

Universidad de Palermo

Doctorado en Psicología

Tesis Doctoral

**Relación entre Potencial de Desempeño Resiliente y Seguridad Operacional en una
Organización de Aviación Militar: Factores Organizacionales Contribuyentes**

Doctoranda

Imelda Reyes Ávila Ps.

Director

Dr. Mario Poy PhD.

Ciudad Autónoma de Buenos Aires (Argentina)

30 de agosto de 2020

Resumen

El objetivo de esta investigación es analizar la relación entre el potencial de desempeño resiliente y la seguridad operacional en una organización de aviación militar colombiana.

Con base en un diseño secuencial explicativo, 545 pilotos militares colombianos valoraron la organización con las escalas de potencial de desempeño resiliente (capacidades de respuesta, monitoreo, aprendizaje y anticipación) y seguridad operacional (componentes de seguridad, gestión de seguridad/operaciones y cultura de la seguridad). Los clúster de incidentalidad se conformaron según la relación funcional Incidentalidad = (#horas de vuelo/Incidente) y el nivel de participación operacional se estableció a partir del rango jerárquico de los participantes.

Se encontró que el potencial de desempeño resiliente promedio es de $70,1 \pm 16,7$ (medio bajo), el nivel de seguridad operacional de $68,2 \pm 16,3$ (bajo) y la correlación entre estas variables es muy alta, $r=0,844$ ($r^2=0,712$; $p<0,001$). Además, se halló que el 71,2% de la seguridad operacional se podría explicar por el potencial de desempeño resiliente.

En el potencial de desempeño resiliente se encontraron diferencias significativas ($p<0,05$) en la escala general y las subescalas capacidad de respuesta (entrenamiento de personal operativo) y capacidad de monitoreo (entrenamiento de personal operativo y supervisión de procesos operativos) entre clúster de alta e intermedia incidentalidad; sin embargo, los tamaños del efecto atribuibles al clúster fueron bajos (0,010 y 0,015). En seguridad operacional los promedios altos fueron del clúster de mayor incidentalidad en aprendizaje, compromiso, legitimidad y adaptabilidad, mientras que el clúster intermedio puntuó con menor seguridad operacional. Seguidamente, se ajustaron modelos predictivos múltiple y logístico para la estimación de la seguridad operacional en función del potencial de desempeño resiliente.

A nivel cualitativo se obtuvo evidencia interpretativa para aproximar posibles configuraciones

organizacionales que dan cuenta de los hallazgos cuantitativos y que se constituyen en oportunidades de mejora de la seguridad operacional.

Se concluye que hay evidencia cuantitativa significativa y apreciativa de que el nivel de seguridad operacional y el potencial de desempeño resiliente no solo están relacionados en función directa, aunque no necesariamente lineal, sino que este último es predictor significativo de la seguridad operacional.

Palabras clave: Potencial de desempeño resiliente, seguridad operacional, gestión de la seguridad operacional, psicología aeronáutica.

Relationship Between Resilient Performance Potential and Operational Safety in a Military Aviation Organization: Contributing Organizational Factors

Abstract

The objective of this research is to analyze the relation between the resilient performance potential and the operational safety inside of a Colombian military aviation organization.

Based in a sequential explanatory design, 545 military pilots evaluated the organization with resilient performance potential scales (response capabilities, monitoring, learning and anticipation) and operational security (security components, security and operational management and safety culture). The incidentality clusters were grouped based in the functional relationship: $\text{Incidentality} = (\text{Number of flight hours} / \text{incident})$ and the level of operational participation was established based in the rank of the participants.

It was noted that the average resilient performance potential is 70.1 ± 16.7 (mid-low), the operational safety level is 68.2 ± 16.3 (low) and the correlation between these variables is too high, $r=0,844$ ($r^2=0,712$; $p<0,001$). Besides this, it was discovered that 71.2% of the operational safety could be explained by the resilient performance potential.

Significant differences ($p<0.05$) were found in the resilient performance in a general scale and in the response capability (training of operational personnel) and monitoring ability (training of operational personnel and operational processes supervision) subscales between the high and mid incidentality cluster; nonetheless, the effect sizes attributable to the cluster were low (0.010 and 0.015). In operational security, the highest average result was the cluster that had greater incidentality in learning, commitment, legitimacy and adaptability, meanwhile the midlevel cluster had a lesser score in operational safety. Afterwards, the logistical and multiple prediction models were adjusted in order to estimate the operational security based on the resilient performance potential.

At the qualitative level, appreciative evidence is gathered to understand the dynamics of safety

in relation to resilient organizational attitudes, identifying aspects that may constitute opportunities for improving safety.

It is concluded that there is significant and appreciative evidence that the level of safety and the potential for resilient performance are not only directly related, but the latter significantly predicts safety.

Keywords: Resilient performance potential, operational safety, operational security management, aeronautical psychology.

Agradecimientos

A Dios, en quien reposa toda fuente de sabiduría, conocimiento y paz para mi vida. Quien, en muchos momentos de oración, me dio la tranquilidad y dirección para llevar a término este proyecto personal.

