GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA

AESF AGENCIA ESTATAL DE SEGURIDAD FERROVIARIA

Guía para la implementación de LA CULTURA DE LA SEGURIDAD EN LOS SGS

DOCUMENTO 7:

El reporte confidencial de riesgos

Versión 01

CONTROL DOCUMENTAL

	NOMBRE	PUESTO	FIRMA
ELABORADO			
REVISADO			
APROBADO			

CONTROL DE VERSIONES

Versión	Fecha	Motivo
1	Junio 2022	Primera edición.

ÍNDICE

INTRODUCCIÓN

Una de las principales novedades introducidas por la "Directiva (UE) 2016/798 del Parlamento Europeo y del Consejo de 11 de mayo de 2016 sobre la seguridad ferroviaria", es su evolución hacia un enfoque de la seguridad en las organizaciones ferroviarias basado en fortalecer su cultura de la seguridad, con un mayor peso en la consideración de los factores humanos y organizativos.

Así, en la Directiva se indica que:

> *"Los administradores de infraestructuras y las empresas ferroviarias fomentarán, a través del sistema de gestión de la seguridad, una cultura de confianza y aprendizaje mutuos, en la que se anime al personal para que contribuya al desarrollo de la seguridad al tiempo que se garantiza la confidencialidad".*

La cultura de seguridad es un conjunto de patrones de comportamiento y pensamiento, compartidos dentro de una organización, relativo a la gestión de los riesgos de la actividad. Y lógicamente, tiene una gran interrelación con los sistemas de gestión de la seguridad de dichas organizaciones, que vienen a establecer la base de sus formas de trabajo. Esas normas y procedimientos escritos, vienen a complementarse con las "normas no escritas que rigen el comportamiento y las decisiones" de las personas y la organización que vendrán determinadas por su cultura.

Las organizaciones ferroviarias y sus trabajadores tienen históricamente una buena cultura de la seguridad con una alta concienciación de la importancia de la seguridad. Sin embargo, a pesar de ello, existe margen para seguir evolucionando en paralelo a la introducción de los nuevos enfoques sistémicos y de orientación a riesgos, más proactivos.

Por tanto, **cultura de la seguridad y sistemas de gestión están indisolublemente unidos**, de modo que un sistema de gestión en una organización sin una sólida cultura de la seguridad será probablemente ineficaz. Y, recíprocamente, para consolidar esa cultura, es necesario sentar sus bases en los procedimientos de la entidad.

En desarrollo de lo anterior, **la cultura de la seguridad pasa a ser uno de los requisitos que deben incluirse en los sistemas de gestión de la seguridad de los actores del sistema**, tal y como se desarrolla en el "Reglamento Delegado (UE) 2018/762 de la Comisión de 8 de marzo de 2018 por el que se establecen métodos comunes de seguridad sobre los requisitos del sistema de gestión de la seguridad de conformidad con la Directiva (UE) 2016/798 del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (UE) nº 1158/2010 y (UE) nº 1169/2010 de la Comisión".

En uno de sus condicionados se recoge:

> *"(7) La manera de percibir la seguridad y de valorarla y darle prioridad en una organización refleja el compromiso real con la seguridad a todos los niveles de la*

organización. Por ello, también es importante que las empresas ferroviarias y los administradores de infraestructuras determinen las medidas y los comportamientos que pueden configurar una cultura positiva de seguridad y fomentar a través de su sistema de gestión de la seguridad esta cultura de confianza y aprendizaje mutuos, en la que se anime al personal para que contribuya al desarrollo de la seguridad comunicando incidencias peligrosas y aportando información relativa a la seguridad."

Incluso de manera más concreta, uno de los criterios objeto de evaluación es el siguiente:

"7.2.3. La organización ofrecerá una estrategia para la mejora continua de la cultura de la seguridad, basándose en el uso de conocimientos técnicos y métodos reconocidos para detectar los elementos del comportamiento que tengan repercusiones en las distintas partes del sistema de gestión de la seguridad e introducir medidas para hacerles frente."

Con estos antecedentes, el campo ferroviario europeo prosigue con una evolución parecida a la que han tenido otros sectores como el industrial, el nuclear o el aeronáutico, en el que se promueve la mejora de los niveles de seguridad a través de cambios culturales de las organizaciones.

