

## CULTURA JUSTA

Este material guía surge como necesidad en el ámbito de la Comisión de Estudio SMS. Su objetivo es proporcionar una serie de pautas para el establecimiento, por parte de la alta dirección de los operadores aéreos, de su política de cultura justa.

Ámbito de Aplicación <sup>1</sup>	
<b>Aeronavegabilidad:</b>	No afecta directamente
<b>Operaciones:</b>	Afecta
<b>Licencias al Personal:</b>	No afecta directamente
<b>Navegación Aérea:</b>	No afecta directamente
<b>Aeropuertos:</b>	No afecta directamente
<b>Otros:</b>	No afecta directamente

## 1. INTRODUCCIÓN

Las organizaciones no son inmunes a las consideraciones culturales. Esto adquiere particular relevancia en el ámbito de la seguridad operacional, donde la gestión efectiva requiere un compromiso real con la seguridad operacional por parte de todos y cada uno de los miembros de una organización, y la prioridad de la seguridad operacional debe manifestarse en las actitudes, comportamientos, decisiones y modos de operación en todos los ámbitos de la organización.

La cultura de seguridad operacional se presenta como un catalizador que tiene una influencia significativa en la integración y evolución de los elementos del Sistema de Gestión de la Seguridad Operacional (Safety Management System – SMS). Es más, el éxito del Sistema de Gestión de la Seguridad Operacional depende, en gran medida, del desarrollo de una cultura de seguridad operacional positiva y preventiva, siendo la mejora de la seguridad operacional clave para el desarrollo sostenible del sector aéreo. Desde la alta dirección de la organización, apoyándose en el departamento de seguridad operacional, es necesario proporcionar una atmósfera de confianza en la que todos los empleados sean animados a proporcionar información relevante y esencial de seguridad operacional y sepan reconocer los criterios para establecer la frontera de lo aceptable e inaceptable.

La potencial disparidad entre lo que se dice sobre la seguridad operacional y lo que realmente se hace está remarcada por lo que creen las personas sobre cómo su organización valora la seguridad operacional, lo que afecta a su propio comportamiento y decisiones y, por tanto, a los auténticos resultados relativos a la seguridad operacional.

Para entender la cultura de seguridad operacional, es necesario entender el significado del concepto de cultura organizacional. OACI, en el doc. 9859 *“Manual de gestión de la seguridad operacional (SMM)”*, define la **cultura organizacional** como *“las características y percepciones de seguridad operacional entre miembros que interactúan dentro de una entidad particular”*. Se trata, por tanto, de un sistema de

<sup>1</sup> Lo indicado en esta Circular Informativa es de aplicación a todos los ámbitos aunque haya surgido como necesidad en la Comisión de Estudio SMS.

valores y creencias compartidas acerca de cómo se hacen las cosas en una organización, y dondequiera que se trabaje, se estará inmerso en una cultura organizacional.

La **cultura de seguridad operacional** es, por tanto, una parte de la **cultura organizacional**, que podría definirse como la forma en que se hace seguridad operacional en la organización, resaltando que se refiere a la realidad de la seguridad operacional y no necesariamente a lo que la gente dice que se debería hacer; es decir, “cómo una organización se comporta en el ámbito de la seguridad operacional cuando nadie mira”. El grupo SM ICG define en su guía sobre “*Terminología de la Gestión de la Seguridad Operacional*” la cultura de seguridad operacional como:

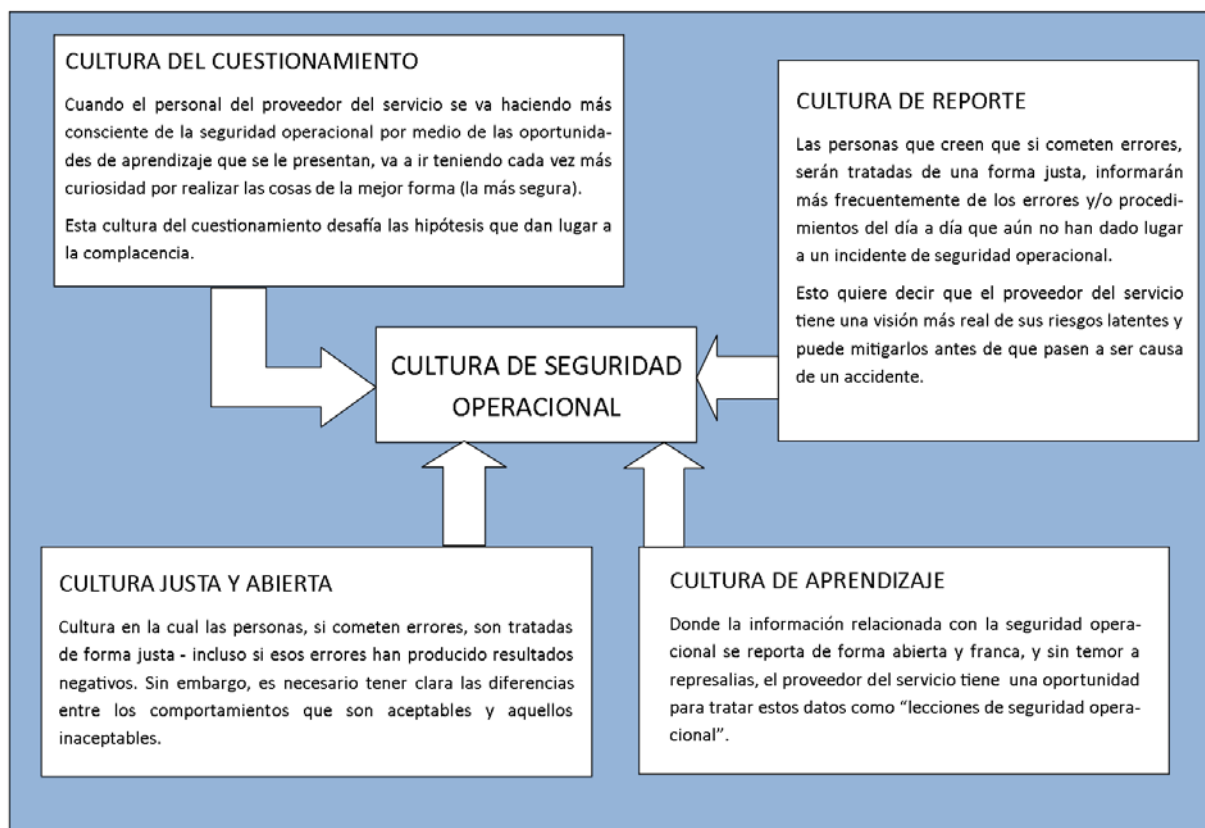
***Conjunto duradero de valores, normas, actitudes y prácticas de una organización preocupada por minimizar la exposición de los trabajadores y del público en general a condiciones peligrosas o con riesgos. En una cultura positiva de seguridad se promueve una preocupación, compromiso y obligación de rendición de cuentas en materia de seguridad operacional compartidas.***

En otras palabras, la cultura de seguridad operacional es la forma en que la seguridad operacional es percibida, valorada y priorizada en una organización.

La cultura de seguridad operacional está relacionada con los sistemas de gestión y de supervisión, y también con la conducta de las personas en su trabajo, resaltando la contribución de cada individuo en todos los ámbitos de la organización, y se refleja en la disposición de la organización para desarrollarse y aprender de los **errores, incidentes y accidentes**.

Asimismo, una buena cultura de seguridad operacional ayuda a arraigar las buenas prácticas y comportamientos relativos a la seguridad operacional. Una cultura de seguridad operacional robusta **empieza con el compromiso de la dirección de hacer de la seguridad operacional una prioridad en cada decisión**. La creencia de que la seguridad operacional no es una prioridad da lugar a actitudes que influyen en las acciones y decisiones de las personas, dando lugar a condiciones inseguras, que conducirán a acciones inseguras y, finalmente, a incidentes y accidentes.

Uno de los pilares claves en los que la cultura de seguridad operacional se asienta es en la “**cultura justa**” (ó Just Culture en inglés).



El Reglamento (UE) nº 376/2014 del Parlamento europeo y del Consejo de 3 de abril de 2014 la define como:

***Aquella en la que no se castigue a los operadores y demás personal de primera línea por sus acciones, omisiones o decisiones cuando sean acordes con su experiencia y capacitación, pero en la cual no se toleren la negligencia grave, las infracciones intencionadas ni los actos destructivos.***

La cultura justa depende fundamentalmente de que esté perfectamente claro y aceptado por todos los individuos de la organización **quién toma la decisión y con qué metodología se toma** a fin de determinar si la conducta que ha dado lugar a un acto inseguro es o no aceptable. Siempre existirá un área "gris" entre los dos extremos, lo indiscutiblemente aceptable e inaceptable, dónde habrá que determinar caso por caso, la responsabilidad de la conducta que se juzga. Aquí es dónde esta guía tiene el objetivo de ser eficaz y encuentra su verdadero valor.

Varias organizaciones y operadores aéreos han afrontado el proceso de implantar la cultura de seguridad operacional dentro de su estructura, y el resultado común aceptado es que una mínima parte de las acciones que han ocasionado una situación no deseada, o perjudicial para la organización, se han considerado como conductas gravemente negligentes o intencionadas, y por tanto punibles. Este dato significa, al menos en principio, que la mayoría de los actos inseguros se pueden reportar sin miedo a una posible sanción.

Una vez que se ha establecido esta confianza fundamental dentro de la organización, ésta comenzará a tener una apropiada cultura de reporte.

El cambio de la “cultura de buscar el culpable” a una más constructiva “cultura justa” tendrá beneficios tangibles que contribuirán positivamente a la cultura de seguridad operacional de una organización haciendo evidentes dos conceptos fundamentales y no mutuamente excluyentes: que el error humano es inevitable y consecuentemente el sistema (la organización) necesita vigilarse y mejorarse para asumir y resistir a esos errores sin que escalen y produzcan consecuencias indeseadas, y que los individuos de la misma son responsables de sus acciones siempre que conscientemente violen los procedimientos o políticas de seguridad operacional establecidos.