A mi familia: mi amado esposo Juan Carlos por su amor, paciencia y apoyo en todo tiempo, quien con sus palabras y compañía se encargó de estar siempre presente, incluso cuando estaba ausente; a mis hijos Daniel Alejandro y David Leonardo que son mi inspiración para la vida; a Juliana Durán Farfán quien pronto hará parte de esta familia y me ha acompañado en cada paso de manera amorosa y genuina.

A mi institución, de la que hice parte durante veintidós años, y a aquellos que me dieron la acogida para realizar esta investigación. Una institución de la que jamás se deja de hacer parte porque es una gran familia: Ramsés Rueda, Alejandro Duarte, Luis Fernando Giraldo y su equipo de trabajo, Gustavo Castellanos y todos aquellos que intervinieron de una u otra manera en la realización de este proyecto ¡Sic itur ad astra!

Al Ps. Jesús Enrique Jaimes que apareció como una respuesta de la vida e hizo posible el desarrollo metodológico de esta investigación. Me brindó sus opiniones profesionales y su confianza personal. Gracias por cada argumento y por su disposición.

Al Dr. Mario Poy, Director de esta investigación, mi más profunda gratitud por su paciencia, disposición y transferencia generosa de conocimiento. Gracias por su pertinencia, por su claridad y por orientar el análisis de este trabajo de manera que fuese realmente un aporte a un área de la psicología que apasiona a quien apasiona.

Para finalizar, un agradecimiento sincero al Dr. Alejandro Castro Solano y su equipo docente, administrativo y logístico del Doctorado en Psicología de la Universidad de Palermo.

Dedicatoria

Oh, Jehová, tú me has examinado y conocido.

Tú has conocido mi sentarme y mi levantarme;

Has entendido desde lejos mis pensamientos.

Has escudriñado mi andar y mi reposo,

Y todos mis caminos te son conocidos,

Pues aún no está la palabra en mi lengua,

Y he aquí, oh, Jehová, tú la sabes toda.

Detrás y delante me rodeaste,

Y sobre mí pusiste tu mano.

Tal conocimiento es demasiado maravilloso para mí;

Alto es, no lo puedo comprender.

Sl 139:1-6 RV1967

Imelda

Tabla de Contenidos

	Pág.
Resumen.....	3
Abstract.....	5
Agradecimientos	7
Dedicatoria.....	8
Lista de Tablas	12
Lista de Figuras.....	15
Lista de Anexos.....	18
Lista de Acrónimos y Abreviaturas	19
Sección Teórica.....	1
1. Introducción	2
1.1 Campo Disciplinar	2
1.2 Problema de Investigación.....	5
2. Sistemas Sociotécnicos Complejos.....	8
2.1 Teoría General de los Sistemas.....	9
2.2 Sistemas Sociotécnicos Complejos.....	12
3. Seguridad Operacional en Organizaciones de Alto Riesgo	16
3.1 Evolución de los Modelos de Análisis de Accidentes	18
3.2 Enfoque de la Seguridad desde los Sistemas Sociotécnicos Complejos.....	24
3.3 Seguridad Operacional en la Institución de Aviación Militar	30
4. Ingeniería de la Resiliencia.....	40
4.1 Aproximación Conceptual	40
4.2 Fallos y Éxitos	43
4.3 Gestión de Riesgos y Amenazas	45

4.4 Responsabilidades de la Alta Dirección en el Enfoque de la Resiliencia.....	47
4.5 La Información.....	48
4.6 Potencial de Desempeño Resiliente y Seguridad.....	50
4.7 Potencial de Desempeño Resiliente e Incidentalidad	58
4.8 Trabajo Diseñado vs. Trabajo Real.....	59
5. Evaluación del Potencial de Desempeño Resiliente	62
5.1 Rejilla para el Análisis de Resiliencia	62
5.2 Otros Métodos de Evaluación de la Resiliencia	72
Sección Empírica	78
6. Marco Metodológico.....	79
6.1 Objetivo General.....	79
6.2 Objetivos Específicos.....	79
6.3 Hipótesis	80
6.4 Método	80
6.5 Muestra	81
6.6 Variables de Investigación.....	84
6.7 Instrumentos de Medición.....	86
6.8 Procedimiento	93
6.9 Plan de Análisis de los Datos.....	96
6.10 Consideraciones Éticas	100
7. Resultados	102
7.1 Caracterización Muestral	102
7.2 Definición de Clúster: Niveles de Incidentalidad Aérea.....	106
7.3 Potencial de Desempeño Resiliente: Comportamiento Muestral.....	107
7.4 Seguridad Operacional: Comportamiento Muestral	113

