte directo del Responsable Corporativo de la Función de Ciberseguridad sobre el cumplimiento de los objetivos estratégicos y de los indicadores clave de desempeño (KPI) definidos a nivel corporativo.
- Facilitará la involucración de la alta dirección en materia de ciberseguridad en aquellos foros de alto nivel en los que el Responsable Corporativo de la Función de Ciberseguridad no participe directamente.
- Establecerá las áreas de CAF que deberán estar representadas en el Comité Corporativo de Ciberseguridad.

d) Función de Ciberseguridad y Responsable Corporativo de la Función de Ciberseguridad

La Función de Ciberseguridad es el órgano interno encargado del desarrollo, la implementación y la aplicación de las directrices estratégicas establecidas por el Consejo de Administración en materia de ciberseguridad. Podrá depender funcionalmente del Consejo de Administración, de la Comisión de Auditoría o de la alta dirección, con independencia de los responsables de sistemas de redes y de información.

Su máximo responsable (el "**Responsable Corporativo de la Función de Ciberseguridad**") será una persona con el conocimiento, experiencia y competencias adecuadas para desarrollar la función y contará con la suficiente capacidad de decisión e influencia en la organización.

Entre sus principales competencias, la Función de Ciberseguridad asegurará la valoración, control, gestión y monitorización de los riesgos de ciberseguridad, y la implementación de mecanismos adecuados de ciberresiliencia, garantizando el correcto reporte a los foros apropiados. Asimismo, definirá los indicadores de rendimiento asociados a la ciberseguridad y promoverá iniciativas de formación y sensibilización en la organización.

El Responsable Corporativo de la Función de Ciberseguridad reportará a la Dirección de Tecnología y, en todo caso, informará periódicamente a la Comisión de Auditoría sobre el ejercicio de sus funciones, en línea con las mejores prácticas en la materia.

La Función de Ciberseguridad será objeto de evaluación periódica en el marco del sistema de control y gestión de riesgos.

e) Comité Corporativo de Ciberseguridad

El Grupo contará con un Comité Corporativo de Ciberseguridad para adoptar aquellas resoluciones de relevancia en materia de seguridad de la información que puedan afectar sustancialmente a la actividad del Grupo.

El Comité Corporativo de Ciberseguridad tendrá un número adecuado de áreas de la organización representadas, además del Director de Tecnología y del Responsable Corporativo de la Función de Ciberseguridad.

Podrán existir otras estructuras colegiadas para el desarrollo de las competencias del Responsable Corporativo de la Función de Ciberseguridad que actuarán bajo la coordinación del mismo.

También se constituirán comités de crisis de ciberseguridad y se hará participe a la Función de Ciberseguridad de otros comités de crisis de otra índole en función de las necesidades.

f) Dirección del Negocio

Se define como Dirección del Negocio al máximo órgano responsable de una división de actividad concreta de negocio dentro del Grupo CAF.

La responsabilidad clave de la Dirección del Negocio en materia de ciberseguridad será la implantación de esta Política, asegurando la definición de planes de despliegue para el desarrollo, supervisión y control dentro del propio Negocio, para lo cual se designará al Responsable de Ciberseguridad del Negocio.

g) Responsable de Ciberseguridad del Negocio

El Responsable de Ciberseguridad del Negocio coordinará todas las gestiones a nivel de Negocio relacionadas con la ciberseguridad, como el despliegue de las directrices corporativas de ciberseguridad en el Negocio y el establecimiento de las competencias en materia de ciberseguridad, habilitando los planes de formación y concienciación corporativos, e identificando las posibles necesidades específicas que el Negocio pueda tener.

6. SISTEMA INTERNO DE INFORMACIÓN (CANALES DE DENUNCIAS)

Todos los miembros del Grupo tienen la obligación de informar sobre comportamientos o conductas identificadas en el contexto laboral o profesional que puedan contravenir los principios y parámetros establecidos en la presente Política, incluidas cualesquiera actuaciones o conductas conocidas que puedan suponer un indicio de riesgo.

Para ello, deberán utilizar al Sistema Interno de Información del Grupo, de acuerdo con lo establecido en la Política del Sistema Interno de Información del Grupo, accediendo al mismo a través de la página web corporativa. Este mecanismo está accesible igualmente a cualquier tercero ajeno al Grupo a efectos de informar sobre incumplimientos derivados de la presente Política.

El Sistema Interno de Información del Grupo ofrece las garantías de confianza, confidencialidad (incluyendo la protección de la identidad del informante) y prohibición de represalias reflejadas en la Política del Sistema Interno de Información y deberá ser empleado de buena fe, sobre la base de una creencia razonable de la existencia de un incumplimiento o de un riesgo de aparición del mismo.

7. REVISIÓN Y ACTUALIZACIÓN

El Consejo de Administración de CAF, a instancia de la Comisión de Auditoría, actualizará la Política, especialmente cuando se produzcan alguna de las siguientes circunstancias:

- Se aprueben cambios normativos relevantes que afecten al contenido de la presente Política.
- Se detecten áreas de mejora o deficiencias sobre el contenido de la presente Política como resultado de revisiones y verificaciones realizadas sobre la misma.

8. APROBACIÓN Y DIFUSIÓN

La presente Política es aprobada por el Consejo de Administración con fecha 10 de octubre de 2024, fecha a partir de la cual entra en vigor.

Para facilitar su contenido por los interesados y destinatarios de la misma, esta Política se publicará en la web de CAF, así como en los canales internos del Grupo.