Contrato de Concesión No.

Apéndice Técnico 14

Programa de Ciberseguridad IT/OT

Tabla de contenido

CAPÍTULO I – DISPOSICIONES GENERALES

SECCIÓN 1 – OBJETO

1.1 El presente Apéndice establece los requisitos mínimos para la gestión de la ciberseguridad del Proyecto durante las fases de diseño, construcción, integración, pruebas, puesta en servicio, operación, mantenimiento, renovación, reposición y reversión.

1.2 El objetivo del presente Apéndice es garantizar la protección de los sistemas, activos digitales, redes, comunicaciones, datos e información del Proyecto frente a amenazas cibernéticas, preservando la seguridad operacional, la continuidad del servicio, la disponibilidad de los sistemas críticos, la integridad de las funciones de seguridad y la confidencialidad de la información.

1.3 Las disposiciones del presente Apéndice serán aplicables a la totalidad de los sistemas ferroviarios, tecnológicos y corporativos del Proyecto, incluyendo, entre otros, los sistemas de señalización y control de trenes, energía, telecomunicaciones, Centro de Control Operacional (OCC), material rodante, patios-talleres y plataformas corporativas, así como a sus interfaces, comunicaciones y a los servicios prestados por terceros que se integren con dichos sistemas.

SECCIÓN 2 – PRINCIPIOS GENERALES

2.1 El Concesionario será responsable de establecer, implementar, mantener y mejorar continuamente un Programa Integral de Ciberseguridad para el Proyecto.

2.2 El Programa Integral de Ciberseguridad deberá basarse en principios de gestión de riesgos, defensa en profundidad, resiliencia operacional, mejora continua, seguridad y privacidad desde el diseño y por defecto, y protección proporcional a la criticidad de los activos.

2.3 El Concesionario será responsable de adaptar y actualizar todo el marco de ciberseguridad durante toda la vigencia de la Concesión, considerando la evolución tecnológica, los cambios regulatorios y la evolución del panorama de amenazas y de los riesgos, de modo que las medidas se mantengan eficaces a lo largo del tiempo.

2.4 El Plan de Ciberseguridad, así como las medidas, controles y procedimientos implementados por el Concesionario para su cumplimiento, deberán ser consistentes y estar plenamente alineados con los requisitos establecidos en los demás Apéndices del Contrato, en particular aquellos relacionados con la seguridad operacional, la seguridad física, la

continuidad del servicio, la disponibilidad de los sistemas, la protección de la información, la gestión de riesgos y la resiliencia del Sistema Ferroviario.

SECCIÓN 3 – OBLIGACIONES DE RESULTADO

3.1 El presente Apéndice no prescribe medios, tecnologías, productos ni soluciones específicas, salvo los mínimos indispensables expresamente señalados. Corresponde al Concesionario definir, en su Plan de Ciberseguridad y atendiendo a la evaluación de riesgos, las medidas, controles y tecnologías necesarias para alcanzar los objetivos y resultados exigidos.

3.2 El Concesionario será responsable de proteger la confidencialidad, la integridad y la disponibilidad de los activos del Proyecto frente a las amenazas cibernéticas actuales y frente a las que puedan surgir durante la vigencia de la Concesión, sobre la base de la gestión de riesgos, la defensa en profundidad y los principios de seguridad y privacidad desde el diseño y por defecto. La adopción de un estándar o la aprobación del Plan no eximen al Concesionario de alcanzar el resultado de protección exigido.

3.3 La aprobación o no objeción de cualquier documento por parte de la Interventoría no eximirá al Concesionario de su responsabilidad por el cumplimiento de los objetivos de ciberseguridad establecidos en el Contrato.

SECCIÓN 4 – ARTICULACIÓN ENTRE SEGURIDAD FUNCIONAL Y CIBERSEGURIDAD

4.1 Las medidas de ciberseguridad deberán diseñarse de manera coordinada con la seguridad funcional (safety) y no podrán degradar el nivel de integridad de seguridad (SIL) ni las funciones de seguridad de los subsistemas, en particular los de señalización y control de trenes.