Una cultura justa contribuirá no sólo a aumentar el reporte de las incidencias y de los peligros, especialmente aquéllos que nunca se hubieran reportado, sino que permitirá identificar las tendencias que nos llevan a localizar las amenazas latentes de seguridad operacional y atajarlas a tiempo.

Todo sistema efectivo de información depende fundamentalmente de la participación voluntaria de los individuos que lo componen, de las personas que están en la “primera línea”, expuestas directamente a los peligros que amenazan la seguridad operacional: pilotos, tripulantes de cabina de pasajeros, técnicos de mantenimiento, personal de agentes de handling, etc., y para conseguir que estas personas reporten se requiere un clima en el que cualquiera pueda reportar sin temor sus errores y las incidencias y peligros que encuentre en la realización de su tarea.

## **2. OBJETO**

El objeto de este documento es presentar una guía sobre la cultura justa, su definición, implantación así como sus características principales dentro del sistema de la aviación. Además se ha incluido el marco legislativo en España, el cual establece los principios que rigen la cultura justa del Estado español y de las organizaciones de aviación civil.

## **3. PERSONA O EMAIL DE CONTACTO PARA CONSULTAS**

Esperanza Herraiz Monseco, e-mail: [ehmonseco@seguridadaerea.es](mailto:ehmonseco@seguridadaerea.es)

## **4. PERIODO DE VALIDEZ O FORMA DE CANCELACIÓN**

El período de validez será desde su publicación en la página web de AESA hasta su cancelación. La cancelación se producirá al darla de baja en la página web.

## 5. MARCO NORMATIVO SOBRE LA PROTECCIÓN DE LA INFORMACIÓN DE SEGURIDAD OPERACIONAL

### 5.1 POSICIÓN DE OACI

El Anexo 19 de la OACI especifica:

---

#### 5.3 Protección de datos sobre seguridad operacional

*Nota.— El Adjunto B contiene orientación jurídica para la protección de la información obtenida por medio de sistemas de recopilación y procesamiento de datos sobre seguridad operacional<sup>2</sup>.*

5.3.1 Los **sistemas de notificación voluntaria de incidentes** serán sin aplicación de sanciones y protegerán las fuentes de la información.

*Nota 1.— Un entorno sin aplicación de sanciones es fundamental para la notificación voluntaria.*

*Nota 2.— Se alienta a cada Estado a facilitar y promover la notificación voluntaria de acontecimientos que podrían afectar a la seguridad operacional de la aviación, armonizando sus leyes, reglamentos y políticas aplicables, según sea necesario.*

*Nota 3.— El Manual de gestión de la seguridad operacional (SMM) (Doc 9859) contiene orientación relativa a los sistemas de notificación de incidentes, tanto obligatoria como voluntaria.*

5.3.2 **Recomendación.**— *Los Estados no deberían proporcionar o utilizar los datos sobre seguridad operacional a los que se hace referencia en 5.1 o 5.2 para fines distintos de aquellos que se relacionan con la seguridad operacional, a menos de que, en casos excepcionales, la autoridad competente determine que, de acuerdo con su legislación nacional, la ventaja de su divulgación o uso, en cualquier circunstancia particular, supera las repercusiones negativas que dicha acción pueda tener en la seguridad operacional de la aviación.*

---

Es más, el propósito del Adjunto B es asistir a los Estados en la promulgación de sus leyes y reglamentos nacionales para proteger la información obtenida de los sistemas de recopilación y procesamiento de datos sobre seguridad operacional (o *Safety Data Collection and Processing Systems* -SDCPS- de sus siglas en inglés), permitiendo al mismo tiempo la administración apropiada de la justicia. El objetivo consiste en impedir que se haga un uso inapropiado de la información recopilada exclusivamente con la finalidad de mejorar la seguridad operacional de la aviación. Por uso inapropiado se entiende la utilización de la información sobre seguridad operacional para fines diferentes de aquéllos para los que fue recopilada — es decir, el uso de la información para

---

<sup>2</sup> **Información sobre seguridad operacional** se entiende aquella que figura en los SDCPS, ha sido establecida con el propósito exclusivo de mejorar la seguridad operacional de la aviación y reúne los requisitos para ser protegida en condiciones específicas de acuerdo con 5.3.1.

**SDCPS** (*Safety Data Collection and Processing Systems*) se refiere a los sistemas de procesamiento y notificación, a las bases de datos, a los esquemas para intercambio de información y a la información registrada, y comprende:

- 1) registros relativos a las investigaciones de accidentes e incidentes, como se describe en el Anexo 13, Capítulo 5;
- 2) sistemas de notificación obligatoria de incidentes, como se describe en el Capítulo 5, 5.1 de este Anexo;
- 3) sistemas de notificación voluntaria de incidentes, como se describe en el Capítulo 5, 5.1 de este Anexo; y
- 4) sistemas de auto-notificación, incluidos los sistemas automáticos de captura de datos, según se describe en el Anexo 6, Parte I, Capítulo 3, así como sistemas manuales de captura de datos.

procedimientos disciplinarios, civiles, administrativos y criminales contra el personal de operaciones y/o la revelación de información al público, salvo que se aplique alguno de los principios de excepción recogido en el punto 4 de dicho Adjunto.

El propio Adjunto B contiene principios de excepción respecto de la protección de la información ante conductas temerarias, negligencias graves o actos dolosos.

**Es necesario aclarar que aunque OACI, de momento, solamente ha establecido requisitos para proteger los sistemas de notificación voluntaria de incidentes, en Europa se han establecido requisitos para proteger ambos sistemas, tanto el obligatorio como el voluntario.**

## **5.2 POSICIÓN DE LA UNIÓN EUROPEA**

En cuanto a la posición europea, la regulación en este ámbito establece:

- **El Reglamento (UE) Nº 996/2010** del Parlamento europeo y del Consejo de 20 de octubre de 2010 sobre investigación y prevención de accidentes e incidentes en la aviación civil y por el que se deroga la Directiva 94/56/CE, en su artículo 14, regula la protección de la información sensible en materia de seguridad.
- **El Reglamento (UE) Nº 376/2014** del Parlamento europeo y del Consejo de 3 de abril de 2014 relativo a la notificación de sucesos en la aviación civil, que modifica el Reglamento (UE) nº 996/2010 del Parlamento Europeo y del Consejo, y por el que se derogan la Directiva 2003/42/CE del Parlamento Europeo y del Consejo y los Reglamentos (CE) nº 1321/2007 y (CE) nº 1330/2007 de la Comisión<sup>3</sup>. Son de interés los artículos 15, confidencialidad y uso adecuado de la información, y 16, protección de las fuentes de información. En concreto el artículo 16 establece en el punto 10:

---

*Artículo 16. Protección de las fuentes de información.*

*10. La protección prevista en los apartados 6, 7 y 9 del presente artículo no se aplicará en cualquiera de las situaciones siguientes:*

*a) En los casos de conducta indebida deliberada;*

*b) Cuando se haya producido una omisión manifiesta, importante y grave del deber de diligencia ante un riesgo evidente y una falta profesional grave a la hora de prestar la diligencia que evidentemente se requiere en esas circunstancias, dando lugar a daños previsibles a personas o bienes o que comprometan gravemente el nivel de la seguridad aérea*

---

- **Directiva 2003/42/CE** del Parlamento europeo y del Consejo de 13 de junio de 2003 relativa a la notificación de sucesos en la aviación civil. Esta Directiva se transpuso al ordenamiento jurídico español mediante el **Real Decreto 1334/2005**, de 14 de noviembre, por el que se establece el sistema de notificación obligatoria de sucesos en la aviación civil. Dejará de ser aplicable una vez sea aplicable el Reglamento (UE) nº 376/2014, el 15 de noviembre de 2015. El Artículo 8 del citado Real Decreto establece:

---

<sup>3</sup> El Reglamento será aplicable a partir del 15 de noviembre de 2015, y no antes de la entrada en vigor de las medidas de ejecución contempladas en el artículo 4, apartado 5.

---

*Artículo 8. Protección de la Información.*

*1. La Dirección General de Aviación Civil adoptará las medidas que a continuación se relacionan para garantizar la confidencialidad adecuada de la información.*

*a) En la base de datos prevista en el artículo 5 no se registrarán nombres o direcciones de personas concretas. Así mismo, en ningún caso se divulgará información que contenga datos técnicos que puedan llevar a identificar al notificador o a terceros, tales como el indicativo de vuelo afectado y la matrícula de la aeronave.*

*b) El personal de la Dirección General de Aviación Civil, y aquel otro que pueda acceder al sistema de notificación de sucesos, deberá guardar el debido sigilo respecto de los sucesos que conozcan por razón de su cargo, así como respecto de hechos, datos o informes que conozcan en el ejercicio de sus funciones.*

*c) La Dirección General de Aviación Civil se abstendrá de entablar procedimientos en relación con infracciones culposas o a título de simple negligencia que hayan llegado a su conocimiento sólo por haber sido notificadas en virtud del sistema nacional de notificación obligatoria de sucesos, **excepto** en casos de notificaciones que revelen de forma manifiesta que el suceso se ha producido con **dolo** o **negligencia grave**.*

*d) Los organismos competentes velarán para que los empleados que notifiquen sucesos de los cuales puedan tener conocimiento no sufran ningún perjuicio por parte de su empleador.*

*2. Este artículo se aplicará sin perjuicio de las normas relacionadas con el acceso a la información por los órganos judiciales o del Ministerio Fiscal para la investigación y persecución de delitos o cuando lo soliciten las comisiones parlamentarias de investigación a que se refiere el artículo 76 de la Constitución.*

---

El **Real Decreto 1334/2005** está en línea con los principios de “Cultura Justa” de la Unión Europea según los cuales no debería realizarse ninguna acción contra los individuos u organizaciones excepto en los casos de dolo o negligencia grave.