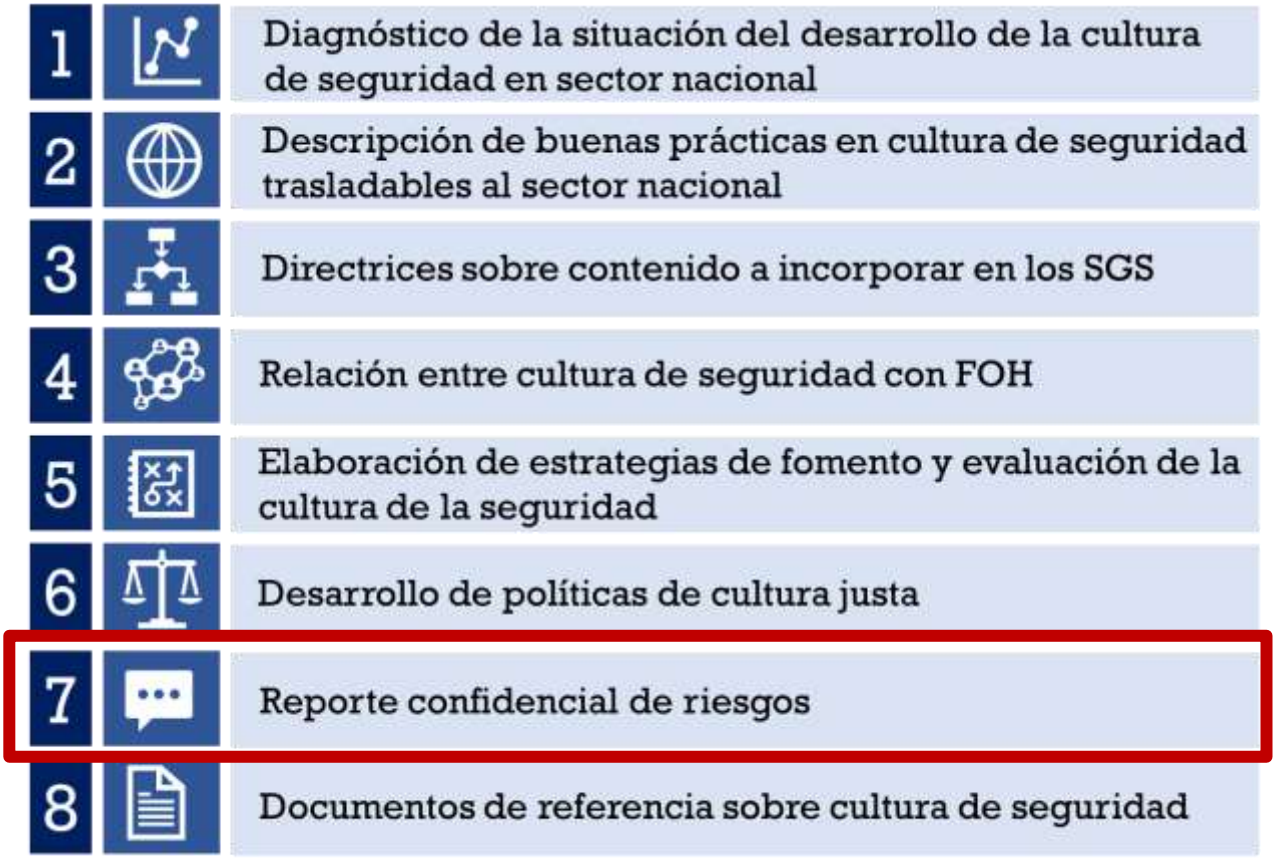
Por tanto, buscar ejemplos de buenas prácticas en otros campos o países que sean trasladables al campo ferroviario nacional, parece oportuno para orientar a las entidades ferroviarias en estos enfoques que pueden ser novedosos.

OBJETO Y ESTRUCTURA DEL CONJUNTO DE GUÍAS SOBRE CULTURA DE LA SEGURIDAD

En el contexto anterior, la AESF ha desarrollado un conjunto de guías que tiene por objeto establecer unas directrices que sirvan de guía para la implementación de la cultura de la seguridad en los SGS de las entidades ferroviarias.

Para la elaboración de este conjunto de documentos, la AESF ha tenido en cuenta las conclusiones del Estudio *"Buenas prácticas para el fomento de la cultura de seguridad en los sistemas de gestión"*. Este estudio ha sido elaborado por ESM Instituto de Investigación en Seguridad y Factores Humanos, S.L. en el periodo comprendido entre julio de 2020 y julio de 2021. Para la elaboración del estudio se han realizado encuestas y entrevistas con representantes de organizaciones de entidades ferroviarias nacionales y europeas, así como con representantes de entidades de otros sectores diferentes al ferroviario.

Esta serie de guías se compone de ocho documentos editados de manera independiente, que abordan diferentes dimensiones de la cultura de la seguridad. Éstos son:



Abreviaturas

AESF	Agencia Estatal de Seguridad Ferroviaria
EUAR	Agencia Ferroviaria de la Unión Europea, en sus siglas en inglés (anteriormente Agencia Ferroviaria Europea -ERA-)
ERSCS	Encuesta europea sobre el clima de seguridad ferroviario
SGS	Sistema de gestión de la seguridad
FHO	Factores humanos y organizacionales
NTS	Habilidades no técnicas
CIAF	Comisión de Investigación de Accidentes Ferroviarios
RCR	Reporte confidencial de riesgos

Definiciones aplicables

- ***Buena práctica:*** Una buena práctica es una experiencia que se ha demostrado que funciona bien y produce buenos resultados y, por lo tanto, se recomienda como modelo.
- ***Cultura de seguridad:*** La Cultura de Seguridad se refiere a la interacción entre los requisitos del Sistema de Gestión de la Seguridad (SGS), la manera en que las personas los interpretan, conforme a sus actitudes, sus valores y sus creencias, y la manera en que realmente actúan, que se ve reflejada en sus decisiones y su comportamiento.
- ***Estrategia/política de cultura de seguridad:*** Una estrategia de Cultura de seguridad se trata de una planificación documentada que conlleva una serie de pasos o fases que van desde la evaluación inicial pasando por diversas acciones, revisión de resultados y mejora continua.
- ***Herramienta/Metodología***: Procedimiento racional utilizado para alcanzar un objetivo. Técnicas, métodos, herramientas de trabajo e investigación social habituales en las organizaciones, avaladas de rigor científico, que se aplican sistemáticamente durante un proceso de transformación, un proceso pedagógico o de investigación para alcanzar un resultado válido. La metodología funciona como el soporte o medio para conseguir el objetivo organizativo.
- ***Iniciativa de fomento de Cultura de Seguridad***: Se trata de actividades de promoción y difusión, a través de instituciones públicas o privadas, grupos de trabajo o asociaciones que sirvan como fomento para la cultura de seguridad.
- ***Cultura Justa***: Es una cultura en la que los operadores de primera línea no son castigados por acciones, omisiones o decisiones tomadas por ellos que estén en consonancia con su experiencia y formación, pero donde no se tolera la negligencia grave, las violaciones deliberadas y los actos destructivos.
- **Sistema de Gestión de Seguridad**: La organización, las medidas y los procedimientos establecidos por una empresa para garantizar la gestión de sus operaciones en condiciones de seguridad.

DOCUMENTACIÓN DE REFERENCIA

Se recomienda visitar la página web de la AESF (www.seguridadferroviaria.es) donde se mantiene un listado actualizado de la legislación nacional y europea aplicable al sector ferroviario.