7.5 Análisis Diferencial en Función de los Clúster de Incidentalidad.....	117
7.6 Análisis Diferencial en Función del Nivel de Participación Operacional	126
7.7 Análisis Diferencial en Función del Tiempo en la Especialidad de Pilotaje	134
7.8 Análisis Correlacional: Relación Potencial de Desempeño Resiliente y Seguridad Operacional	141
7.9 Análisis Regresional: Modelamientos Predictivos de la Seguridad Operacional en Función del Potencial de Desempeño Resiliente	146
7.10 Análisis Cualitativo.....	151
7.11 Re-análisis de la Potencia (power).....	169
8. Discusión.....	172
8.1 De la Relación entre Potencial de Desempeño Resiliente y Seguridad Operacional. (Hipótesis 1 y 4).....	172
8.2 De la Relación del Potencial de Desempeño Resiliente y la Seguridad Operacional con otras Variables de Estudio. (Hipótesis 2, 3 y complementarias).	177
8.3 De los Hallazgos Derivados del Diseño.....	179
8.4 Discusión Final	181
8.5 Limitaciones y Futuras Líneas de Investigación.....	183
9. Conclusiones y Recomendaciones.....	186
9.1 Conclusiones	186
9.2 Recomendaciones	189
Referencias.....	191
Anexos	199

Lista de Tablas

	Pág.
Tabla 1 Método de Trist para el análisis de un sistema sociotécnico	15
Tabla 2 Esquema para el análisis de riesgo y decisión	27
Tabla 3 Tipología de los eventos de seguridad operacional en la entidad.....	33
Tabla 4 Estructura de la seguridad operacional	56
Tabla 5 Capacidad para responder	65
Tabla 6 Capacidad para monitorear	67
Tabla 7 Capacidad para aprender.....	69
Tabla 8 Capacidad para anticipar.....	71
Tabla 9 Definición operacional de variables	84
Tabla 10 Validación de contenido escala PoDeRe: concordancia de jueces y claridad de los ítems.....	86
Tabla 11 Análisis de consistencia interna: Alpha de Cronbach de las subescalas y la escala PoDeRe	89
Tabla 12 Estadísticos de validación del análisis factorial de componentes principales de las escalas	90
Tabla 13 Validación de contenido escala SegOp: concordancia de jueces y claridad de los ítems	91
Tabla 14 Análisis de consistencia interna: Alpha de Cronbach de las subescalas y la escala PoDeRe	92
Tabla 15 Ordenamiento de las unidades según horas de vuelo / incidente para la conformación de clúster de incidentalidad.....	106
Tabla 16 Frecuencia de respuesta en la categoría “No sabe” de las escalas.....	108

Tabla 17 Estadísticas de la escala y subescalas de potencial de desempeño resiliente PoDeRe en la entidad militar	109
Tabla 18 Categorías de escala y subescalas del potencial de desempeño resiliente en la entidad militar.....	111
Tabla 19 Estadísticas de la escala de seguridad operacional SegOp y sus componentes	114
Tabla 20 Categorías de escala y subescalas de seguridad operacional en la entidad militar.	116
Tabla 21 Distribución y prueba de homogeneidad de varianza de las variables de medida..	118
Tabla 22 Promedios de la escala PoDeRe diferenciados según clúster de incidentalidad.....	119
Tabla 23 Pruebas de Anova para los promedios de la escala PoDeRe según los clúster de incidentalidad y los respectivos tamaños del efecto	121
Tabla 24 Promedios de la escala SegOp diferenciados según clúster de incidentalidad	123
Tabla 25 Anova para los promedios de la escala SegOp según clúster de incidentalidad.....	125
Tabla 26 Promedios de la escala PoDeRe diferenciados según el nivel de participación operacional.....	126
Tabla 27 Pruebas de Anova para los promedios de la escala PoDeRe según nivel de participación operacional y los respectivos tamaños del efecto	129
Tabla 28 Promedios de la escala SegOp diferenciados según nivel de participación operacional	130
Tabla 29 Anova para los promedios de la escala SegOp según rango jerárquico	132
Tabla 30 Pruebas inferenciales de las escalas PoDeRe y SegOp según el nivel de participación operacional, niveles 1° y 2° vs el nivel 3°	133
Tabla 31 Promedios de escala PoDeRe diferenciados según tiempo en la especialidad de pilotaje.....	135
Tabla 32 Pruebas de Anova para promedios de la escala PoDeRe según el tiempo en la especialidad de pilotaje y los respectivos tamaños del efecto	137

Tabla 33 Promedios de la escala SegOp según el tiempo en la especialidad de pilotaje	138
Tabla 34 Anova para los promedios de la escala SegOp según tiempo en la especialidad de pilotaje.....	140
Tabla 35 Matriz correlacional entre potencial de desempeño resiliente y seguridad operacional y sus respectivas subescalas.....	142
Tabla 36 Modelo predictivo de seguridad operacional en función del potencial de desempeño resiliente.....	147
Tabla 37 Modelo predictivo step waise forward de la seguridad operacional en función de las capacidades del desempeño resiliente.....	148
Tabla 38 Modelo logístico de estimación de la seguridad operacional en función de predictores del potencial de resiliencia.....	149
Tabla 39 Participantes en los grupos focales y las entrevistas.....	151
Tabla 40 Configuraciones organizacionales para el potencial de desempeño resiliente y la seguridad operacional	155
Tabla 41 Configuraciones organizacionales para capacidad de anticipación.....	157
Tabla 42 Configuraciones organizacionales para la capacidad para aprender	159
Tabla 43 Configuraciones organizacionales para gestión de la información	160
Tabla 44 Configuraciones organizacionales para las asociaciones por clúster de incidentalidad	162
Tabla 45 Configuraciones organizacionales para comprender los hallazgos para nivel de diseño de operaciones vs. operadores: Comparación por antigüedad militar.	166
Tabla 46 Configuraciones organizacionales para resiliencia y seguridad	168