### **5.3 POSICIÓN ESPAÑOLA**

Además del **Real Decreto 1334/2005**, la **Ley 21/2003**, de 7 de julio, de Seguridad Aérea en su artículo 12 regula la protección de la información y del notificante salvo en caso de dolo o negligencia grave. En concreto:

---

**Artículo 11. Programa Estatal de Seguridad Operacional para la Aviación Civil.**

1. ....

*La información sobre seguridad operacional facilitada voluntariamente en la que no se aprecie dolo o negligencia grave no podrá utilizarse como medio de prueba válido para cualquier tipo de procedimiento administrativo, ni podrá revelarse al público, salvo lo dispuesto en el artículo 19, con el fin de asegurar la continua disponibilidad para poder tomar medidas preventivas adecuadas y oportunas.*

2. ...

*Para la aprobación del Programa Estatal de Seguridad Operacional se deberá tener en cuenta como principio básico la protección sobre la información de Seguridad Operacional con el fin de que esta no se utilice de forma inapropiada.*

**Artículo 12. Protección de la información del Programa Estatal de Seguridad Operacional para la Aviación Civil.**

*1. Los organismos, órganos, entes y entidades del sector público a que se refiere el artículo 11.3, primer párrafo, utilizarán la información facilitada por los proveedores de servicios y productos aeronáuticos en el marco del Programa a los exclusivos efectos de prevenir, evaluar los riesgos para la seguridad y mejorar los niveles de seguridad operacional. Así mismo, dichos obligados se abstendrán de adoptar cualquier tipo de*

*medida desfavorable como consecuencia de dicha información o de incorporarla a procedimientos ya iniciados, salvo que conste de forma manifiesta que las actuaciones realizadas se han producido con **dolo o negligencia grave**.*

*Lo dispuesto en el párrafo anterior no obsta para que se utilice el resultado de los análisis de la información facilitada en el marco del citado Programa para orientar la inspección aeronáutica hacia las áreas que requieran mayor prevención.*

*2. Los empleados, civiles y militares, de los proveedores de servicios y productos aeronáuticos obligados por el Programa que informen sobre accidentes, sucesos, deficiencias de seguridad, o amenazas con afección, real o potencial, sobre la seguridad operacional, no podrán sufrir, por el hecho de informar, efectos adversos en su puesto de trabajo por parte del empleador, público o privado, **salvo** en los supuestos en que se acredite **mala fe en su actuación**.*

*Se entenderán nulas y sin efecto legal alguno las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a lo señalado en el párrafo anterior.*

*3. Lo dispuesto en el apartado 1 será aplicable a las medidas preventivas adoptadas por los proveedores de servicios y productos aeronáuticos en el marco de sus sistemas de gestión de la seguridad operacional o mecanismos equivalentes habilitados conforme a lo previsto en el artículo anterior.»*

#### **Artículo 18. Carácter reservado de la información.**

*1. Los datos, registros, grabaciones, declaraciones, comunicaciones, indicadores e informes facilitados en el marco del Programa Estatal de Seguridad Operacional para la Aviación Civil por los profesionales aeronáuticos y proveedores de servicios y productos aeronáuticos a los organismos, órganos, entes y entidades del sector público a que se refiere el artículo 11.3, párrafo primero, tienen carácter reservado y sólo pueden ser utilizados para los fines previstos en él.*

*El deber de reserva en relación con la información obtenida en la investigación técnica de los accidentes o incidentes en la aviación civil se regirá por lo previsto en el Reglamento (UE) n.º 996/2010 del Parlamento Europeo y del Consejo, de 20 de octubre de 2010.*

*En todo caso, la información a que se refieren los párrafos anteriores se recaba con la única finalidad de reforzar la seguridad operacional y prevenir futuros accidentes e incidentes, y no con la finalidad de determinar culpas o responsabilidades.*

#### **Artículo 19. Cesión o comunicación de la información.**

*1. La información a la que se refiere el artículo 18.1 sólo podrá ser comunicada o cedida a terceros en los casos siguientes:*

*a) Cuando sea requerida por los órganos judiciales o el Ministerio Fiscal para la investigación y persecución de delitos.*

*La Comisión de Accidentes e Incidentes de Aviación Civil remitirá la información necesaria, limitándose a facilitar los antecedentes que obren en su poder en relación a los factores contribuyentes que hayan provocado un accidente o incidente aéreo. La identificación de los factores no implica la asignación de la culpa o la determinación de la responsabilidad, civil o penal.*

*b) Cuando lo soliciten las Comisiones parlamentarias de investigación a que se refiere el artículo 76 de la Constitución. Los miembros de la Comisión de investigación que reciban la información vendrán obligados a mantener su reserva.*

*El Director de la Agencia Estatal de Seguridad Aérea podrá solicitar motivadamente que las sesiones de dichas Comisiones parlamentarias se declaren secretas.*

*c) Cuando la Agencia Estatal de Seguridad Aérea actúe en cumplimiento de deberes de colaboración establecidos en normas internacionales, comunitarias o nacionales, bajo la exigencia de recíproca confidencialidad.*



*d) Cuando a juicio de los organismos, órganos, entes y entidades del sector público a que se refiere el artículo 11.3, párrafo primero, se considere que la comunicación de determinados datos entre sí o a la autoridad aeronáutica y a las personas y organizaciones aeronáuticas afectadas, sea necesaria para prevenir accidentes o incidentes.*

*2. La información a que se refiere el artículo 18.1, segundo párrafo, sólo podrá ser comunicada o cedida a terceros en los supuestos previstos por la normativa comunitaria que resulte de la aplicación.*

*La Comisión de Investigación de Accidentes e Incidentes de Aviación Civil y el resto de las autoridades o instituciones que pudieran estar implicadas en las actividades relacionadas con la investigación deberán suscribir los Acuerdos previos de conformidad con lo previsto en el artículo 12.3 del Reglamento (UE) n.º 996/2010 del Parlamento Europeo y del Consejo, de 20 de octubre de 2010, en los que se abordará, entre otros aspectos, el intercambio de la información y el uso adecuado de la información relativa a la seguridad.*

*3. En el supuesto previsto en el apartado 1.a) los obligados a facilitar la información podrán solicitar a los órganos judiciales o al Ministerio Fiscal que mantengan el carácter reservado de esa información y que adopten las medidas pertinentes para garantizar la reserva durante la sustanciación del proceso.*

*El órgano judicial podrá adoptar cuantas medidas procedan para proteger la información y, en particular, podrá prohibir su publicación o comunicación.*

#### **5.4 PREOCUPACIONES SOBRE EL MAL USO DE LA INFORMACIÓN**

Uno de los principales obstáculos de la **cultura de notificación** es que la información de seguridad operacional pueda utilizarse indebidamente. El uso indebido ocasiona un daño considerable. La legislación española ha regulado los potenciales siguientes malos usos de la información:

##### **Castigos/ Sanciones**

En primer lugar, el notificante puede estar preocupado de que la gestión de su empresa y/o AESA utilicen la información para castigarle o sancionarle. Por ejemplo, un mecánico podría ser reacio a denunciar un manual de mantenimiento confuso que condujo a una instalación incorrecta, por temor a que la gestión de la empresa y/o AESA estuviesen en desacuerdo en que el manual de mantenimiento fuese confuso y posteriormente fuese castigado por la instalación incorrecta. Tal castigo provoca dos problemas:

- En primer lugar, el manual de mantenimiento confuso estaría en uso dentro de la organización y potencialmente podría confundir e inducir a error a otros mecánicos
- En segundo lugar, y mucho peor, es que tal castigo se interpreta como "*matar al mensajero*". Con este castigo, la gestión de la empresa y/o AESA desmotiva a otros futuros notificantes. Con lo cual, los problemas se mantendrán como "sucesos sin reportar" hasta que causen un accidente o incidente, tras lo cual se podrán de manifiesto el hecho de que "todos conocíamos el problema".

El artículo 11, 12 y 18 de la actual Ley de Seguridad Aérea, que se encuentra reproducido en el apartado anterior, reguló este aspecto con el fin de proteger al notificante frente a posibles sanciones o castigos tanto por parte de su compañía como por parte de la autoridad española.

## **Acceso Público**

Otra de las preocupaciones acerca del mal uso de la información puede deberse al acceso público, incluyendo acceso por parte de los medios de comunicación, a información que esté en poder de los organismos gubernamentales.

En la actual legislación española, el artículo 18 de la Ley de Seguridad Aérea confiere carácter reservado a la información facilitada en el ámbito del Programa Estatal de Seguridad Operacional para la Aviación Civil por parte de los proveedores de servicios y productos aeronáuticos. Y el artículo 19 de la citada Ley establece los supuestos en los cuales la información podría ser cedida o comunicada. Dentro de estos supuestos no se incluye el acceso público a la información facilitada en el marco del Programa Estatal de Seguridad Operacional para la Aviación Civil.

## **Sanciones Penales**

Un obstáculo importante para la recopilación y el intercambio de información sobre seguridad operacional es la preocupación por la persecución penal por infracciones reglamentarias. En España está vigente la Ley 209/1964 de 24 de diciembre, Penal y Procesal de la Navegación Aérea.

Es más, el artículo 18 de la Ley de Seguridad Aérea confiere carácter reservado a la información facilitada en el ámbito del Programa Estatal de Seguridad Operacional para la Aviación Civil por parte de los proveedores de servicios y productos aeronáuticos. Y el artículo 19 de la citada Ley establece los supuestos en los cuales la información podría ser cedida o comunicada. En concreto el punto a) regula:

---

*Artículo 19. Cesión o comunicación de la información.*

*1. La información a la que se refiere el artículo 18.1 sólo podrá ser comunicada o cedida a terceros en los casos siguientes:*

*a) Cuando sea requerida por los órganos judiciales o el Ministerio Fiscal para la investigación y persecución de delitos.*

*La Comisión de Accidentes e Incidentes de Aviación Civil remitirá la información necesaria, limitándose a facilitar los antecedentes que obren en su poder en relación a los factores contribuyentes que hayan provocado un accidente o incidente aéreo. La identificación de los factores no implica la asignación de la culpa o la determinación de la responsabilidad, civil o penal.*

---

Por tanto el legislador español ha considerado conveniente desproteger la información en caso de investigación y persecución de delitos a fin de depurar responsabilidades penales.