A continuación, se expone una lista, no exhaustiva, de la principal normativa referenciada en estos documentos[1]:

Normativa europea y otros documentos de referencia

- Directiva (UE) 2016/798 de 11 de mayo de 2016, sobre la seguridad ferroviaria.
- Reglamento Delegado (UE) 2018/762 de la Comisión de 8 de marzo de 2018 por el que se establecen métodos comunes de seguridad sobre los requisitos del sistema de gestión de la seguridad de conformidad con la Directiva (UE) 2016/798 del Parlamento Europeo y del Consejo, y por el que se derogan los Reglamentos (UE) nº 1158/2010 y (UE) nº 1169/2010 de la Comisión
- Modelo europeo de cultura de la seguridad, elaborado por la Agencia Europea de Seguridad Ferroviaria (EUAR): https://www.era.europa.eu/safety-culture-model/

Normativa nacional de referencia

- Real Decreto 929/2020 de 27 de octubre, de seguridad operacional e interoperabilidad ferroviarias.

OBJETO DEL PRESENTE DOCUMENTO Nº 7

El conocimiento de las posibles amenazas, peligros, riesgos o situaciones mejorables debe ser un objetivo estratégico de la organización y, según consta en la Recomendación Técnica 7/2017 de la AESF, independientemente de otras fuentes (comunicaciones externas), dentro de las entidades ferroviarias existe otra potencial fuente de información de gran relevancia sobre posibles riesgos: las "**comunicaciones ascendentes**" sobre situaciones que los propios empleados, en el desempeño de sus funciones, pueden detectar y canalizar (reportar) dentro de su organización .

[1] Para información concreta más detallada, véase el documento específicamente dedicado a este tema, documento 8. "Documentos de referencia sobre cultura de seguridad"

Igualmente, en el artículo 9.2 de la Directiva 2016/798, establece que las entidades ferroviarias a través del SGS fomentarán **una cultura de confianza y aprendizaje mutuos**, en la que se anime al personal para que contribuya al desarrollo de la seguridad al tiempo que se garantiza la confidencialidad.

Asimismo, el Reglamento Delegado (UE) 2018/762 de la Comisión en el apartado 2.4 "*Consultas al personal y al resto de las partes*", hace hincapié en la necesidad de consultar al personal para la mejora del sistema de gestión de la seguridad y los procedimientos operativos.

Los procedimientos sobre las comunicaciones ascendentes deberían ser conocidos por todos los empleados, que deberían estar formados para que utilicen los canales adecuados. Las organizaciones facilitarán que se consulte al personal mediante métodos y recursos que faciliten su participación. Finalmente, todas estas comunicaciones e informaciones enviadas por el personal de las entidades ferroviarias sobre cuestiones relacionadas con la seguridad deberían gestionarse en un entorno de cultura justa.

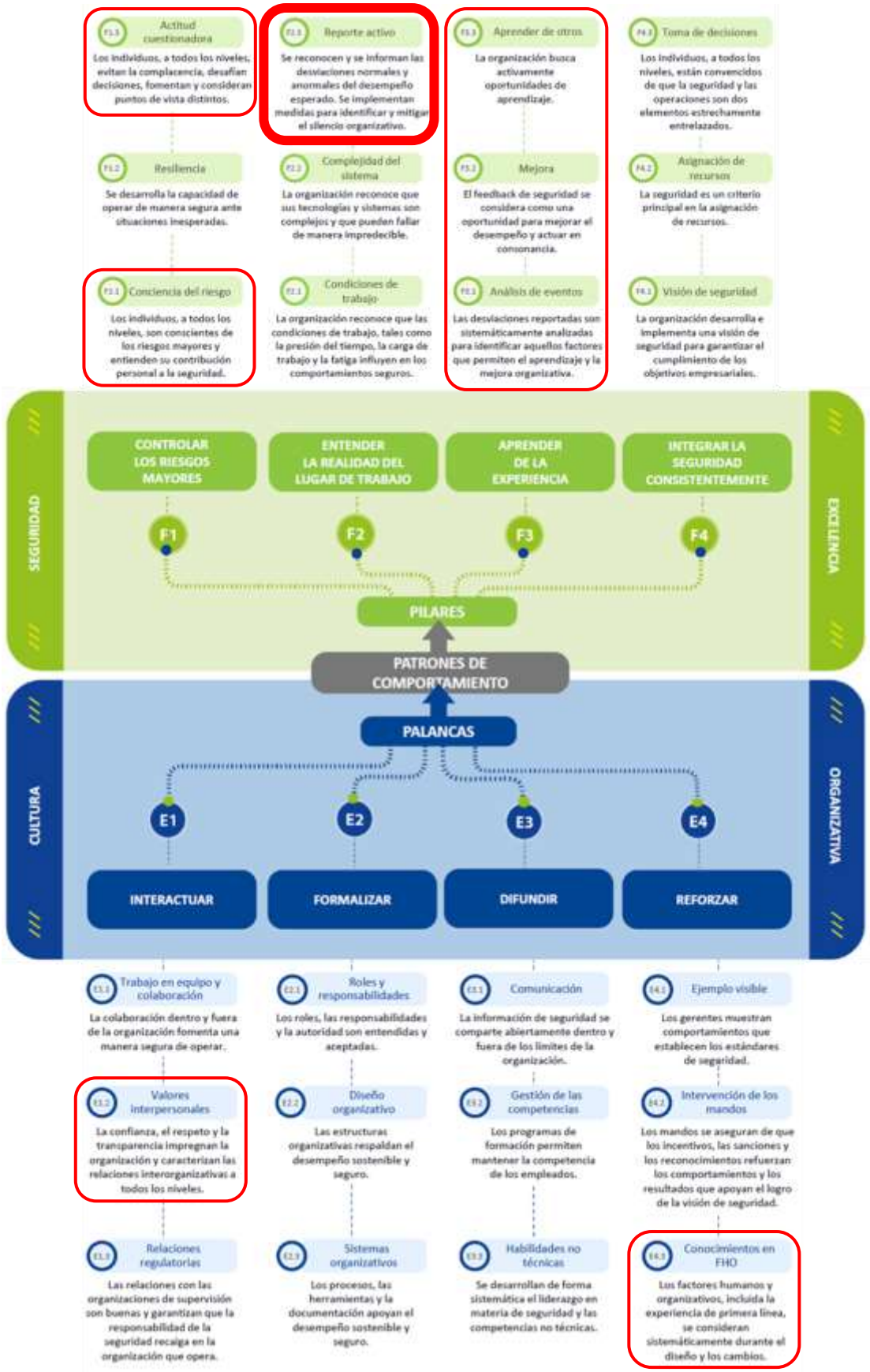
En este documento se describen, por tanto, los pasos mínimos necesarios para la implementación de un sistema de notificación confidencial, en el marco de una política de cultura justa.