Lista de Figuras

	Pág.
Figura 1. Interrelación recíproca de los tres sistemas. Modelo de Kingdon, 1973.....	14
Figura 2. Teoría del dominó de Heinrich.....	20
Figura 3. Modelo del factor actitudinal de Heinrich.....	20
Figura 4. Modelo de queso suizo.....	21
Figura 5. Categorización de resultados operacionales.....	28
Figura 6. Relación gestión de riesgos y garantía de la seguridad. S.....	32
Figura 7. Árbol relacional de los factores de riesgo y los eventos de seguridad operacional. 37	
Figura 8. Esquemmatización de la dinámica de la seguridad	55
Figura 9. Modelo de la tarea prescrita.	60
Figura 10. Modelo de Van der Vorm, et al. (s.f.).	63
Figura 11. Método FRAM..	73
Figura 12. Factores contribuyentes de éxito modelo REWI.....	75
Figura 13. Cálculo del tamaño muestral	83
Figura 14. Esquemmatización del comportamiento del constructo escalar potencial de desempeño resiliente.....	88
Figura 15. Esquemmatización del plan aplicado de la investigación	96
Figura 16. Distribución muestral según el rango jerárquico de los oficiales participantes ...	103
Figura 17. Distribución muestral de las bases operacionales de procedencia	104
Figura 18. Distribución muestral según el tiempo de experiencia de vuelo	104
Figura 19. Distribución muestral de la experticia como oficial de seguridad operacional....	105
Figura 20. Distribución muestral según el tiempo de experiencia en cargos de seguridad ...	105
Figura 21. Distribución de la muestra de pilotos en clúster de incidentalidad	107
Figura 22. Perfil de desempeño resiliente de la entidad militar.....	110

Figura 23. Categorías de escala y subescalas del potencial de desempeño resiliente de la entidad militar.....	112
Figura 24. Perfil de componentes de la seguridad operacional	115
Figura 25. Categorías de subescalas y escala de seguridad operacional en la entidad militar	116
Figura 26. Subescalas de la escala PoDeRe según los clúster de incidentalidad.....	120
Figura 27. Promedios de las subescalas de la escala PoDeRe según los clúster de incidentalidad	120
Figura 28. Subescalas de la escala SegOp según clúster de incidentalidad.....	124
Figura 29. Promedios de las subescalas de la escala SegOp según los clúster de incidentalidad	124
Figura 30. Subescalas de la escala PoDeRe según el nivel de participación operacional	128
Figura 31. Promedios de subescalas de PoDeRe según el nivel de participación operacional	128
Figura 32. Subescalas de la escala SegOp según el nivel de participación operacional.....	131
Figura 33. Promedios de las subescalas de la escala SegOp según el nivel de participación operacional.....	131
Figura 34. Subescalas de la escala PoDeRe según el tiempo en la especialidad de pilotaje .	136
Figura 35. Promedios de subescalas de PoDeRe según el tiempo en la especialidad de pilotaje	136
Figura 36. Subescalas de la escala SegOp según el tiempo en la especialidad de pilotaje....	139
Figura 37. Promedios de las subescalas de la escala SegOp según el tiempo en la especialidad de pilotaje.....	140
Figura 38. Scatterplot de potencial de desempeño resiliente y la seguridad operacional en los clúster de incidentalidad	144

Figura 39. Scatterplot entre las dimensiones del potencial de desempeño resiliente y la seguridad operacional de la entidad militar	145
Figura 40. Análisis Cualitativo: Mapeo de la estructura categorial y segmentación codificada	153
Figura 41. Nube de códigos: Análisis categorial de la visión interpretativa de la seguridad operacional en torno al potencial resiliente	154
Figura 42. Re-cálculo de la potencia (power) de la investigación	170

Lista de Anexos

	Pág.
Anexo A. Cronograma Inicial de Ejecución	200
Anexo B. Descripción de Eventos de Incidentalidad/Accidentalidad de la Entidad de Aviación (Años 2015-2017)	201
Anexo C. Escala PoDeRe	205
Anexo D. Instrumento para Validación de Expertos de la Escala PoDeRe.....	208
Anexo E. Escala SegOp	213
Anexo F. Instrumento para Validación de Expertos Escala SegOp.....	215
Anexo G. Guía para la Realización de Grupos Focales y Entrevistas Semiestructuradas.	220
Anexo H. Consentimiento Informado.....	223
Anexo I. Respuestas Directas de los Ítems de la Escala PoDeRe.....	224
Anexo J. Respuestas Directas de los Ítems de la Escala SegOp y sus Subescalas	226
Anexo K. Análisis Cualitativo: Informe resumen de Segmentos Codificados (editado) ..	228

Lista de Acrónimos y Abreviaturas

APA: American Psychological Association.