## **Litigios Civiles**

Otra de las preocupaciones es que la información recopilada sea utilizada en contra de la fuente durante litigios civiles en caso de accidentes. Es decir, que durante litigios civiles en caso de accidentes, esté en riesgo la confidencialidad de la información recogida en el ámbito del Programa Estatal de Seguridad Operacional.

El citado artículo 19 de la Ley de Seguridad Aérea no contempla entre sus supuestos que la información sea desprotegida en caso de litigios civiles.

## **6. DEFINICIONES Y PRINCIPIOS DE LA CULTURA JUSTA**

### **6.1 DEFINICIÓN DE CULTURA JUSTA<sup>4</sup>**

En el **El Reglamento (UE) Nº 376/2014** del Parlamento europeo y del Consejo de 3 de abril de 2014 se define cultura justa como:

***Aquella en la que no se castigue a los operadores y demás personal de primera línea por sus acciones, omisiones o decisiones cuando sean acordes con su experiencia y capacitación, pero en la cual no se toleren la negligencia grave, las infracciones intencionadas ni los actos destructivos.***

La Cultura Justa está referida a la forma como se piensa en seguridad operacional, promoviendo una actitud de interrogación, resistente a la complacencia, buscando la mejora permanente y exigiendo la responsabilidad individual y corporativa a través de un compromiso organizacional con la seguridad operacional.

Una cultura “justa” de la seguridad operacional es, por lo tanto, la actitud y estructura en relación con los individuos y las organizaciones. Las actitudes personales y el estilo corporativo pueden permitir o facilitar el conocimiento de los actos y condiciones inseguras que son los precursores de los accidentes e incidentes. No sólo se requiere identificar activamente los problemas de seguridad operacional, sino también responder con las medidas adecuadas.

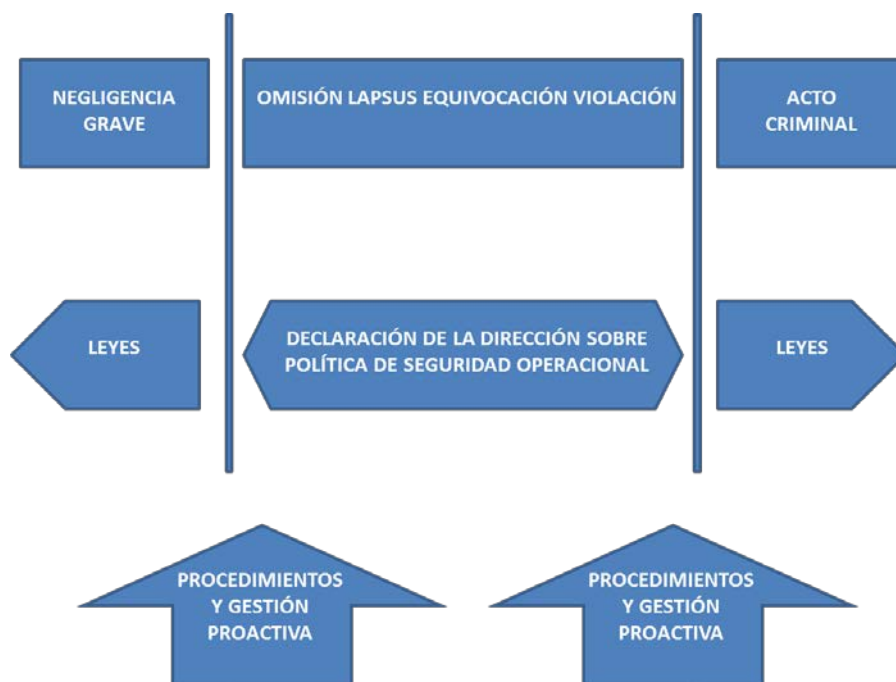
### **6.2 LOS TRES TIPOS DE COMPORTAMIENTOS INSEGUROS**

Marx (2001) ha identificado tres tipos de conducta que pueden resultar en actos inseguros. La cuestión que se ha planteado Marx (2001) y otros es que no todos estos comportamientos necesariamente justifican una sanción disciplinaria.

La siguiente figura ilustra las fronteras entre las conductas aceptables e inaceptables, en las primeras se trata el error humano (omisión, lapsus, equivocación y violación) a través de las políticas internas, y en las segundas son las leyes las que actúan en caso de imprudencia temeraria o negligencia grave y actos criminales. Aquellas situaciones que se encuentren en los límites entre unas y otras, pueden ser resueltas mediante procedimientos específicos y una gestión proactiva:

---

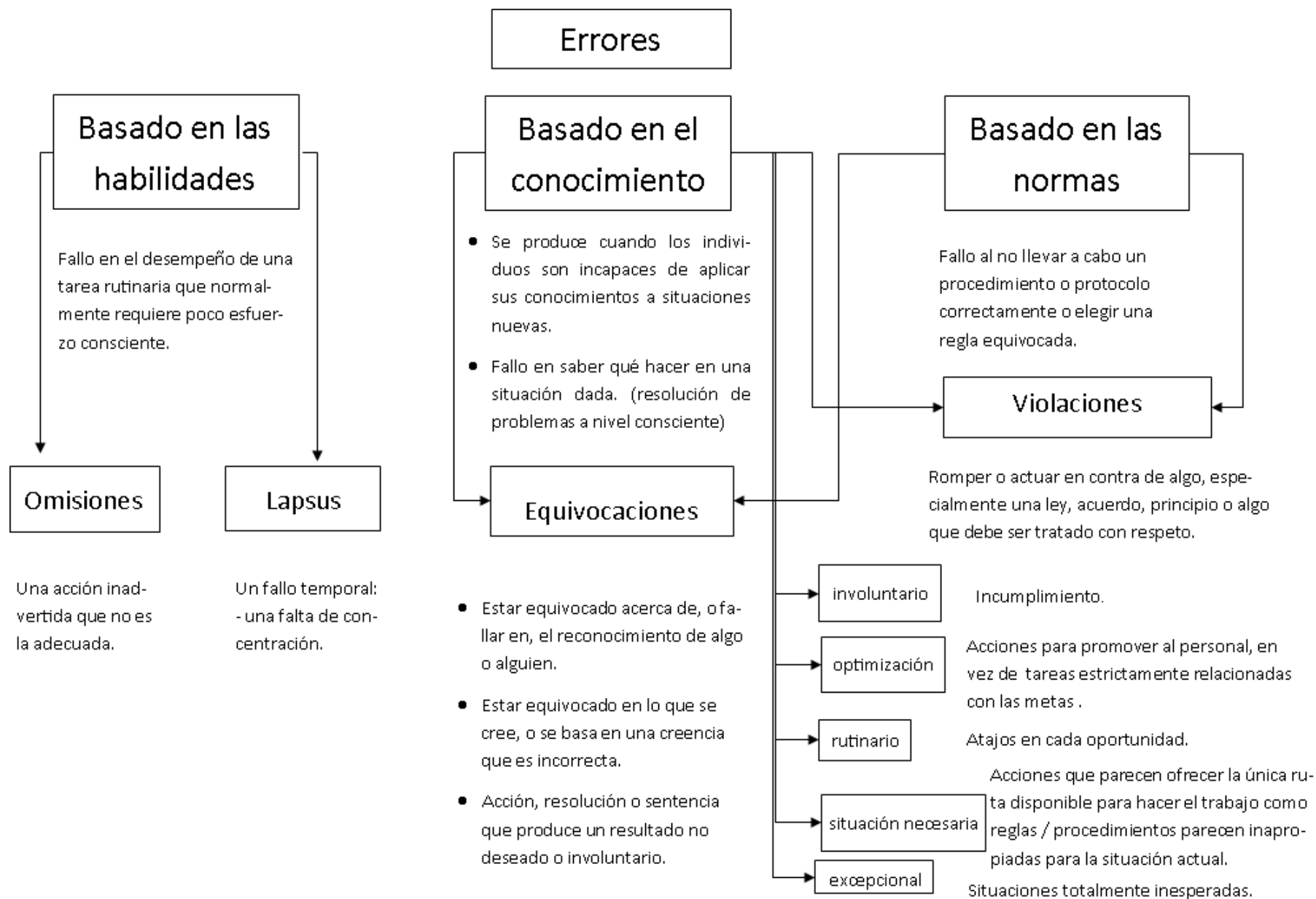
<sup>4</sup> James Reason definió, en 1997, la **cultura justa** como una atmósfera de confianza en la cual las personas son animadas (incluso recompensadas) por proporcionar información esencial para la seguridad operacional, pero en la que debe estar claramente definida la línea entre las conductas aceptables y las que no sean aceptables.



**El error humano** – Según James Reason, es un término genérico que engloba todas esas acciones en las cuales la secuencia de actividades físicas o mentales falla al intentar obtener un resultado deseado y esos fallos no son atribuibles a la intervención de algún agente de cambio.

En las siguientes gráficas se proporciona más información sobre los diversos errores humanos y las posibles medidas a adoptar para evitarlos.