RELACIÓN CON EL MODELO DE CULTURA DE LA SEGURIDAD DE EUAR

El contenido de este documento está relacionado principalmente con el atributo **F2.3 "Reporte activo"** del modelo de cultura de seguridad de la EUAR.

También está relacionado, en menor medida con otros como

- F1.1. Conciencia del riesgo
- F1.3. Actitud cuestionadora
- F3.1. Análisis de eventos
- F3.2. Mejora
- F3.3. Aprender de otros
- E1.2. Valores interpersonales
- E4.3. Conocimientos en FHO


Actitud cuestionadora
Los individuos, a todos los niveles, evitan la complacencia, desafían decisiones, fomentan y consideran puntos de vista distintos.
Reporte activo
Se reconocen y se informan las desviaciones normales y anormales del desempeño esperado. Se implementan medidas para identificar y mitigar el silencio organizativo.
Aprender de otros
La organización busca activamente oportunidades de aprendizaje.
Toma de decisiones
Los individuos, a todos los niveles, están convencidos de que la seguridad y las operaciones son dos elementos estrechamente entrelazados.
Resiliencia
Se desarrolla la capacidad de operar de manera segura ante situaciones inesperadas.
Complejidad del sistema
La organización reconoce que sus tecnologías y sistemas son complejos y que pueden fallar de manera impredecible.
Mejora
El feedback de seguridad se considera como una oportunidad para mejorar el desempeño y actuar en consonancia.
Asignación de recursos
La seguridad es un criterio principal en la asignación de recursos.
Consciencia del riesgo
Los individuos, a todos los niveles, son conscientes de los riesgos mayores y entienden su contribución personal a la seguridad.
Condiciones de trabajo
La organización reconoce que las condiciones de trabajo, tales como la presión del tiempo, la carga de trabajo y la fatiga influyen en los comportamientos seguros.
Análisis de eventos
Las desviaciones reportadas son sistemáticamente analizadas para identificar aquellos factores que permiten el aprendizaje y la mejora organizativa.
Visión de seguridad
La organización desarrolla e implementa una visión de seguridad para garantizar el cumplimiento de los objetivos empresariales.
SEGURIDAD
EXCELENCIA
CONTROLAR LOS RIESGOS MAYORES
ENTENDER LA REALIDAD DEL LUGAR DE TRABAJO
APRENDER DE LA EXPERIENCIA
INTEGRAR LA SEGURIDAD CONSISTENTEMENTE
F1
F2
F3
F4
PILARES
PATRONES DE COMPORTAMIENTO
PALANCAS
CULTURA
ORGANIZATIVA
E1
E2
E3
E4
INTERACTUAR
FORMALIZAR
DIFUNDIR
REFORZAR
Trabajo en equipo y colaboración
La colaboración dentro y fuera de la organización fomenta una manera segura de operar.
Roles y responsabilidades
Los roles, las responsabilidades y la autoridad son entendidas y aceptadas.
Comunicación
La información de seguridad se comparte abiertamente dentro y fuera de los límites de la organización.
Ejemplo visible
Los gerentes muestran comportamientos que establecen los estándares de seguridad.
Valores interpersonales
La confianza, el respeto y la transparencia impregnan la organización y caracterizan las relaciones interorganizativas a todos los niveles.
Diseño organizativo
Las estructuras organizativas respaldan el desempeño sostenible y seguro.
Gestión de las competencias
Los programas de formación permiten mantener la competencia de los empleados.
Intervención de los mandos
Los mandos se aseguran de que los incentivos, las sanciones y los reconocimientos refuerzan los comportamientos y los resultados que apoyan el logro de la visión de seguridad.
Relaciones regulatorias
Las relaciones con las organizaciones de supervisión son buenas y garantizan que la responsabilidad de la seguridad recaiga en la organización que opera.
Sistemas organizativos
Los procesos, las herramientas y la documentación apoyan el desempeño sostenible y seguro.
Habilidades no técnicas
Se desarrollan de forma sistemática el liderazgo en materia de seguridad y las competencias no técnicas.
Conocimientos en FHO
Los factores humanos y organizativos, incluida la experiencia de primera línea, se consideran sistemáticamente durante el diseño y los cambios.

¿QUÉ ES UN SISTEMA DE REPORTE DE RIESGOS?

Un sistema de reporte o notificación confidencial de riesgos o de información relativa a la seguridad (en adelante, sistema RCR) es una estrategia (procedimiento/herramienta) que permite la recolección de datos reportados por los empleados de una entidad ferroviaria (incluyendo las contratas que trabajan para ellas) sobre eventos de riesgo, amenazas para la seguridad, peligros, condiciones inseguras, actos inseguros, errores humanos, transgresiones normativas, errores organizacionales, fallos del sistema, y cualquier circunstancia o preocupación que pueda afectar a la seguridad.

¿POR QUÉ ES NECESARIO UN SISTEMA DE REPORTE?