4.2 El Concesionario aplicará un enfoque de ingeniería conjunta de seguridad funcional y ciberseguridad (safety-security co-engineering), de modo que la acreditación de ciberseguridad y la aprobación de seguridad se desarrollen de forma articulada, integrando el proceso de ciberseguridad con el ciclo de vida RAMS conforme al Apéndice Técnico 1 y a las normas aplicables conforme al Apéndice Técnico 2, particularmente la norma CLC/TS 50701.

SECCIÓN 5 – RÉGIMEN DE REVISIÓN Y NO OBJECIÓN

5.1 El Plan de Ciberseguridad y los demás entregables previstos en el presente Apéndice serán presentados por el Concesionario acompañados del respectivo medio de acreditación. La Interventoría emitirá la respectiva No Objeción técnica a la propuesta presentada por el Concesionario. Solo podrán requerirse los ajustes necesarios cuando alguna de las especificaciones propuestas no permita garantizar el cumplimiento funcional y operacional de las exigencias previstas en el Contrato.

5.2 Los medios de acreditación podrán comprender, según corresponda, certificaciones de organismos independientes, informes de pruebas y ensayos, resultados de evaluaciones de vulnerabilidades y de pruebas de penetración, análisis de riesgos, el caso de ciberseguridad y demás evidencias verificables que permitan a la Interventoría comprobar el cumplimiento de los requisitos del presente Apéndice.

CAPÍTULO II – MARCO DE CUMPLIMIENTO Y ESTÁNDARES DE REFERENCIA

SECCIÓN 6 – ESTÁNDARES DE REFERENCIA, CERTIFICACIONES Y ACREDITACIONES

6.1 Sin perjuicio de lo establecido en el Apéndice Técnico 2 y del cumplimiento de la Ley Aplicable, el Plan de Ciberseguridad y su implementación deberán ser conformes con los estándares y marcos de referencia relacionados en el presente numeral, en las versiones que resulten aplicables conforme al Apéndice Técnico 2 y, en su defecto, en sus versiones vigentes al momento de su aplicación:

a) Serie IEC 62443 (seguridad de los sistemas de automatización y control industrial – IACS) como marco base del dominio OT, incluyendo, entre otras, las partes 2-1, 3-2, 3-3, 4-1 y 4-2.

b) CLC/TS 50701 (Aplicaciones ferroviarias – Ciberseguridad), integrada con el ciclo de vida RAMS de la norma EN 50126, y la norma internacional IEC 63452 una vez vigente y aplicable.

c) ISO/IEC 27001 e ISO/IEC 27002, como marco base del dominio IT.

d) Marco de Ciberseguridad del NIST (NIST CSF), guía NIST SP 800-82 y CIS Controls, como referencias complementarias de buenas prácticas.

6.2 Las referencias normativas incluidas en el presente Apéndice corresponden a las versiones vigentes al momento de su elaboración. En caso de que dichas normas sean actualizadas, modificadas, sustituidas, derogadas o reemplazadas por nuevas versiones durante la vigencia del Contrato, se entenderá que la referencia corresponde a la versión vigente respectiva, salvo disposición expresa en contrario o cuando el presente Contrato establezca una versión específica de obligatorio cumplimiento.

6.3 El Concesionario deberá tratar el Proyecto, para efectos de ciberseguridad, como infraestructura crítica cibernética asociada a un servicio esencial, identificando sus activos e infraestructuras críticas, reportando la información que corresponda ante las autoridades competentes y articulándose con las instancias nacionales de coordinación y respuesta a incidentes que defina la Ley Aplicable.

6.4 El Concesionario deberá acreditar, mediante certificaciones de organismos independientes o evidencias verificables por la Interventoría, el cumplimiento de los estándares de referencia, incluyendo, como mínimo indispensable, la certificación ISO/IEC 27001 del sistema de gestión de seguridad de la información para el alcance del Proyecto y la conformidad de los subsistemas OT con los niveles de seguridad objetivo (SL-T) definidos conforme a la serie IEC 62443 y a la norma CLC/TS 50701.