EVESO: Evento (s) de seguridad operacional.

HFACS: Human Factors Analysis and Classification System

NOOPER: Novedad operacional.

OACI: Organización de Aviación Civil Internacional.

PoDeRe: Escala de Potencial de Desempeño Resiliente.

RAG: Rejilla de Análisis de la Resiliencia (Resilience Analysis Grill).

RECIL: Evento de seguridad operacional que afectó equipo recuperable, con personal ileso

RELES: Evento de seguridad operacional que afectó equipo recuperable, con personal lesionado.

RR: Riesgo relativo.

SegOp: Escala de Seguridad Operacional.

Sección Teórica

Capítulo

1. Introducción

A manera de introducción tanto en la temática de la psicología de aviación como parte de la psicología del trabajo, como de la investigación, se describe este campo disciplinar como ámbito científico y luego se formula el problema investigativo que se aborda en el estudio.

1.1 Campo Disciplinar

El reconocimiento del carácter científico de la psicología industrial o del trabajo, lo realiza la American Psychological Association (APA) en 1944, vinculando su objeto de estudio al entendimiento de los fenómenos psicológicos individuales dentro de las organizaciones, la comprensión del impacto de los procesos organizacionales en las personas y las relaciones entre productividad y bienestar de los trabajadores (Gómez, 2016).

Sin embargo, históricamente esta relación surge a finales del siglo XIX y comienzos del XX vinculada a la eficiencia en los negocios y la industria, con una clara dirección en torno a los procesos de selección de personal, metodologías para incrementar la eficiencia en el trabajo y su aplicación en el campo del mercadeo y la publicidad (Gómez, 2016).

Este desarrollo se extendió también a las organizaciones de aviación como respuesta a las demandas del cambio social y tecnológico que se produjo a finales del siglo XIX y principios del XX. Más específicamente, este campo aplicado fue impulsado por las circunstancias militares que trajo consigo la I Guerra Mundial, aunque antes de este hecho, en algunos países europeos, la psicología estaba al servicio del mundo aeronáutico en los procesos de selección de pilotos (Saíz y Saíz, 2012).

Para Saíz y Saíz (2012) este énfasis en los procesos de selección caracterizó los desarrollos iniciales de la psicología durante las primeras décadas del siglo XX. Su principal enfoque fue establecer las aptitudes que debían poseer los aviadores, estudiando los aspectos que les afectaba durante el vuelo (oxígeno, luminosidad, ruido, vibración, altitud, aceleración,

velocidad, entre otras) y cómo funcionaban los procesos psicológicos que debían estar presentes en la conducción del avión (procesos perceptuales básicos relacionados con la visión, percepción espacial, orientación, audición y sentido vestibular), con objeto de poder producir protocolos y herramientas de selección que evitaran posibles accidentes.

Para la década de los treinta, estos avances llevaron a la construcción de mejores simuladores de vuelo, la creación de dispositivos para la medición del sentido del equilibrio o el sentido vestibular y aparecieron diversos instrumentos para medir temas como la adaptación, la capacidad de control, la concentración interna y la fatiga (Saíz y Saíz, 2012).

Aunque los avances mostrados en ese campo eran claros, se hizo evidente la inconveniencia de centrar la responsabilidad de los siniestros aéreos en los fallos o aciertos del piloto. La selección buscaba un individuo preparado para conducir con eficacia una aeronave, pero no se tenían en cuenta limitaciones físicas y anatómicas que llevaban a la comisión de errores y esto cuestionaba la precisión de la evaluación psicotécnica como herramienta de prevención (Saíz y Saíz, 2012).

En el periodo entre guerras –desde 1918 hasta 1939– se da un crecimiento importante de la aviación comercial que opaca el desarrollo de la aviación militar y trajo consigo un progreso tecnológico en el mundo de la aviación. Posiblemente por esta razón, autores como Roscoe (1980) vinculan el origen de la psicología aplicada a la aviación en los comienzos de la II Guerra Mundial, en Inglaterra, centrado en el uso temprano de escalas de factores humanos para enfrentar problemas de diseño en los equipos.

Uno de los pioneros en la ingeniería de los factores humanos fue el psicólogo estadounidense Alphonse Chapanis quien combinó su interés en la investigación psicológica básica en visión y percepción con aplicaciones al diseño de ingeniería, interés que se incrementó durante la Segunda Guerra Mundial y llevó en 1949 a la publicación del libro “Psicología Experimental Aplicada: Factores Humanos en Diseños de Ingeniería”, escrito en

compañía de dos colegas suyos, Garner y Morgan (Pew, 2010).