- Un sistema RCR es un elemento fundamental para la revisión de los sistemas de gestión de la seguridad operacional, ya que proporciona información relevante sobre su efectividad.
- Los sistemas de RCR son piezas básicas de organizaciones con una cultura de seguridad consolidada, en las que se entienden los incidentes y los sucesos no intencionados como una oportunidad para aprender y mejorar.
- Cuantas más oportunidades se tenga de captar y analizar esos riesgos, más oportunidades habrá de prevenir de forma ascendente incidentes y accidentes.
- Este conocimiento de los riesgos aportados por el RCR puede ayudar claramente a definir las estrategias de actuación, a proponer las barreras preventivas más eficaces, a comprender mejor la actuación humana, a la mejora de los procedimientos operacionales y a controlar su impacto en la seguridad.
- Es importante animar a la dirección de la empresa a dedicar recursos en la implementación de un sistema de notificación y de una cultura no punitiva, pues los resultados obtenidos en otros sectores y en otras empresas son muy convincentes, y la normativa ferroviaria como hemos visto apoya esta estrategia.
- También es importante involucrar a los trabajadores, que sientan confianza en el sistema, compartan con la dirección de la empresa el compromiso por la seguridad, superen las barreras y proporcionen información relativa a la seguridad diligentemente.

¿QUÉ CARACTERÍSTICAS ESENCIALES TIENE UN SISTEMA DE REPORTE?

En consonancia con la normativa y recomendaciones citadas anteriormente, la recopilación de datos sobre seguridad operacional ha de poner el énfasis en aquellos riesgos que se puedan identificar, reportar y evaluar para poder prevenirlos antes de que se transformen en incidentes disruptivos o accidentes.

Las características generales indican que el sistema de RCR debe ser:

1. Confidencial, por medio de la desidentificación de datos de los reportadores.
2. Gestionado de forma independiente de cualquier departamento que tenga responsabilidades disciplinarias, por un departamento independiente o incluso, por una entidad externa.
3. Apoyado con el compromiso explícito de la dirección, bajo los criterios de una política de cultura justa.
4. Integrado en el SGS de la empresa.
5. Diseñado en base a un procedimiento que defina claramente:
    - Los empleados que pueden hacer uso del sistema RCR,
    - La persona o departamento al que deben dirigirse las comunicaciones,
    - Los canales a través de los cuales deben de realizarse los reportes,
    - El contenido mínimo que deben incluir,
    - La gestión de estos reportes,
    - Los plazos para su tratamiento y, en su caso, el establecimiento de las medidas preventivas o correctoras correspondientes,
    - La retroinformación o feedback al personal sobre las lecciones aprendidas.
6. Conocido por el personal, que debería conocer sus ventajas.
7. Resultado del compromiso de toda la organización y su personal para el reporte de riesgos y la mejora de la seguridad.

Todo ello, siempre bajo la premisa:

"Toda la información recibida en el sistema de RCR se utilizará exclusivamente para fines de seguridad operacional, y se evitarán represalias o sanciones al personal por la información remitida, excepto en los casos de negligencia grave, dolo o conductas destructivas".

¿QUÉ INFORMACIÓN SE DEBE REPORTAR?

La organización debería dar la oportunidad a sus trabajadores de informar de forma voluntaria sobre cualquier elemento o suceso que, a su juicio, afecte a la seguridad de la operación (eventos de riesgo), cuasi-accidentes, estados no deseados, incidentes, errores humanos, errores organizativos, preocupaciones, infracciones normativas, o cualquier acontecimiento relacionado con la seguridad que ponga o pudiera llegar a poner en peligro la operación, a las personas, infraestructuras, material móvil y equipos.

En definitiva, se debería poder notificar cualquier elemento o suceso que a juicio del observador pueda llegar a suponer un peligro. Se deberían reportar los riesgos observados durante la operación, aunque no hayan ocasionado ningún incidente, pero que podrían provocarlo en otras circunstancias o en otro momento, así como aquellas circunstancias que por ser un error repetitivo están aumentando la probabilidad de un evento no deseado y requieren poner defensas y medidas preventivas.

Ejemplos más comunes susceptibles sobre los que informar:

- Incumplimientos de reglas.
- Errores
- Fallos al aplicar el procedimiento.
- Falta de entrenamiento o cualificación para llevar a cabo una tarea.
- Falta de información de seguridad.
- Comunicaciones inseguras.
- Fatiga.

- Defectos de diseño y ergonómicos.
- Fallos de planificación, gestión y ejecución.
- Condiciones inseguras.
- Prácticas inseguras.
- Aspectos de interacción entre personas y equipos.
- Cualquier suceso que pueda afectar a la seguridad de la operación.

Para saber si cualquiera de estas circunstancias anteriores es notificable, es fundamental el buen criterio, conocimiento y experiencia del notificador.

Se puede y debe notificar un riesgo observado tanto si el propio reportador está involucrado o afectado por el mismo, como si está involucrado o afectado otro personal. Sin embargo, no se deben notificar circunstancias que no han sido observadas directamente por el reportador. Por ejemplo, algo que ha oído o le ha sido comentado por otras personas.

Los sistemas para la notificación voluntaria no deben sustituir a los sistemas reglamentarios de comunicación de riesgos inminentes o urgentes.

Sin embargo, es importante recalcar que el uso del sistema de RCR no sustituye otros cauces establecidos para la comunicación de que pueda haber en la organización, ya sean de uso obligatorio, reglamentario o potestativo, como, por ejemplo:

- los sistemas para comunicación de accidentes.
- los cauces para la comunicación de riesgos inminentes entre empresas ferroviarias y administradores de infraestructuras.
- los cauces para la formulación de denuncias.

También debe recordarse al personal que no se debe reportar durante la operación, sino que se deben aprovechar los descansos o a la salida del turno.

¿QUIÉN PUEDE USAR ESTOS SISTEMAS DE NOTIFICACIÓN?

Los sistemas para la notificación voluntaria deberían alentar la participación de todos los trabajadores.

Dado que esta información es vital para la gestión de riesgos de una organización, todas las personas empleadas en la empresa, en todas las áreas (gerenciales, mandos intermedios, áreas operativas, áreas de mantenimiento…), deberían estar en disposición de informar sobre los sucesos y riesgos observados que puedan afectar a la seguridad. También deberían estarlo las personas que de forma indirecta o mediante contratas tengan relación con las tareas que puedan afectar el riesgo de una operación.