Además en el Anexo A se proporcionan ejemplos de los diversos tipos de errores humanos tomados del curso sobre SMS de la CAA de Australia:



Omisión	Acciones involuntarias	No hay una solución obvia
Lapsus	Fallo involuntario al actuar	No hay una solución obvia
Equivocación	Acciones previstas que dan un resultado diferente del esperado	Formación

Violación	Rotura "deliberada" de los supuestos de los sistemas de gestión de la seguridad: se seguirán las reglas	Incumplimiento involuntario: Las personas no saben como aplicar la norma. Las personas actúan como si no hubiera procedimiento	Formación
		Rutinario: Las reglas se rompen debido a que se sienten irrelevantes o porque las personas no aprecian más peligros	Cambio de comportamiento
		Optimización: A veces es posible hacer el trabajo más rápido, más conveniente o experimentar una emoción por no adherirse a las normas	
		Situacional: Es imposible hacer el trabajo mediante la aplicación estricta de las normas.	Cuestionar las reglas y el lugar de trabajo
		Excepcional: La gente tiene que resolver el problema por primera vez y falla al no seguir las buenas prácticas	No hay una solución obvia

**Imprudencia temeraria (o negligencia grave)** según el artículo 16.10 del Reglamento (UE) nº 376/2014 del Parlamento Europeo y del Consejo de 3 de abril de 2014 se define como:

*cuando se haya producido una omisión manifiesta, importante y grave del deber de diligencia ante un riesgo evidente y una falta profesional grave a la hora de prestar la diligencia que evidentemente se requiere en esas circunstancias, dando lugar a daños previsibles a personas o bienes o que comprometan gravemente el nivel de la seguridad aérea.*

**Violaciones "intencionadas"** - cuando la persona conoce o prevé el resultado de la acción, pero sigue adelante y lo hace de todos modos.

### 6.3 DETERMINACIÓN DE LA 'CULPABILIDAD' CASO POR CASO

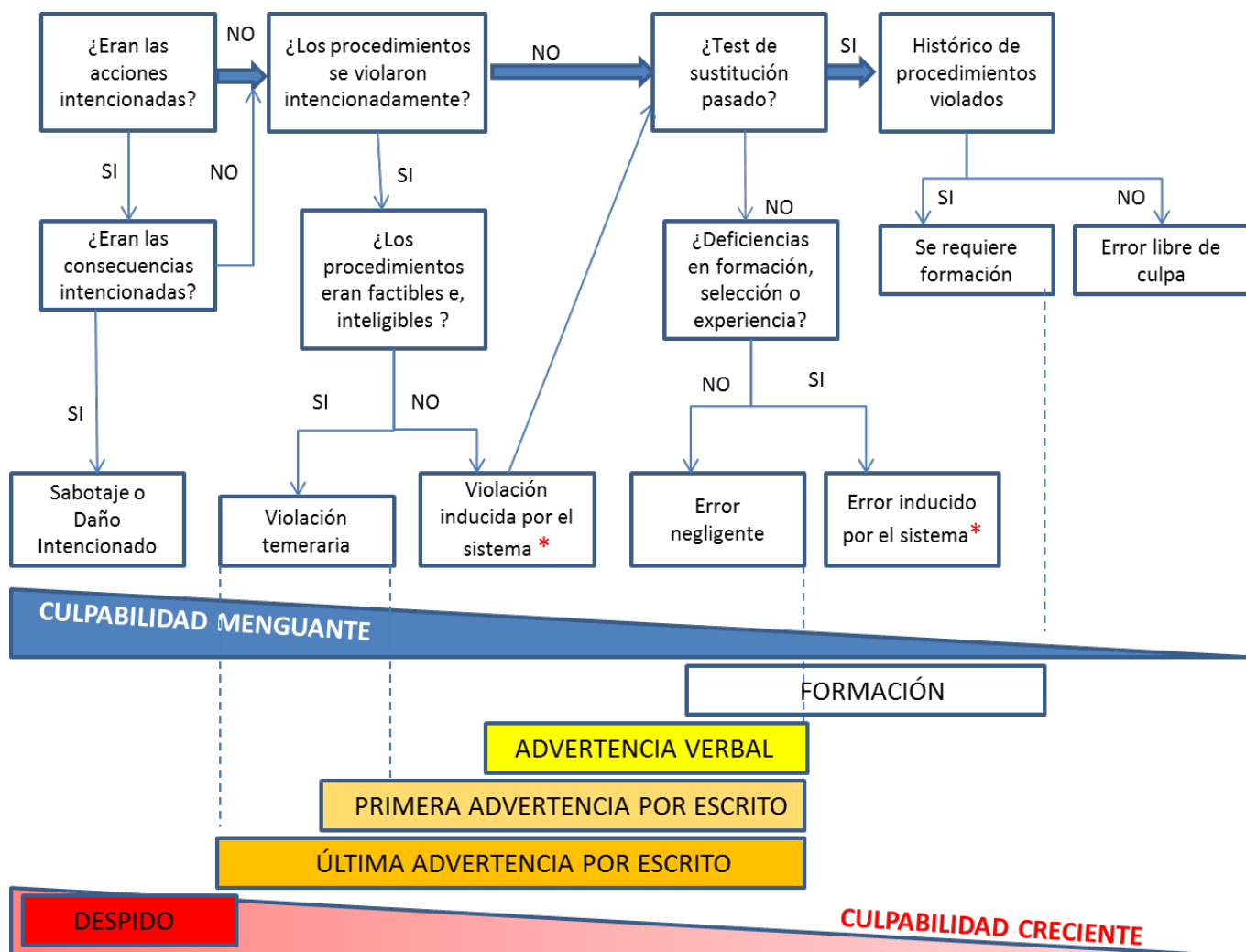
Con el fin de decidir si un determinado comportamiento es lo suficientemente culpable para requerir una acción disciplinaria, se requiere una política para decidir de manera equitativa a partir de una base caso por caso. Tres tipos de política disciplinaria se describen a continuación (Marx, 2001). La tercera política sienta las bases para una cultura justa. A continuación se presenta el árbol de decisión de culpabilidad de Reason, que proporciona un método estructurado para la determinación de la culpabilidad.

- ✓ **Toma de decisiones disciplinarias basada en los resultados** - se centra en el resultado (la gravedad) de la prueba: cuanto más grave es el resultado, más percepción de

culpabilidad para el actor. Este sistema se basa en la idea de que podemos controlar totalmente el resultado de nuestra conducta. Sin embargo, sólo podemos controlar nuestros comportamientos encaminados a reducir el riesgo de cometer el error, pero realmente no podemos controlar cuándo y dónde se producirá el error humano. La disciplina no puede disuadir a los que no tienen la intención de cometer un error (Marx, 2001).

- ✓ **Toma de decisiones disciplinarias basada en las reglas** - La mayoría de las industrias de alto riesgo tienen normas basadas en resultados (por ejemplo, los mínimos de separación) y normas basadas en el comportamiento (por ejemplo, limitación de horas de trabajo). No necesariamente una violación de la norma debe castigarse, ya que puede que las normas no se ajusten a las circunstancias particulares. Las violaciones proporcionan oportunidades de aprendizaje fundamentales para mejorar la seguridad operacional - por qué, por ejemplo, ciertas violaciones se convierten en la norma.
- ✓ **Toma de decisiones disciplinarias basada en el riesgo asumido** - Este método considera la intención de un empleado en relación con el resultado no deseado. Las personas que actúan imprudentemente, se piensa que demuestran una mayor intención (ya que intentan asumir un riesgo importante e injustificable) que los que demuestran una conducta negligente. Por lo tanto, cuando un empleado debería saber, pero no era consciente, del riesgo que él/ella estaba tomando, él/ella ha sido negligente, pero no es culpable de ello, y por lo tanto, no sería castigado en un ambiente de cultura justa. Si es una negligencia grave (ver apdo. 6.3) sí sería castigado.

**Tabla de Decisión de Culpabilidad de Reason** - La siguiente figura muestra una metodología para ayudar a decidir sobre la culpabilidad de un acto peligroso. Se aplica para analizar las conductas en casos de accidente o incidente grave. Si hubiera distintos actos inseguros que hayan contribuido al mismo suceso, se aplicará separadamente para cada uno de ellos. El problema aparece con actos inseguros individuales cometidos ya sea por una sola persona o por diferentes personas en diferentes puntos de la secuencia de eventos. Consta de cuatro etapas y se trata de una metodología post-investigación:



\* Responsabilidad de la Gestión/Supervisión para corregir las causas raíz del sistema

1. **Intencionalidad del acto y sus consecuencias:** La primera pregunta en la tabla de decisión se refiere a la intención, y si hubiera intención en ambas (acciones y consecuencias), entonces es posible que la conducta delictiva pueda ser tratada fuera de la empresa (como sabotaje o daño malévolo).
2. **Violación deliberada de las normas:** Se estudia si la propia organización promueve, tolera o desalienta las violaciones. En la literatura, se han identificado varios tipos de violaciones. El Anexo A proporciona ejemplos de las distintas violaciones.
3. **Test de Sustitución:** Preguntarse si otra persona con las condiciones adecuadas para cumplir la tarea, habría cometido el mismo error en circunstancias similares. En este caso quedaría exonerada si no se determinase negligencia.
4. **Errores repetitivos:** Se recaba la información relativa a actos inseguros previos del mismo individuo. Solo al objeto de determinar si necesita entrenamiento adicional o consejo.



**Test de previsión de Reason** - Proporciona un test anterior al de “sustitución”. Se realiza la siguiente pregunta: *¿Era consciente el individuo, que su conducta hubiera sido reconocida por otra persona de un nivel equivalente de competencia, como posiblemente contribuyente a incrementar la probabilidad de cometer un error de seguridad crítico?*

Si la respuesta es afirmativa, se considera que el individuo puede ser considerado culpable. Sin embargo, si se dieran alguna de las siguientes circunstancias, sería necesario discriminar a través del test de sustitución:

- Encontrarse bajo los efectos de un medicamento o sustancia que pudiera disminuir las habilidades
- Encontrarse haciendo bromas mientras se encontraba en su puesto
- Encontrarse excesivamente fatigado como consecuencia de trabajar con mínimos descansos
- Usar equipos que se conozcan como inadecuados

#### **6.4 CREACIÓN E IMPLEMENTACIÓN DE LA CULTURA JUSTA**

En esta sección se describen brevemente algunas de las principales medidas, así como los posibles obstáculos para alcanzar una cultura justa.