Según Roscoe (1980), la persona que tuvo mayor influencia en el surgimiento de la psicología de aviación como ciencia sistemática fue Alexander Coxe Williams, Jr., quien estableció en 1946 un laboratorio de psicología de aviación en la Universidad de Illinois. Sus aportes en la primera década de investigación (1946 a 1955) se relacionaron con la transferencia en el entrenamiento de pilotos, la definición de los fundamentos conceptuales para el análisis de la misión y la investigación del desempeño de pilotos.

Independientemente de las diversas aplicaciones iniciales, la misma naturaleza de la ciencia psicológica la unió sólidamente al individuo y su desempeño. Para Roscoe (1980), las investigaciones psicológicas cubrían problemas considerados como reales en el mundo de la aviación; aspectos que iban desde los factores humanos involucrados en el diseño hasta la operación de los sistemas de aviación y la predicción del desempeño del piloto.

Pese a estas contribuciones de indiscutible importancia y al avance tecnológico que caracterizaba la aviación, desde la década de los setenta las investigaciones de accidentes aéreos señalaban al hombre como la causa principal de los siniestros y esto llevó a la ciencia psicológica a dirigirse hacia la comprensión de las circunstancias y razones del error humano con el fin de prevenirlo (Sebastián, 2009).

Sin embargo, pronto este interés también se fue transformando por cuanto estos modelos explicativos atomizaban una realidad por demás compleja. El poder explicativo de los modelos centrados en fenómenos psicológicos individuales era insuficiente para dar cuenta de la complejidad de hechos y situaciones involucradas en un siniestro aéreo, de modo se adoptó una visión sistémica de la seguridad operacional (Hollnagel, 2006).

Por lo anterior, y en el mismo sentido planteado por Poy (2006), la intención de este documento es enriquecer la comprensión de las interacciones entre acciones humanas, organización y seguridad operacional dejando atrás los modelos lineales que reducen la visión

a causas inmediatas entre variables, para adoptar abordajes de mayor complejidad en seguridad operacional.

La resiliencia organizacional es el modelo tomado para lograr este objetivo cuyos principios fundamentales fueron expuestos en el libro “Resilience engineering: concepts and precepts”, editado por Erik Hollnagel, David Woods y Nancy Leveson en 2006 (Hollnagel, Woods y Leveson, 2006).

Cabe aclarar que el marco conceptual de esta investigación no se relaciona con el abordaje psicológico de la resiliencia como fenómeno individual dentro de la organización, sino de la resiliencia como fenómeno sistémico en el que distintos componentes de la organización interactúan para generar capacidades organizacionales resilientes que le permitan al sistema, en su totalidad, hacer frente a situaciones inesperadas y/o anticiparlas para no afectar su funcionamiento normal o recuperarse rápidamente una vez ha sufrido una perturbación.

1.2 Problema de Investigación

Para los expertos en seguridad es un hecho visible que en los últimos años se ha dado una ampliación del alcance de la investigación de accidentes a través de diferentes sectores de alto riesgo. En los años sesenta, cuando la participación del error en grandes desastres empezaba a llamar la atención, se pensaba que la más baja contribución (20%) correspondía al factor humano y el 80% se debían a factores físicos o técnicos (Reason, 2011).

Después de 1990, frente a la mejora en los materiales, tecnología y procedimientos de ingeniería se invirtieron los porcentajes de participación, de manera que el factor humano adquirió otra connotación: la colisión entre dos aviones Boeing 747 en el aeropuerto “Los Rodeos” en marzo de 1977 en el que fallecieron todos los ocupantes del KLM (248 personas) y 335 de las 396 del Pan Am, el accidente nuclear de Chernóbil en abril de 1986 cuya controversia sobre el cálculo de víctimas está vigente hoy y muchos otros eventos catastróficos, pusieron en la mira de los expertos la decisiva participación de los factores

humanos en la ocurrencia de accidentes en sectores de alto riesgo (Reason, 2011).

Es así como en el mundo de la aviación se intensifica el interés científico por comprender y mejorar la gestión de la seguridad operacional, prevenir accidentes e incidentes y perfeccionar la seguridad de los sistemas (Woods y Hollnagel, 2006).

En 1988, un Airbus A-320 se accidentó mientras realizaba una revista aérea en una población francesa; tres personas murieron y otras 133 resultaron heridas. En 1990, otro Airbus se estrelló cerca del aeropuerto de destino en Bagalone, India; murieron 92 personas. En 1992, otro desastre ocurre en la cordillera de los Vosgos y 87 personas perdieron la vida. En 2006, 113; en 2007, 199; en 2014 un avión de Malasya Airlines desaparece con 239 personas a bordo; en 2015, 116 mueren en un accidente aéreo en Mali y un copiloto accidenta intencionalmente la aeronave causando 150 decesos. Esto por mencionar algunas de las grandes catástrofes aéreas del mundo.