El único requisito para poder notificar debería ser estar dado de alta en el sistema con perfil de notificador o reportador, incluyendo a empleados de la organización ferroviaria, trabajadores de contratas vinculados a la operación y el mantenimiento, responsables de la infraestructura y mantenimiento, y personas vinculadas en el diseño y fabricación.

Habitualmente existen tres niveles de participación en los sistemas de reporte de riesgos. En el nivel 1, el más usual, donde reportan los empleados de la empresa. En un nivel 2, pueden enviar reportes los empleados de contratas y otras empresas vinculadas a la operación, y en un nivel 3, podrían recibirse observaciones de riesgos o peligros externos del sistema, como los comunicados por otros usuarios, incluidos los pasajeros.

Además, es necesario prever que al sistema puedan incorporarse notificaciones procedentes de los sistemas de notificación de otras entidades, especialmente para la gestión de riesgos compartidos.

Aunque debe hacerse un esfuerzo divulgativo importante dentro de la organización para que esta situación no se presente, también es posible que, en algunos casos, se tengan que incorporar comunicaciones internas pero que no empleen los cauces oficiales de reporte, cuando sean suficientemente relevantes. En esos casos, conviene informar al notificador de que tiene disponible un sistema de notificación establecido y que, si no lo emplea, corre el riesgo de que su información no llegue correctamente y no pueda ser tratada de manera adecuada.

Por tanto, para alentar la participación, es necesario elaborar estrategias de promoción y marketing, mediante la realización de acciones de capacitación y motivación, al inicio de la implantación del sistema de RCR y de forma periódica. Las personas usuarias deben saber claramente cómo y qué reportar en todo momento, y el sistema ha de garantizar siempre la confidencialidad.

Algunas ideas para esta estrategia de promoción podrían ser: folletos, carteles, videos, seminarios, reuniones, difusión en el transcurso de las acciones de formación, comunicaciones en los comités de seguridad, recordatorios en la web o por mail, concursos y premios de seguridad, etc.

Realizar y mantener acciones de promoción y sensibilización del sistema RCR es una pieza fundamental para el éxito de su implantación en la empresa.

ALGUNAS SUGERENCIAS EN EL DISEÑO DE UN SISTEMA DE REPORTE

Uno de los principios básicos a la hora de diseñar un sistema de RCR debe ser el de **facilidad de empleo para el usuario.** Realizar una notificación sobre un posible riesgo que se acaba de observar en el desarrollo de sus funciones, debería ser una tarea fácil y rápida, mediante tecnologías amigables, que consuma poco tiempo y esfuerzo.

Los canales habituales para la notificación de riesgos son hoy día mayoritariamente electrónicos, normalmente sistemas web basados en internet, o bien herramientas tipo app para teléfonos móviles que no requieran conexión a internet permanente.

Ahora bien, como el objetivo primordial es facilitar y motivar lo más posible la notificación de riesgos, en función del tamaño de la empresa y su estructura, podrían llegar a ser admisibles otros medio como el correo electrónico, los mensajes SMS, o, incluso, a través de atención en persona o por teléfono, siempre y cuando se aseguren los requisitos imprescindibles de **posibilidad de anonimizar la información y que quede un registro y evidencias de la notificación**.

En todo caso, el formulario de notificación debe ser muy sencillo, buscando siempre la agilidad del proceso de reporte. Siempre que sea posible, para facilitar esta notificación y su posterior gestión y

tratamiento de la información, debe ofrecerse **una taxonomía de los sucesos** o hechos sobre los que se informa. A pesar de ello, hay que tener en cuenta que, en ocasiones, información no clasificable, a pesar de las dificultades para su gestión posterior, también puede ser de interés. Por ello, las entidades deberían valorar si es conveniente disponer de campos abiertos en los que completar la información tabulada conforme a las categorías prestablecidas. En cualquier caso, si se opta por una clasificación conforme a taxonomías, el modelo debe ser suficientemente flexible para permitir su revisión periódica y adaptación a las sugerencias recibidas.

El diseño de la aplicación debe ser intuitivo, fácil de comprender y de manejar, basado en iconografía reconocible por el usuario, y con la información estructurada en un árbol lógico de "comprobar y clicar", que permita la utilización de recursos, como adjuntar fotos, documentos, comentarios, etc.

La información a incorporar por el usuario, se puede agrupar en bloques:

- **¿Quién?** – Aunque los datos del informante tienen que poder ser eliminados en el momento de pasar a la unidad encargada de su gestión, la notificación debe incluir esta información para permitir enviarle al informante un acuse de recibo o, incluso, ponerle en conocimiento de eventuales medidas tomadas como resultado de su sugerencia. Sin embargo, como la confidencialidad es un principio básico, el sistema debe guardar esta información de manera separada al resto de la notificación (por ejemplo, generándose un código interno, completamente "opaco" para la organización que relacione informante y notificación).

- **¿Cuándo?** - Se enmarca temporalmente la observación del riesgo. Los sistemas electrónicos toman por defecto automáticamente la fecha y la hora actual, pero el reportador puede modificarlos en caso necesario.

- **¿Dónde?** - Es aconsejable ubicar el lugar de la observación del riesgo. Los sistemas basados en móviles pueden incluso geolocalizar automáticamente por medio del GPS el lugar exacto en el caso de que la notificación se pueda realizar en el momento del suceso, aunque esto no debería ser lo más habitual. Además, se pueden acompañar fotografías de apoyo.

- **¿Qué?** – Se debe indicar el peligro o error observado, la operación, la tarea y la descripción de lo observado. El sistema debe ayudar a realizar esta función de una manera ágil e intuitiva.

- **¿Por qué?** - En este apartado se puede añadir información de apoyo si se estima conveniente, los factores que han influido en el riesgo, fotos, esquemas, documentos, u observaciones.

Todas las comunicaciones recibidas y enviadas por el sistema deben quedar registradas para permitir su auditoría tanto interna, como externa, por ejemplo, de la AESF.