Para obtener más detalle acerca de alguno de los pasos para la implementación de la cultura justa relacionados con el Sistema de Notificación de Sucesos, el operador puede consultar la guía elaborada por AESA: “El Sistema de Notificación de Sucesos del Operador” publicada en la página web:

[http://www.seguridadaerea.gob.es/lang\\_castellano/g\\_r\\_seguridad/drgi/default.aspx](http://www.seguridadaerea.gob.es/lang_castellano/g_r_seguridad/drgi/default.aspx)

##### **6.4.1 POLÍTICA Y PROCEDIMIENTOS DE REPORTE**

Es importante que se consideren los siguientes temas en relación con la estructura de la información subyacente y el compromiso de la empresa:

- ✓ Confidencialidad o desidentificación de los informes. La guía sobre “El Sistema de Notificación de Sucesos del Operador” proporciona pautas en este sentido.
- ✓ Separación del departamento de recopilación y análisis de los informes de los órganos para iniciar procedimientos disciplinarios e imponer sanciones dentro de la organización.
- ✓ Compromiso de la empresa con la seguridad operacional.
- ✓ Debe concederse a los gerentes del sistema de notificación un cierto grado de independencia.

**Obstáculo potencial:** Puede ser difícil persuadir a la alta dirección de la necesidad de crear una cultura justa y de comprometer recursos suficientes.

#### **6.4.2 LOS MÉTODOS DE REPORTE**

La guía sobre “El Sistema de Notificación de Sucesos del Operador” proporciona pautas tanto para establecer el proceso de notificación como el proceso de análisis preliminar y detallado, si fuese necesario.

Los primeros pasos para desarrollar un sistema de notificación de " cultura justa " podrían ser:

- ✓ Desarrollar los procedimientos para la determinación de culpabilidad (como por ejemplo, la tabla de decisión de cultura justa) y las medidas de seguimiento (tipo de disciplina o entrenamiento).
- ✓ Decidir quién decidirá la culpabilidad (por ejemplo, un equipo relacionado con la seguridad operacional, operaciones, gestión, recursos humanos).
- ✓ Elaborar un plan y discutirlo con una pequeña selección del personal operativo.

**Obstáculos potenciales:** Un sistema que no es claro y es ambiguo podría crear desconfianza en el sistema, por lo que es necesario que los procedimientos para decidir la culpabilidad sean claros y comprensibles para todos.

#### **6.4.3 DETERMINACIÓN DE LAS FUNCIONES Y LAS RESPONSABILIDADES, TAREAS Y CALENDARIO**

Para que este sistema prospere, un conjunto de diferentes personas necesita involucrarse en la implementación y mantenimiento del sistema. Se necesitará un 'líder local' para promover y garantizar que el anonimato se conserva frente a las presiones externas o de gestión. Decidir y elegir a alguien que:

- ✓ Lidere el sistema.
- ✓ Eduque a los usuarios e implemente el sistema.
- ✓ Recopile y analice los reportes.
- ✓ Decida qué departamento estará involucrado en el proceso disciplinario (toma de decisiones).
- ✓ Realimente la información (desarrollo de un boletín de noticias).
- ✓ Desarrolle y mantenga el sistema de recopilación de datos.

**Obstáculos potenciales:** Tener recursos suficientes (por ejemplo, personal) para ejecutar el sistema, además de tener suficiente personas del tipo "adecuado", es decir, enérgicas, muy queridas, muy conocidas y respetadas en la empresa. El mantenimiento de la energía necesaria para que el sistema funcione es otro de los potenciales obstáculos.

#### **6.4.4 DESARROLLO DEL FORMATO DE REPORTE**

La guía sobre “El Sistema de Notificación de Sucesos del Operador” proporciona pautas para establecer el formato del reporte.

#### **6.4.5 DESARROLLO DE PLANTILLAS PARA PROPORCIONAR FEEDBACK A LOS USUARIOS POTENCIALES**

Determine:

- ✓ Qué tipo de información desea difundir (por ejemplo, resumen, estudios de casos, "puntos calientes", datos de factores humanos).
- ✓ Cómo difundir la información (por ejemplo, boletines).
- ✓ Quién participará (escrito; edición de un boletín, plan de acción de respaldo de la alta dirección).
- ✓ Con qué frecuencia se difundirá la información.
- ✓ Estilo de plantilla de la revista, título, etc.

**Obstáculos potenciales:** El boletín no se lee. Puede que sea necesario averiguar qué tipo de información quiere saber el público, proporcionar ejemplos que sean de interés y relevantes para su trabajo. Puede ser necesario variar el estilo con el tiempo, para mantener su atención, y así probablemente contribuirán a ello.

#### **6.4.6 DESARROLLO DE UN PLAN PARA EDUCAR A LOS USUARIOS Y PARA LA IMPLEMENTACIÓN DEL SISTEMA**

Los potenciales notificantes deben conocer el método de reporte y saber cómo presentar un reporte, esto incluirá cursos de iniciación; refresco periódico para recordar al personal la importancia de reportar y garantizar que el personal tiene acceso a los formularios de presentación de reportes. A continuación se presentan algunos pasos iniciales para la implementación del sistema.

- ✓ Desarrollar folletos para explicar los cambios en la organización.
- ✓ Presentar los cambios a todo el personal.
- ✓ Entrenar a un "líder" (o un equipo) para ser el foco principal del sistema.
- ✓ Explicar a los usuarios cómo este nuevo sistema se ajustará en el sistema actual.
- ✓ Tener una campaña como "La semana de la seguridad operacional" para promover el sistema de información.
- ✓ Incluir una sección sobre el sistema de reporte en el curso de iniciación en seguridad operacional.

- ✓ Utilización del correo electrónico e internet para comunicarse, anunciando la nueva información, y felicitando a los participantes.
- ✓ Diseño de carteles para describir gráficamente el proceso del sistema de información.

**Obstáculos potenciales:** La información sobre el sistema no se puede difundir a un público lo suficientemente amplio y a un nivel lo suficientemente profundo dentro de la organización.

#### **6.4.7 DESARROLLO Y MANTENIMIENTO DE LA "CULTURA" CORRECTA**

Es necesaria una serie de cuestiones adicionales relativas a los aspectos "culturales" de los reportes para mantener la motivación por reportar, tales como la confianza que debe existir realmente entre los notificantes y los responsables para que el sistema de reporte funcione. Los principales objetivos son el desarrollo de una cultura abierta en la que la gente se siente capaz de confiar en el sistema y el desarrollo de nuevas formas de motivar a la gente a usar el sistema. A continuación se presentan las ideas iniciales.

Visibilidad del sistema - los posibles contribuyentes para estar al tanto de los procedimientos y mecanismos que apoyan el sistema de notificación de incidentes

El mantenimiento de la voz de los trabajadores - debe asegurarse de que los reportes se utilizan para expresar la voz de los empleados y no se utilizarán para satisfacer las prioridades existentes de gestión.

Difusión de la participación, - publicar la tasa de contribución de las diferentes partes de la organización para demostrar que otros tienen confianza en el sistema (pero deben asegurarse de que esto no tiene el efecto contrario, como pedir determinadas cuotas de reportes mensuales).

Desarrollar "estrategias de marketing" para mejorar la cultura de seguridad (ver Vecchio - Sadus y Griffiths, 2004): a) Centrado en el cliente - centrar la estrategia de marketing para adaptarse a la audiencia (por ejemplo, gestión tendrá un enfoque diferente que el personal de operaciones), b) Enlace de los valores de seguridad operacional con la actividad principal - y mostrar una evidencia tangible de su impacto, por ejemplo, cómo la seguridad operacional puede mejorar la producción, la eficiencia, la comunicación e incluso los beneficios de costes; c) Recompensa y reconocimiento - el refuerzo positivo de los incidentes reportados.

Cambio de actitudes y comportamientos - se centran en las consecuencias ciertas, inmediatas, y positivas del reporte de incidentes y dar a conocer los "resultados" de los incidentes reportados.

Compromiso de la dirección - dar a conocer el compromiso de la gerencia con la seguridad operacional, con un "enfoque práctico", ha participado en la gestión del proceso de reporte y demostrar que visiblemente creen y promueven la cultura justa.

Participación de los empleados - asegurar la participación de los empleados para que estén comprometidos con la necesidad de participar de forma activa en la toma de decisiones y el proceso de resolución de problemas.

**Obstáculos potenciales:** se necesita tiempo y perseverancia para tratar de cambiar las actitudes y comportamientos en seguridad operacional. Puede ser un obstáculo potencial el mantenimiento de la motivación del personal establecido para la tarea de mejorar la información de seguridad operacional.

Deben tenerse en cuenta tres aspectos de planificación: 1) el tiempo necesario para llevar a cabo los pasos y subsiguientes pasos (incluido las fechas de inicio y fin), 2) los costes estimados involucrados y 3) quién llevará a cabo el trabajo.

#### **6.4.8 CONCLUSIÓN**

**Como conclusión de lo expuesto en los párrafos anteriores, la implantación de una cultura justa con el fin de facilitar una cultura de reporte, no es posible sin el compromiso y la involucración de la alta dirección de una organización.**

## **ANEXO A: EJEMPLOS DE ERROR HUMANO<sup>5</sup>**

Ejemplo de omisión en la escalera:

Un ingeniero de mantenimiento estaba supervisando los trabajos de reparación de los alerones cuando perdió el equilibrio subiendo por una escalera. El ingeniero resbaló en el peldaño superior de la escalera, y su pie quedó atrapado entre la plataforma y el peldaño. Su pierna quedó anclada al caer, soportando toda la fuerza de la caída. Un compañero de trabajo, que se encontraba de pie junto al ingeniero, logró sujetarlo evitando que cayese al suelo. El ingeniero llevaba calzado de seguridad y la superficie de la plataforma estaba limpia y seca. La plataforma no disponía de asidero para ayudar a subir o bajar de la escalera, y las barandillas no se erigieron correctamente. El ingeniero estaba distraído por la presencia de otro trabajador cerca y no prestaba atención cuando ponía el pie en el peldaño de la escalera.