CAPÍTULO III – PLAN DE CIBERSEGURIDAD

SECCIÓN 7 – OBLIGACIÓN DE ELABORAR Y MANTENER EL PLAN

7.1 El Concesionario deberá elaborar, implementar, mantener y mejorar de forma continua un Plan de Ciberseguridad del Proyecto que dé cumplimiento a los objetivos, resultados y requisitos del presente Apéndice y a los estándares y normas de la SECCIÓN 6. El Plan de Ciberseguridad es el instrumento mediante el cual el Concesionario define las medidas, controles, procesos y tecnologías con los que alcanzará dichos objetivos, comprendiendo, entre otros aspectos, la gobernanza de la ciberseguridad, la gestión de riesgos, el inventario y la clasificación de activos, la implementación de controles técnicos, administrativos y físicos, la gestión de identidades y accesos, la protección de redes, sistemas e información, la gestión de vulnerabilidades e incidentes, la continuidad y recuperación de los servicios, la gestión de terceros, el monitoreo y la auditoría de los controles, la capacitación del personal y el proceso de revisión y mejora continua.

7.2 El Plan de Ciberseguridad y sus actualizaciones se someterán al régimen de revisión, no objeción y derecho de oposición de que trata el Contrato de Concesión. La no objeción del Plan no traslada a la EFR ni a la Interventoría responsabilidad alguna por su suficiencia, ni exime al Concesionario de su obligación de resultado.

7.3 El Concesionario deberá presentar una versión inicial del Plan de Ciberseguridad en la fase Previa, dentro de los sesenta (60) días siguientes a la suscripción del Acta de Inicio, y mantenerlo vigente y actualizado durante toda la ejecución del Contrato. La vigencia del Plan actualizado, la demostración del cumplimiento de sus objetivos y la aceptación del riesgo residual, constituyen condiciones para la Puesta en Servicio Comercial.

SECCIÓN 8 – OBJETIVOS Y RESULTADOS DEL PLAN DE CIBERSEGURIDAD

8.1 El Plan de Ciberseguridad deberá garantizar, como mínimo, los siguientes resultados:

a) La protección de la confidencialidad, integridad y disponibilidad de los activos de información y de los sistemas de control del Proyecto.

b) La preservación de la seguridad funcional, de modo que ninguna medida de ciberseguridad degrade las funciones de seguridad ni el SIL de los subsistemas.

c) La separación efectiva entre los dominios IT y OT y el control de los flujos de información entre zonas de distinta criticidad.

d) La detección oportuna, la contención, la respuesta y la recuperación frente a incidentes, preservando la continuidad y la seguridad de la operación.

e) El cumplimiento de la Ley Aplicable y de los estándares de referencia, y la disponibilidad de evidencias verificables de dicho cumplimiento.

SECCIÓN 9 – CONTENIDO MÍNIMO DEL PLAN

9.1 El Plan de Ciberseguridad deberá comprender, como mínimo, los siguientes componentes, cuyo desarrollo detallado corresponde al Concesionario:

a) Política, organización, roles y responsabilidades de ciberseguridad, con segregación de funciones e independencia respecto de las áreas auditadas.

b) Inventario y gestión de los activos IT/OT y de su criticidad.

c) Metodología y resultados de la gestión de riesgos de ciberseguridad, incluida la definición de los niveles de seguridad objetivo (SL-T) por zona, conforme a IEC 62443-3-2 y CLC/TS 50701.

d) Arquitectura de seguridad y segmentación IT/OT, mediante un modelo de zonas y conductos.
e) Gestión de identidades, accesos y acceso remoto.
f) Medidas de protección de los sistemas OT, preservando la seguridad funcional.
g) Medidas de protección de los sistemas IT y de los datos, incluida la protección de datos personales.
h) Seguridad en el ciclo de vida y en la cadena de suministro, con requisitos verificables a proveedores y fabricantes.
i) Aseguramiento y configuración segura de los sistemas, y gestión de vulnerabilidades y de parches, diferenciada para IT y OT.
j) Capacidades de monitoreo, detección y respuesta a incidentes, y procedimientos de notificación.
k) Plan de continuidad y de recuperación ante ciberataques, con objetivos de recuperación por sistema crítico.
l) Seguridad física de los activos críticos, seguridad del personal y programa de cultura y formación.
m) Programa de auditoría, métricas, pruebas periódicas, acreditación y mejora continua. Las pruebas podrán comprender, entre otras, evaluaciones de vulnerabilidades, pruebas de penetración, revisión de configuraciones de seguridad, pruebas de recuperación y ejercicios de respuesta a incidentes, orientadas a verificar la eficacia de los controles implementados y a gestionar oportunamente las desviaciones identificadas.
n) Caso de ciberseguridad, entendido como la argumentación estructurada y respaldada por evidencias que demuestra que los objetivos de ciberseguridad se han alcanzado y que el riesgo residual es aceptable.