Lograr un acercamiento adecuado al tema de la accidentalidad y la gestión de la seguridad operacional (cara y contracara del mismo fenómeno) no resulta una tarea sencilla. Sebastián (2009) plantea que tanto el análisis del error humano como la confiabilidad de la actuación humana, es un tema que reviste gran complejidad en el que es conveniente considerar que el individuo actúa siempre por y desde un amplio número de variables personales, organizacionales, situacionales y ambientales que hacen parte de una causalidad por demás compleja.

A este argumento se le añade que los accidentes rara vez ocurren porque una sola cosa salga mal o como no estaba planeada; sin embargo, la postura teórica que soporta esta investigación es que los accidentes no son inevitables. Es necesario alcanzar una comprensión aguda acerca de por qué ocurren para encontrar formas efectivas de contenerlos, pero esa comprensión solo se da cuando se cambia la manera de pensar acerca de lo que son los accidentes (Hollnagel, 2009).

Para Hollnagel (2009), un accidente puede definirse como un evento o un acontecimiento corto, súbito e inesperado, producto directo o indirecto de una acción humana que conduce a un resultado no deseado.

De hecho, se considera que los eventos no deseados son también producto del azar (Hollnagel, 2009; Reason, 2011), por ende, ni los accidentes ni los no accidentes hablan por sí mismos de la resiliencia del sistema. Así las cosas, la resiliencia es un paradigma distinto para abordar la seguridad que se enfoca en el desarrollo de capacidades que hacen posible anticipar posibles perturbaciones en el funcionamiento del sistema y, por tanto, disminuir la ocurrencia de eventos no deseados.

Para Rae y Provan (2019), trabajar en seguridad es trabajar en un fenómeno social complejo, en el que las acciones dentro de la organización cumplen una función tanto instrumental -logro de objetivos-, como expresiva; es decir, marcan una distinción entre “estar seguro” y “sentirse seguro”. Otros autores (Hollnagel, 2015) parecen priorizar la función instrumental de la seguridad, es decir, el mejoramiento de los resultados de seguridad.

Sin embargo, algunas organizaciones han realizado millonarias inversiones en la mejora de sus sistemas de gestión de la seguridad sin disminuir significativamente la ocurrencia de accidentes. Esto muestra que la gestión de la seguridad operacional puede llegar a tener un componente expresivo (número de eventos), pero su verdadero valor radica en el potencial de la actuación en seguridad para modificar las estructuras que mantienen las creencias y no en la capacidad de esa acción para llegar a prevenir accidentes (Rae y Provan, 2019).

De allí surge este estudio cuya pregunta central de investigación es: ¿Qué relación existe entre el potencial de desempeño resiliente y la seguridad operacional en una organización de aviación militar colombiana y cuáles factores organizacionales contribuyen a la comprensión de esta relación?

Capítulo

2. Sistemas Sociotécnicos Complejos

El principal rastro del pensamiento positivista en el paradigma científico mecanicista fue la tendencia a descomponer un fenómeno en estudio en partes con el fin de observar sus actividades en procesos más pequeños de categoría heterogénea. Esta tendencia estuvo presente hasta mitad del siglo VIII, pero sus consecuencias se recogerían hasta el siglo XX (Morin, 1990), pues se llegó a un reduccionismo científico en el que las ciencias naturales se convirtieron en un modelo de cientificidad basado en datos que respondía a postulados del positivismo (Flórez y Tomas, 1993).

Como resultado de esto, las ciencias en sus diversas áreas de conocimiento generaban principios universales circunscritos a sus propios postulados, pues respondían a construcciones científicas limitadas, exclusivas y, de alguna forma, fragmentadas (Flórez y Tomas, 1993).

La teoría general de los sistemas surgió como una propuesta paradigmática que pretendía romper esta manera de ver el mundo para acceder a una realidad completa, compleja, unificadora y total (Von Bertalanffy, 1989).

Se consolida así una ruptura entre, por un lado, el ideal de reducción y/o simplificación como manera legítima y deseable para conocer, apropiarse y transformar un mundo que se considera ya hecho y susceptible de explicar y, por otro, la complejidad que no reduce ni simplifica, sino que asume el reto de la multidiversidad y el carácter inacabado del mundo circundante (Torres, s.f.).

Este movimiento paradigmático no fue ajeno a la psicología: la concepción clásica trataba de resolver fenómenos humanos dividiéndolos en unidades, tales como sensaciones, síntomas, estados de conciencia. Sin embargo, la psicología de la Gestalt mostró la existencia y preponderancia de todos psicológicos que no son suma de unidades elementales y que están

gobernados por leyes dinámicas (Von Bertalanffy, 1989). Desde esta mirada epistemológica se aborda el problema de investigación planteado.

En el siguiente apartado se realiza un resumen de los principales postulados y principios generales de la teoría de sistemas, pues es necesario entrar en este orden de pensamiento para acceder a la comprensión de la gestión de la seguridad al interior de una dinámica sistémica propia de un sistema abierto: la organización.

Las organizaciones de alto riesgo se consideran sistemas sociotécnicos complejos, por tanto, el capítulo finaliza ampliando este concepto en que se circunscribe la acción de la seguridad.