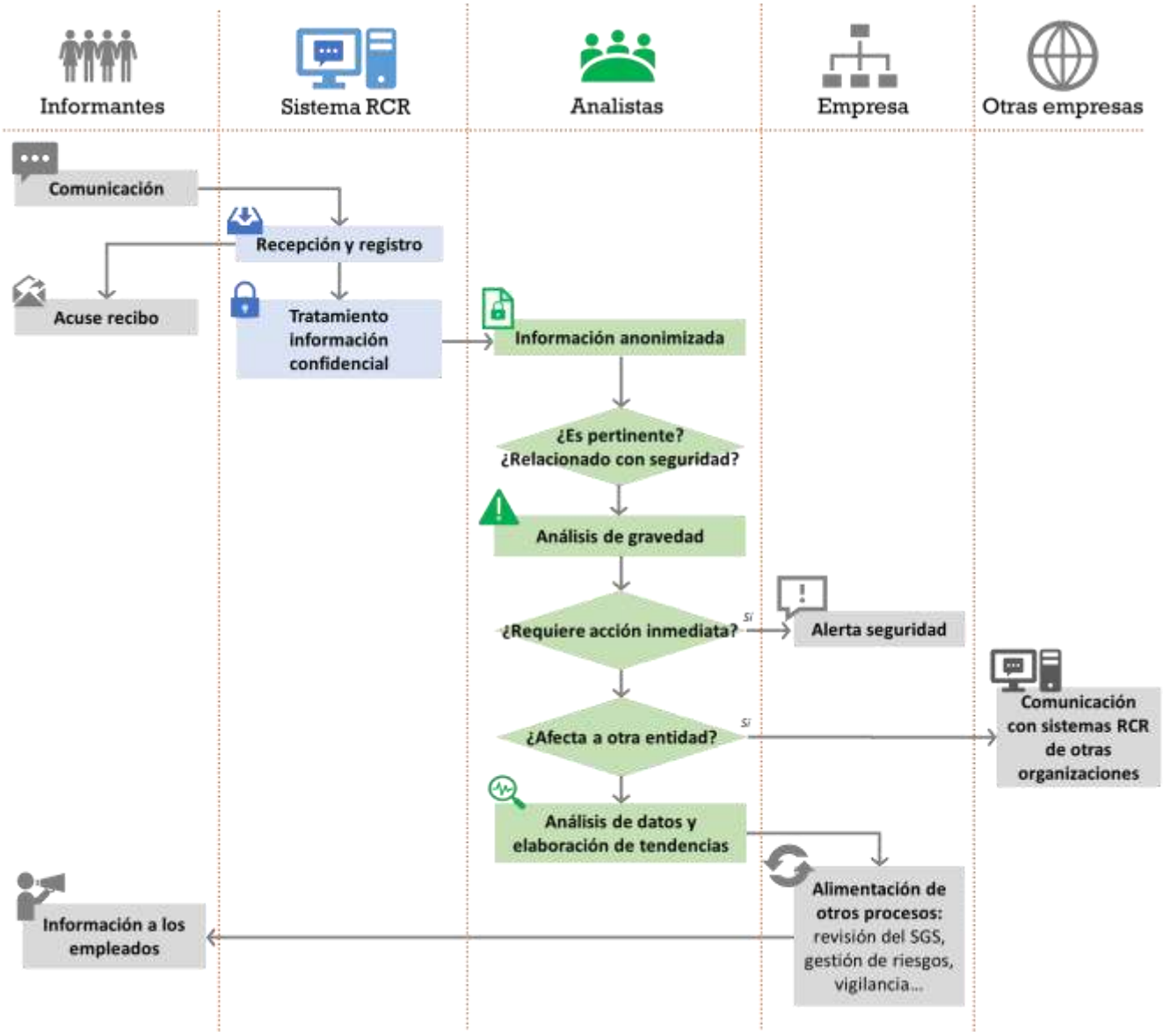
¿QUIÉN ANALIZA Y GESTIONA LOS REPORTES DEL RCR?

Un sistema de RCR no es eficaz si no hay una estructura encargada del análisis de la información recibida a través de él.

Paralelamente al sistema de notificación tiene que haber **una estructura suficientemente potente, encargada de analizar y gestionar la información recibida**.

Este grupo de analistas, una vez recibida la información anonimizada del sistema RCR debe ser capaz de:

- Discernir si la información comunicada es realmente relevante a efectos de seguridad operacional o no, descartando comunicaciones no válidas (notificaciones falsas o infundadas, comunicaciones no relacionadas con la seguridad, informaciones incompletas…).
- Valorar el nivel de gravedad de la notificación y si requiere un tratamiento inmediato, derivándola a los cauces prestablecidos para alertas de seguridad. Aunque el sistema RCR no debe ser el sistema empleado para este tipo de comunicaciones, no siempre será posible evitar que llegue este tipo de reportes.
- Decidir si es una información que trasciende a la entidad y puede ser interesante para otras empresas, para lo cual se debe derivar la información relevante a otros sistemas RCR de otras entidades o a través de otros organismos de coordinación.
- Realizar un análisis de datos y de tendencias que puedan servir de alimentación de otros procesos de mejora continua de la organización.



Este análisis y tratamiento de toda la información, la elaboración de estadísticas, indicadores y tendencias, etc., se deben realizar por personal especializado, suficientemente cualificado y bajo estrictas medidas de confidencialidad. El grupo de analistas debe asegurar algunos requisitos como:

- Independencia dentro de la organización.
- Conocimientos del sistema ferroviario y de la operación en general y de los procedimientos internos de la propia entidad incluidos en su SGS.
- Conocimientos de factores humanos y organizativos.
- Capacidad de análisis y espíritu crítico.

Una buena práctica es que los analistas y responsables del sistema RCR puedan mantener encuentros con otras empresas para compartir experiencias sobre la aplicación de sistema análogos.