SECCIÓN 10 – ACTUALIZACIÓN Y VIGENCIA

10.1 El Concesionario deberá actualizar el Plan de Ciberseguridad periódicamente, y como máximo cada año, así como ante cambios significativos en los sistemas, en la evaluación de riesgos o en la Ley Aplicable, y presentar las respectivas actualizaciones para la No Objeción de la Interventoría.

10.2 El Concesionario deberá elaborar y mantener un caso de ciberseguridad (cybersecurity case) que provea la argumentación estructurada y respaldada por evidencias del

cumplimiento de los requisitos del presente Apéndice y de los estándares de referencia y de la aceptabilidad del riesgo residual, articulado con la aprobación de seguridad y manteniendo la separación apropiada entre ambos procesos conforme a la normativa aplicable según el Apéndice Técnico 2, en particular la CLC/TS 50701.

CAPÍTULO IV – REQUISITOS DE SEGURIDAD DE LOS SISTEMAS OT

SECCIÓN 11 – REQUISITOS GENERALES

11.1 El Plan de Ciberseguridad deberá establecer las medidas necesarias para proteger los sistemas OT, priorizando la disponibilidad y la integridad de las funciones de operación y control, sin comprometer la seguridad funcional. Dichas medidas deberán ser compatibles con las restricciones de tiempo real, los ciclos de vida prolongados y las condiciones operativas de los sistemas industriales ferroviarios, y no podrán introducir latencias o indisponibilidades que afecten la operación segura.

11.2 El Plan deberá prever la segmentación y la separación efectiva entre los dominios IT y OT; la interconexión entre ambos, cuando sea estrictamente necesaria, se realizará mediante mecanismos de control de flujo acordes con la criticidad, según el Concesionario lo justifique en el Plan.

SECCIÓN 12 – TRATAMIENTO POR SUBSISTEMA

12.1 El Plan deberá definir el tratamiento de ciberseguridad de cada subsistema OT en función de su criticidad, garantizando, como mínimo:

a) Para la señalización y control de trenes, de acuerdo con el Apéndice Técnico 10, el tratamiento de máxima criticidad bajo el enfoque de ingeniería conjunta seguridad-ciberseguridad, sin degradar las funciones de seguridad ni el SIL, privilegiando esquemas de monitoreo que no interfieran con la operación crítica.

b) Para el sistema de energía y su SCADA, de acuerdo con el Apéndice Técnico 9, la protección acorde con su criticidad para la continuidad de la tracción y la seguridad eléctrica.

c) Para el Centro de Control Operacional, de acuerdo con el Apéndice Técnico 12, la protección como zona crítica de convergencia, con segmentación respecto de IT, monitoreo y redundancia.

d) Para el Material Rodante y las comunicaciones tren-tierra, de acuerdo con el Apéndice Técnico 15, la incorporación de requisitos de ciberseguridad desde el diseño, incluida la protección de las interfaces de mantenimiento y diagnóstico.

e) Para los demás sistemas OT de estación (puertas de andén, información al pasajero, CCTV y control de edificaciones), su integración en el modelo de zonas y conductos con el nivel de protección que corresponda a su criticidad.

12.2 El Plan deberá prever el aseguramiento y la configuración segura de los sistemas OT, así como la gestión de vulnerabilidades y de parches mediante procedimientos específicos para entornos OT, con evaluación de impacto, pruebas previas en entornos representativos y ventanas de mantenimiento que preserven la seguridad y la disponibilidad de la operación.