Ejemplo de lapsus: Olvido del cierre de la puerta de la capota del ventilador

El 20 de enero del 2000, un avión Airbus A-320 comenzó la carrera de despegue desde el aeropuerto de Gatwick Londres, ambas puertas de la capota del ventilador del motor nº 1 se abrieron y golpearon la aeronave. Las puertas fueron destruidas y el motor nº 1 y su pilón, el ala izquierda, los flaps y los slats izquierdos, el fuselaje y la cola resultaron dañados. Lo más probable es que las puertas se hubiesen cerrado tras el mantenimiento, sin embargo, el cierre no habría sido seguro o no se habría trabado. Cuando las puertas están cerradas, no hay señales visibles que indiquen que están desenganchados ni alguna indicación en la cabina de vuelo. En todo el mundo se han contabilizado al menos 7 incidentes similares.

Ejemplo de equivocación: ¿Estás perdido? Aterrizas y pregunta la dirección

Un piloto de un Cherokee Six se perdió durante un vuelo de Uluru a Alice Springs. Decidió aterrizar en una carretera de grava y preguntar dónde se encontraba. Durante la aproximación final, era evidente que la zona de carretera seleccionada no era adecuada, pero el piloto continuó el aterrizaje. Durante el aterrizaje, la aeronave se golpeó con los árboles y se estrelló. El avión se dañó sin posibilidad de reparación, pero los seis ocupantes salieron ilesos. No había ninguna razón apremiante para que el piloto aterrizase con tanta prisa: las condiciones meteorológicas eran buenas, era temprano y disponía de combustible remanente para al menos 3 horas. El piloto podría haber subido a una altitud superior que le permitiese establecer su posición o utilizar la carretera como una ayuda a la navegación.

Las violaciones pueden ser: rutinarias, circunstanciales, para optimizar el trabajo (personal o de la organización), excepcionales o un acto de sabotaje. A continuación se presentan ejemplos de cada tipo de violación. Ejemplo de violación rutinaria

---

<sup>5</sup> Los ejemplos han sido tomados del material de formación en SMS elaborado por la CAA australiana.

Un piloto de un Cherokee Six se perdió durante un vuelo de Uluru a Alice Springs. Decidió aterrizar en una carretera de grava y preguntar dónde se encontraba. Durante la aproximación final, era evidente que la zona de carretera seleccionada no era adecuada, pero el piloto continuó el aterrizaje. Durante el aterrizaje, la aeronave se golpeó con los árboles y se estrelló. El avión se dañó sin posibilidad de reparación, pero los seis ocupantes salieron ilesos. No había ninguna razón apremiante para que el piloto aterrizase con tanta prisa: las condiciones meteorológicas eran buenas, era temprano y disponía de combustible remanente para al menos 3 horas. El piloto podría haber subido a una altitud superior que le permitiese establecer su posición o utilizar la carretera como una ayuda a la navegación.

#### Ejemplo de violación circunstancial

El 2 de noviembre de 1996, la manija de la puerta 4 izquierda de un Boeing 747 se cambió a la posición “abierta” durante el ascenso. El capitán decidió realizar un vaciado rápido del combustible y volver a Gatwick, y el avión aterrizó sin problemas. Una investigación reveló que el tubo de torsión de la puerta había sido incorrectamente perforado/instalado. El manual de mantenimiento requiere usar una plantilla de perforación para montar el nuevo tubo de torsión aún sin perforar, pero la plantilla no estaba disponible. El ingeniero con licencia para el mantenimiento de aeronaves y el ingeniero de enlace técnico de la flota decidieron perforar el tubo en el taller sin plantilla de perforación, por falta de tiempo y la necesidad operacional de la aeronave. El problema en la puerta fue debido a que los agujeros perforados no se habían posicionado correctamente para la fijación del tubo de torsión de la puerta.

#### Ejemplo de violación para optimizar el trabajo personal

En Athlone, Irlanda, el 9 de mayo de 2008, un piloto aterrizó su helicóptero en la parte superior de un aparcamiento de varios pisos, ya que quería ir a un centro comercial cercano.

El encargado del aparcamiento, que afirmó que había expulsado previamente al helicóptero cuando intentaba aterrizar el pasado mes de julio sobre el techo del aparcamiento vacío, dijo que se vio obligado a refugiarse detrás de una puerta para protegerse.

Dijo que se lesionó cuando el flujo descendente del rotor principal movió la puerta y ésta le apresó la mano. La Unidad de Investigación de Accidentes Aéreos concluyó que piloto, que creía que tenía permiso para aterrizar, disponía de escasa aptitud para volar e incumplió el derecho aéreo irlandés.

“El centro comercial estaba abierto cuando ocurrió el accidente y por razones obvias de seguridad operacional la zona debería haber sido totalmente evitada.”

El informe de la investigación señaló que el aterrizaje era contrario a las reglas del aire y que la zona estaba congestionada y debería haberse evitado.

#### Ejemplo de violación excepcional

Un trabajador subcontratado por el aeroclub local estaba utilizando una afiladora con un cable eléctrico deshilachado enchufado a una toma de corriente improvisada y sin autorización para uso

externo. El trabajador no llevaba ningún equipo de protección personal, no disponía de extintor en el lugar de trabajo y estaba sentado en una escalera mientras trabajaba sin un vigilante de seguridad operacional.



## **ANEXO B: PROPUESTA DE POLÍTICA DE CULTURA JUSTA**

1. [Organización] tiene el firme propósito de establecer una política de reporte abierta y honesta en la que todo el personal, independientemente de su estatus o su experiencia, sean tratados de una manera justa, coherente, objetiva y oportuna.
2. La misión de [Organización] es [indicar la misión de la Organización]
3. Para lograr este objetivo, es esencial cumplir con los requisitos de seguridad operacional en todos los aspectos de la actividad de [Organización]. Para ello, los eventos de seguridad operacional han de gestionarse de forma sistemática y activa equilibrando requisitos potencialmente contradictorios de seguridad operacional y de producción. Tengo la intención de hacer esto dentro de una cultura justa que anime al reporte, abierto y honesto, de los eventos de seguridad operacional.
4. Reconozco que cometer errores es parte de la condición humana, y que los factores humanos desempeñan un papel importante en la aviación y en la seguridad operacional. Es mi intención implementar un Sistema de Gestión de la Seguridad Operacional ejemplar teniendo en cuenta para ello las mejores prácticas y cumpliendo con los estándares más altos de regulación. Animo a todos a contribuir activamente a la mejora de la seguridad operacional y os aseguro que vais a ser elogiados por reportar vuestras equivocaciones cometidas honestamente por hacer lo mejor.
5. Todo el personal involucrado en las actividades de aviación en [Organización], sin importar su estatus o experiencia, serán tratados de una manera justa, coherente, objetiva y oportuna. Es más, todo el personal involucrado en las actividades de aviación tienen la responsabilidad de participar activamente en el Sistema de Gestión de la Seguridad operacional informando de los sucesos y los peligros detectados con el fin aprender y mejorar.
6. En virtud de esta cultura justa, [Organización] seguirá una metodología definida y coherente para gestionar los errores. Los responsables de aplicar esta metodología serán personas independientes de la organización o de la cadena de mando de la organización. [A definir por la Organización la forma más conveniente]. No es una cultura "culpable" ni "no culpable". Todos los incidentes serán investigados por personal capacitado y autorizado por mí y, cuando los incidentes sean reportados oportuna y abiertamente, la presunción de inocencia será la norma y la expectativa de una acción disciplinaria será la excepción. Si se requiere cualquier acción disciplinaria o administrativa, no se hará sin una investigación adecuada y sin una revisión completa de las conclusiones de esa investigación.
7. Sin embargo, los siguientes comportamientos serán sancionables:
  - a. Dolo, es decir, actos premeditados o intencionales que causen daños a los equipos o la propiedad
  - b. Negligencia grave, es decir, cuando se haya producido una omisión manifiesta, importante y grave del deber de diligencia ante un riesgo evidente y una falta profesional grave a la hora de prestar la diligencia que evidentemente se requiere

en esas circunstancias, dando lugar a daños previsibles a personas o bienes o que comprometan gravemente el nivel de la seguridad aérea

- c. No reportar incidentes como lo requiere esta política.
8. Todo el personal de [Organización], dondequiera que trabajen y cualquiera que sea su función, debe ser consciente que tiene un papel que desempeñar y la responsabilidad de participar activamente para alcanzar los estándares de seguridad de vuelo más altos.
9. La Cultura Justa, y el sistema de notificación de sucesos, permitirán a [Organización] cumplir eficientemente con los requisitos operacionales al tiempo que garantiza los estándares de seguridad de vuelo más altos posibles. El sistema ayudará a disminuir los errores sin dejar de reconocer que la gente comete errores y la cultura justa posibilitará cumplir con este objetivo.

## **ANEXO C: CUESTIONARIO PARA EVALUAR LA CULTURA JUSTA**

Se propone el siguiente cuestionario para evaluar la cultura justa implantada por una organización:

### **Marco legal:**

1. ¿Los empleados de su organización pueden sufrir acciones legales como resultado de un error cometido durante su trabajo o una involucración en un incidente?
2. ¿Los empleados están protegidos por su organización contra la persecución? ¿En qué sentido?
3. ¿El marco legal existente tiene efectos positivos o negativos sobre la notificación, el análisis y el aprendizaje de los sucesos de seguridad operacional en su organización? ¿Qué tipo de efectos?
4. ¿Qué tipo de cambios en el marco legal promoverían la notificación e investigación de los sucesos de seguridad operacional?