Los analistas podrán ser de la propia empresa, o, incluso expertos externos en el caso de que la empresa prefiera contar con un sistema RCR independiente y externalizado que realice algunas de las fases del proceso. Sin embargo, en este último caso, habrá que disponer de medidas complementarias que permitan asegurar el conocimiento real de la organización, que puede perderse en el caso de analistas completamente externos.

Todo el funcionamiento del sistema de reporte confidencial de riesgos RCR, junto con la actividad del grupo de análisis, debería estará integrado en los procedimientos del SGS. En especial, el SGS debería aportar criterios de toma de decisiones para el grupo de análisis de la información del sistema RCR.

EL RCR Y LOS CRITERIOS DE CULTURA DE SEGURIDAD Y CULTURA JUSTA

Cualquier sistema de notificación de riesgos debe estar desarrollado bajo los paraguas conceptuales de "**cultura de seguridad y cultura justa",** por lo que se evitará en todo momento:

a) la identificación de los notificadores

b) la estimación de culpa o sanción, salvo dolo o imprudencia temeraria.

Sería contradictorio un sistema orientado a la penalización cuando el objetivo principal de estos sistemas es el autoaprendizaje como organización y la colaboración.

Por tanto, como regla general, no se aplicarán acciones disciplinarias por acciones o infracciones involuntarias que hayan sido reportadas, salvo casos de dolo, culpa o negligencia grave. Ahora bien, "cultura justa" no quiere decir "cultura de la impunidad". Por ello, tienen que estar claros los criterios para separar lo aceptable de lo no aceptable (dolos, culpas y negligencias graves) en las conductas relacionadas con la seguridad. Los métodos como el **diagrama de decisión** y el test de sustitución pueden ser una herramienta adecuada.

Todo el sistema debe estar elaborado en forma de procedimiento lo suficientemente claro para todo el personal. Un sistema ambiguo crea desconfianza.

El compromiso de la dirección de la empresa es la pieza clave en todos los sistemas RCR. Si existe un apoyo explícito de la gerencia, está descrito en el SGS dentro de la política de la empresa, y la

dirección se preocupa de hacer un seguimiento de su funcionamiento, la eficacia del sistema RCR está asegurada.

LA PROTECCIÓN DEL REPORTADOR

Bajo la premisa de que la información sobre riesgos operacionales no debe ser utilizada para fines distintos para los que fue registrada, el sistema RCR deberá establecer dos niveles de protección de datos:

- Por un lado, la integridad de la información recibida y,
- Por otro lado, la de los datos de los informantes. En este caso, esta información debe preservarse especialmente, para crear confianza en la confidencialidad del sistema.

Se debe asegurar la confidencialidad mediante la encriptación de la procedencia de la información, o por medio de la desidentificación de los datos del reportador antes de su distribución a los equipos de analistas o al resto de la organización.

Pese a lo anterior, puede ser conveniente que en los sistemas RCR se solicite permiso al reportador, así como datos de contacto, para poder ampliar información sobre la información enviada, siempre asegurando la privacidad.

Se deben implementar acuerdos para asegurar el cumplimiento del deber de reserva por parte de las empresas, o la entidad encargada de custodiar esta información. Estos acuerdos para la protección de la información recibida de los reportadores, serán posible siempre que impere en las organizaciones ferroviarias un clima de confianza, y que la información notificada se emplee únicamente para mejorar la seguridad.

Se puede considerar mal uso de la información recibida en el sistema RCR, entre otra, la utilización de la misma en procesos disciplinarios, o la revelación de datos personales de los reportadores, con la excepción de las conductas temerarias, negligencias graves o actos dolosos. Por lo tanto, cuando se aprecie indicadores fiables de dolo o negligencia grave en la conducta reportada y solo en ese caso, podrá aplicarse la desprotección de la información del sistema RCR.

Además, hay que tener en cuenta que, en casos de negligencias graves, que pudiera ser consideradas delitos, podría ser requerida la información por parte de jueces y fiscales, en la posibilidad de aplicación de procedimientos penales.

LECCIONES APRENDIDAS Y FEEDBACK

Reportar riesgos exige tiempo, compromiso y una actitud proactiva con la seguridad, además de salvar las barreras de la confianza en el sistema. Por ello, el reportador debería tener algún tipo de reconocimiento, recibir información de las mejoras conseguidas y agradecerle su participación.

El modelo implantado para reportar riesgos debería devolver información al usuario de forma inmediata, como un refuerzo de conducta y una demostración de que la organización valora el esfuerzo y el compromiso del informante.

Esta primera comunicación con el informante puede incluir, por ejemplo, si se ha recibido el reporte correctamente, el tratamiento que se va a realizar a partir de ese momento con la información reportada, etc.

Posteriormente, una vez que se ha tratado la información recibida en el sistema, también es una buena práctica compartir con los trabajadores las conclusiones alcanzadas mediante los boletines digitales de información, lecciones aprendidas, pequeñas píldoras formativas e informativas, mensajes de prevención, análisis de sucesos, tendencias o estadísticas, etc.

Todo ello con independencia de que la información que el RCR aporta a los gestores del SGS será clave para definir las medidas preventivas sobre los principales riesgos reportados por los empleados. Para ello, las conclusiones de la información obtenida en el sistema de notificación alimentarán los sistemas de mejora continua:

- En la revisión de los procedimientos del SGS (por ejemplo, para implantar medidas mitigadoras en la ejecución de algunas operaciones) o de la propia organización.
- Sirviendo de base para la gestión de riesgos (por ejemplo, detectando amenazas que deberían incorporase en el registro de peligros de la entidad).
- Como punto de partida de la vigilancia interna (por ejemplo, orientando sobre la necesidad de realizar acciones de vigilancia o inspección sobre determinadas operaciones o de establecer planes de acción concretos).
- Durante las acciones formativas y de reciclaje del personal.
- En la revisión de las estrategias de fomento de cultura de seguridad de la organización.
- Incluso, puede servir para extraer conclusiones para mejorar el propio sistema RCR, por ejemplo, a través de cambios en la taxonomía de sucesos