CAPÍTULO V – REQUISITOS DE SEGURIDAD DE LOS SISTEMAS IT Y DE LA INFORMACIÓN

SECCIÓN 13 – PROTECCIÓN DE LOS SISTEMAS IT

13.1 El Plan de Ciberseguridad deberá establecer las medidas necesarias para proteger los sistemas de IT corporativo, back-office, bases de datos y servicios de soporte, garantizando la confidencialidad, integridad y disponibilidad de la información conforme a ISO/IEC 27001 e ISO/IEC 27002.

13.2 El Plan deberá garantizar el control de acceso bajo el principio de mínimo privilegio y la autenticación reforzada de los accesos privilegiados y remotos, con la asignación y revocación oportuna de permisos y su revisión periódica, conforme al riesgo de cada activo.

13.3 El Plan deberá prever la clasificación de la información según su criticidad y sensibilidad y la aplicación de controles de protección proporcionales, incluida la protección de la información sensible en reposo y en tránsito. El tratamiento de datos personales deberá cumplir la Ley Aplicable.

13.4 El Plan deberá prever la protección de equipos y servidores frente a código malicioso y las capacidades de detección y respuesta acordes con su criticidad.

13.5 Cuando el Concesionario desarrolle o integre aplicaciones, el Plan deberá prever prácticas de desarrollo seguro a lo largo del ciclo de vida y la gestión de las vulnerabilidades identificadas, incluida la evaluación del código fuente o del código ejecutable mediante herramientas automatizadas o revisiones técnicas, con el propósito de identificar

vulnerabilidades, errores de programación, incumplimientos de estándares de desarrollo seguro y otras debilidades que puedan afectar la seguridad, la confiabilidad o la integridad del software. Cuando se empleen servicios en la nube, el Plan deberá garantizar los niveles de seguridad, disponibilidad, soberanía y protección de datos exigidos, con un modelo claro de responsabilidad compartida.

CAPÍTULO VI – SEGURIDAD EN EL CICLO DE VIDA Y CADENA DE SUMINISTRO

SECCIÓN 14 – SEGURIDAD EN EL CICLO DE VIDA

14.1 El Plan deberá garantizar que la ciberseguridad se incorpore desde las fases de diseño de todos los subsistemas, con configuraciones seguras por defecto, y se verifique en cada hito del ciclo de vida, de forma articulada con el proceso RAMS del Apéndice Técnico 1.

14.2 El Plan deberá establecer requisitos de ciberseguridad verificables a proveedores y fabricantes, incluyendo procesos de desarrollo seguro de productos (IEC 62443-4-1) y requisitos de seguridad de componentes (IEC 62443-4-2), así como el soporte de seguridad durante el ciclo de vida y la gestión de los riesgos de la cadena de suministro y de los terceros con acceso a los sistemas.

14.3 Como mínimo indispensable y condición para la Puesta en Servicio Comercial, el Concesionario deberá realizar evaluaciones de vulnerabilidades y pruebas de penetración sobre los sistemas IT y OT, con remediación verificada de los hallazgos críticos y altos, bajo la supervisión de la Interventoría.

14.4 El Plan deberá prever un proceso continuo de identificación, evaluación, priorización y remediación de vulnerabilidades y de gestión de parches, con plazos acordes a la criticidad, así como la gestión de la obsolescencia de los componentes con impacto en la ciberseguridad durante toda la vigencia del Contrato.

CAPÍTULO VII – MONITOREO, DETECCIÓN Y RESPUESTA A INCIDENTES

SECCIÓN 15 – MONITOREO, DETECCIÓN Y RESPUESTA A INCIDENTES

15.1 El Plan deberá prever capacidades de monitoreo continuo de la seguridad y de detección de eventos y anomalías, incluida la detección en entornos OT sin interferir con los sistemas críticos, así como la conservación de los registros de seguridad por el período que defina la Ley Aplicable. Dichas capacidades se soportarán en un Centro de Operaciones de Seguridad (SOC), propio o provisto por un tercero, que opere de forma continua.