### **Política y procedimientos para notificar aspectos de seguridad operacional:**

5. ¿Su organización ha desarrollado una política y/o procedimientos para la notificación proactiva de situaciones relevantes en el ámbito de la seguridad operacional? ¿Cuál es esa política?
6. ¿Su organización ha desarrollado una política para la notificación reactiva de situaciones relevantes en el ámbito de la seguridad operacional? ¿Cuál es esa política?
7. ¿Cómo apoya la dirección de la organización esa política?
8. ¿Se estimula la notificación de los temas relacionados con la seguridad operacional?
9. ¿De qué manera pueden notificar los empleados temas relacionados con la seguridad operacional?
10. ¿Existen procedimientos para notificar temas relacionados con la seguridad operacional? Por favor, explique.
11. ¿Los procedimientos son accesibles para los empleados? ¿De qué manera?

### **Confidencialidad:**

12. ¿El sistema de notificación de seguridad operacional es des-identificado? ¿El sistema de notificación de seguridad operacional es confidencial? ¿Quién tiene acceso a las notificaciones?
13. ¿El nivel de confidencialidad tienen efectos positivos o negativos en la notificación, análisis y aprendizaje de los sucesos de seguridad operacional en su organización? ¿Qué tipo de efectos?
14. En su opinión, ¿debería cambiarse este aspecto de su sistema de notificación? ¿En qué sentido?

**Sistema de Notificación de Seguridad operacional:**

**Notificación obligatoria/ voluntaria:**

15. ¿El sistema de notificación de seguridad operacional es obligatorio o voluntario?
16. ¿Tiene efectos positivos o negativos en la notificación, el análisis y el aprendizaje de los sucesos de seguridad operacional en su organización? ¿Qué tipo de efectos?
17. En su opinión, ¿debería cambiarse este aspecto de su sistema de notificación?

**Hardware:**

18. ¿Cuál es el formato actual para notificar (si existe): papel/ electrónico?
19. ¿La forma de notificar está adaptada al usuario (educación, nacionalidad, etc)?
20. En su opinión, ¿debería cambiarse el formato para notificar? ¿En qué sentido?

**Información:**

21. ¿Qué tipo de información debe proporcionarse verbalmente o en el formato actual?
22. Se solicita la información suficiente para el aprendizaje de la organización?
23. ¿Cuánto tiempo se tarda en completar un formulario?
24. ¿El formulario actual tiene efectos positivos o negativos sobre la notificación, análisis y el aprendizaje de los sucesos de seguridad operacional en su organización? ¿Qué tipo de efectos?
25. En su opinión, ¿debería cambiarse este aspecto? ¿En qué sentido?

**Formación:**

26. ¿Cómo se forma a las personas para usar el sistema de notificación de seguridad operacional?
27. ¿Cómo se estimula a las personas para utilizar el sistema de notificación de seguridad operacional?
28. ¿Hay gente designada para promover el uso del sistema de notificación de seguridad operacional?
29. ¿La educación actual tiene efectos positivos o negativos sobre la notificación, el análisis y el aprendizaje de los sucesos de seguridad operacional?
30. En su opinión, ¿debería cambiarse este aspecto? ¿En qué sentido?

**Realimentación:**

31. ¿Cómo se distribuye la información sobre cuestiones de seguridad operacional en la organización? ¿Quién recibe esta información?
32. ¿De qué manera se determinan las lecciones aprendidas de las cuestiones de seguridad operacional reportadas? ¿Quiénes están involucrados en la determinación de las lecciones aprendidas?
33. ¿Cómo se distribuye la información sobre las lecciones aprendidas de las cuestiones de seguridad operacional en la organización?

34. ¿La realimentación tiene efectos positivos o negativos sobre la notificación, el análisis y el aprendizaje de las cuestiones de seguridad operacional en su organización? ¿Qué tipo de efectos?

35. En su opinión, ¿debería cambiarse este aspecto? ¿En qué sentido?

**Análisis detallado:**

36. ¿Quién decide si se analizarán en detalle y cómo ciertas cuestiones de seguridad operacional?

37. ¿Existen procedimientos para decidir qué cuestiones de seguridad operacional se analizarán en detalle? ¿Cuáles son estos procedimientos? ¿Se cumplen?

38. ¿Quién analiza en detalle los problemas de seguridad operacional reportados?

39. ¿El equipo que analiza en detalle los problemas de seguridad tiene una posición independiente dentro de la organización?

40. ¿Existen procedimientos sobre cómo han de realizarse los análisis detallados y sobre qué resultados han de alcanzarse? ¿Cuáles son estos procedimientos? ¿Se cumplen?

41. ¿El análisis detallado tiene efectos positivos o negativos sobre la notificación, el análisis y el aprendizaje de las cuestiones de seguridad operacional en su organización? ¿Qué tipo de efectos?

42. En su opinión, ¿debería cambiarse este aspecto? ¿En qué sentido?

**Culpabilidad:**

43. ¿Quién decide sobre la aceptabilidad del comportamiento de los empleados en el contexto de un suceso de seguridad operacional?

44. ¿Existen procedimientos para determinar la aceptabilidad del comportamiento en el contexto de un suceso de seguridad operacional? ¿Cuáles son estos procedimientos? ¿Se cumplen?

45. ¿Quién decide sobre las acciones a tomar (capacitación, disciplina, entrenamiento, etc)

46. ¿Existen procedimientos para decidir las acciones a tomar? ¿Cuáles son estos procedimientos? ¿Se cumplen?

47. ¿La toma de decisiones sobre la culpabilidad tiene efectos positivos o negativos sobre la notificación, el análisis y el aprendizaje de los sucesos de seguridad operacional en su organización? ¿Qué tipo de efectos?

48. En su opinión, ¿debería cambiarse este aspecto? ¿En qué sentido?

**Otros temas:**

49. ¿Tiene algún otro comentario o sugerencia para mejorar la cultura justa?

## ANEXO D: EVALUACIÓN DE CULTURA JUSTA EN EL ÁMBITO DE LOS PROVEEDORES DE SERVICIOS DE NAVEGACIÓN AÉREA

### Política y su implementación

Área	Pregunta
Elementos de la política	¿Hay una política de Cultura Justa explícita, que está formalmente aprobada por la dirección y los representantes de los empleados y que es pública?
Elementos de la política	¿La política de Cultura Justa contiene una descripción acerca de lo que se considera comportamiento inaceptable?
Elementos de la política	¿La política de Cultura Justa garantiza que no se tomarán acciones disciplinarias contra el notificante de sucesos en los cuales haya estado involucrado por parte del proveedor de servicios (excepto en los casos definidos como comportamiento inaceptable)?
Elementos de la política	¿El proveedor de servicios proporciona apoyo legal a sus empleados en caso de persecución/ acción legal relacionada con un suceso de seguridad operacional?
Elementos de la política	¿Hay establecido y es conocido el programa de Gestión del Stress de Incidentes Críticos (CISM)?
Elementos de la política	Tras el suceso y hasta que no haya finalizado la investigación, ¿se toman acciones de seguridad operacional sin impacto en el salario del personal involucrado?
Roles y Responsabilidades definidos e implementados	¿Los investigadores de seguridad operacional del proveedor de servicios son independientes y están separados de cualquier línea, competencia o gestión de operaciones?
Roles y Responsabilidades definidos e implementados	¿Los investigadores de seguridad operacional del proveedor de servicios tienen acceso pleno y libre a todos los datos relevantes para la investigación?
Roles y Responsabilidades definidos e implementados	¿El acceso a los datos de seguridad operacional está claramente definido y la confidencialidad está asegurada?
Roles y Responsabilidades definidos e implementados	¿El personal que Gestiona el Stress de los Incidentes Críticos está nominado y ha sido formado adecuadamente?
Formación	¿Hay formación regular y/o sesiones informativas sobre legislación de seguridad operacional relevante en el ámbito de la Cultura Justa?
Formación	¿Los principios de Cultura Justa están incluidos en todos los planes de formación (inicial y recurrente)?
Formación	¿Los requisitos sobre cualificación y formación en el ámbito de Cultura Justa están claramente definidos para los investigadores de seguridad operacional del proveedor de servicios?

### Legal/ Judicial

Área	Pregunta
Procedimientos	¿Está transpuesto plenamente el espíritu de la Directiva 2003/42/CE sobre la notificación de

judiciales y legislación de aviación específica	sucesos en la aviación civil y en particular lo dispuesto en el Artículo 8 (Protección de la información) en los procedimientos internos?
Acuerdo formal	¿Existe algún acuerdo entre el proveedor de servicios y las autoridades judiciales/policiales para asegurar la protección de los incidentes reportados y de las personas involucradas?
Acuerdo formal	¿Existe un proceso acordado entre el proveedor de servicios y su autoridad nacional de aviación para tratar cuestiones de incidentes?

### Notificación e investigación de sucesos

Área	Pregunta
Notificación e investigación de sucesos	¿La identidad del personal involucrado en los sucesos está protegida por los estatutos de personal?
Notificación e investigación de sucesos	¿Las personas sujetas a investigaciones de sucesos reportados tienen acceso a la información relacionada con los mismos?
Notificación e investigación de sucesos	¿Existe el requisito de que las personas sujetas a investigaciones firmen su acuerdo o desacuerdo con los resultados de la investigación?
Notificación e investigación de sucesos	¿Existe un procedimiento formal para informar al personal que ha notificado un suceso del progreso de la investigación?
Notificación e investigación de sucesos	¿Proporciona regularmente el proveedor de servicios feedback o retroalimentación sobre los sucesos notificados al personal?
Notificación e investigación de sucesos	¿Proporciona el informe anual público del proveedor de servicios feedback o retroalimentación estadística sobre los sucesos reportados?
Notificación e investigación de sucesos	¿La notificación automatizada es aceptada por el personal y está implantada por el proveedor de servicio?
Notificación e investigación de sucesos	¿Existe un organismo independiente con expertos en la materia para la toma de decisión acerca de si es un error "honesto" o si entra dentro de la categoría "comportamiento inaceptable"?