15.2 El Plan deberá establecer un proceso documentado de gestión de eventos e incidentes y un plan de respuesta que defina los roles y los procedimientos de detección, contención, erradicación y recuperación, así como los protocolos de comunicación y el análisis posterior y lecciones aprendidas. El Plan deberá clasificar los incidentes por niveles de severidad, conforme a la Tabla 1, y asociar a cada nivel los tiempos máximos de notificación y de respuesta.

Tabla 1. Niveles de severidad de incidentes de ciberseguridad y tiempos máximos de notificación

Nivel	**Descripción de referencia**	**Notificación a la EFR y a la Interventoría**	**Respuesta**
Crítico	Incidente que afecta o compromete la seguridad de la operación, la disponibilidad de sistemas críticos o la integridad de las funciones de seguridad, o que implica una violación de datos de gran impacto	Inmediata y, en todo caso, dentro de las 2 horas siguientes a su detección	Inmediata, con activación del plan de respuesta
Alto	Incidente con impacto significativo en sistemas IT u OT no críticos, o con potencial de escalar a crítico	Dentro de las 4 horas siguientes a su detección	Dentro de las 8 horas siguientes
Medio	Incidente con impacto limitado y contenido, sin afectación de la operación	Dentro de las 24 horas siguientes a su detección	Dentro de las 72 horas siguientes
Bajo	Evento o incidente menor sin impacto operacional, gestionado como parte de la operación ordinaria	En el informe periódico de ciberseguridad	Conforme al procedimiento ordinario

15.3 Los niveles, descripciones y tiempos de la Tabla 1 constituyen mínimos de referencia. El Concesionario podrá proponer una clasificación más granular en su Plan, siempre que no resulte menos exigente, y deberá conciliarla con los plazos y niveles que establezca la Ley Aplicable, que prevalecerán cuando sean más estrictos.

15.4 El Concesionario deberá notificar los incidentes a la Interventoría y a la EFR, así como a las autoridades competentes, conforme a la Tabla 1, a la Ley Aplicable y dentro de los plazos que esta establezca.

15.5 El Plan deberá integrar los escenarios de ciberataque en la continuidad y recuperación de la operación, definiendo objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO) por sistema crítico, copias de respaldo seguras y aisladas y procedimientos de operación en modo degradado, articulados con los requisitos de disponibilidad del Apéndice Técnico 1.

CAPÍTULO VIII – SEGURIDAD FÍSICA, DEL PERSONAL Y CULTURA

SECCIÓN 16 – SEGURIDAD FÍSICA Y DEL PERSONAL

16.1 El Plan deberá prever la seguridad física de los activos de información y de los sistemas de control críticos, articulada con los Apéndices Técnicos 12 (CCO) y 6 (Estaciones), así como los controles de seguridad asociados al personal propio y de terceros, incluida la gestión de altas y bajas y la asignación y revocación oportuna de accesos.

16.2 El Plan deberá incluir un programa permanente de concientización, formación y desarrollo de competencias en ciberseguridad para el personal con responsabilidades en IT y OT, con contenidos y periodicidad acordes a los roles y a la criticidad de las funciones.

CAPÍTULO IX – ACREDITACIÓN, AUDITORÍA Y MEJORA CONTINUA

SECCIÓN 17 – ACREDITACIÓN DE CIBERSEGURIDAD

17.1 La acreditación de ciberseguridad, sustentada en el caso de ciberseguridad y en la verificación del cumplimiento del Plan, constituirá un requisito para la Puesta en Servicio Comercial, articulada con la aprobación de seguridad conforme a la normativa aplicable según el Apéndice Técnico 2, en particular con la norma CLC/TS 50701 y al Apéndice Técnico 1, en su capítulo de RAMS.

17.2 El cumplimiento del Plan será objeto de auditorías internas y externas y de pruebas periódicas (evaluaciones de vulnerabilidades, pruebas de penetración y ejercicios de respuesta a incidentes), con una periodicidad máxima anual, y remediación verificada. La EFR y la Interventoría tendrán el derecho de auditar, en cualquier momento, el cumplimiento de los requisitos del presente Apéndice, y el Concesionario deberá facilitar el acceso a la información y a las evidencias necesarias.