2.1 Teoría General de los Sistemas

Para Von Bertalanffy (1989) esta teoría pretende ser general e integrativa en el sentido de que es posible aplicar sus abstracciones y modelos conceptuales a fenómenos diversos, en tanto ciencia de los sistemas, pero como filosofía de los sistemas, se convierte en un nuevo paradigma para observar el mundo.

La teoría, como epistemología, establece la distinción entre los objetos observados en tanto sistemas reales y las construcciones conceptuales, simbólicas y/o mentales que se hacen de ellos. Las cosas que percibe un observador no son solo datos, sino producto de múltiples factores endógenos y exógenos que determinan la manera de leer el fenómeno observado. Aquí se establece una diferencia radical entre la epistemología de los sistemas y la epistemología positivista, según la cual, la percepción y/o el dato es una reflexión de un hecho real (Von Bertalanffy, 1989).

Este aspecto también fue señalado por Von Foerster (2006), considerado en mucho el padre de la cibernética, quien plantea que cuando se quiere conocer la naturaleza de los objetos, es importante recordar que ni los objetos ni las leyes que los rigen están simplemente allí; ambos aparecen, emergen y el observador está inmerso en esa aparición y debe ocuparse de los

procesos mentales que los generan.

En este sentido, la teoría de los sistemas aporta una visión organísmica a la biología moderna que conduce a resolver los problemas al interior de la organización y del orden que unifica las partes o elementos del sistema como producto de su interacción dinámica, postura que lleva a una observación diferente cuando se analizan las partes aisladas o el todo (Von Bertalanffy, 1989).

Así lo sostiene Stingfellow (2010) que plantea que los sistemas complejos solo pueden ser entendidos como sistemas, examinando su totalidad. Muchas características clave de un sistema son fenómenos emergentes y solo pueden ser analizados desde la perspectiva sistémica; es decir, en la comprensión de sus interacciones dinámicas evidenciadas en la diferencia de conducta de las partes aisladas, dentro del concepto de organización.

Estas consideraciones, entre otras, caracterizan esta forma de abordar el mundo que formula principios válidos para sistemas en general, sea cual fuere la naturaleza de sus componentes y las fuerzas interactivas o de organización presentes en ellas, por tanto, los sistemas humanos y sociales podrían entonces ser comprendidos a través de problemas de orden, organización, totalidad, teleología, excluidos prácticamente de la ciencia mecanicista.

2.1.1 Principios fundamentales de los sistemas. La existencia de modelos, principios y leyes aplicables a sistemas, sin importar su género, llevó a plantear que existen modelos, principios y leyes generalizadas que constituyen el punto de arranque para la teoría general de los sistemas.

Los desarrollos teóricos de la teoría general de los sistemas llevarían con el tiempo a plantear la teoría de los sistemas abiertos, producto de una expansión de la teoría física y la generalización de los principios cinéticos y de la teoría termodinámica haciendo manifiesto que en las ciencias sociales y del comportamiento, resultan aplicables expresiones y modelos matemáticos (Von Bertalanffy, 1989).

La característica más importante de los sistemas abiertos es que se mantienen en continua incorporación y eliminación de materia sin alcanzar un estado de equilibrio tal y como se conoce en la física; sin embargo, sí llegan a un estado uniforme (Von Bertalanffy, 1989).

En este punto es pertinente mencionar brevemente algunos conceptos que son fundamento de la teoría y que hacen parte del entendimiento sistémico de un fenómeno observado. El ambiente es el área de sucesos que influyen el comportamiento de un sistema debido a que este último absorbe selectivamente aspectos del primero; sin embargo, existe un límite nominal o frontera que separa al sistema de su entorno y define lo que le pertenece y lo que no (Arnold y Osorio, 1998).

En su estructura, un sistema está conformado por subsistemas o conjunto de elementos y relaciones que tienen su propia estructura y funciones, pero comparten las mismas propiedades del sistema mayor (sinergia) y su delimitación depende del observador. La sinergia es resultado de las interacciones internas del sistema e implica que la observación de sus partes aisladas no puede explicar el comportamiento del sistema (Arnold y Osorio, 1998).

La relación entre elementos del sistema o en su intercambio con el medio ambiente, es de carácter circular. Esto significa que algo que no sucede desde el punto de vista material y energético, puede ser un evento desde el punto de vista de la información (Von Foerster, 2006). Se entiende del modo: “cuando A causa B y B causa C, pero C causa A, luego A en lo esencial, es autocausado” (Arnold y Osorio, 1998).

La complejidad es otro concepto fundamental. No sólo indica la cantidad de elementos del sistema, sino también sus interacciones actuales, potenciales y el número de estados posibles que se producen a partir de ellas. Las interrelaciones más o menos estables que se da entre los componentes del sistema constituyen la estructura del sistema (Arnold y Osorio, 1998).

Según la segunda ley de la termodinámica, los sistemas tienden a un estado progresivo de desorganización hasta su homogenización con el ambiente, a lo que se llama entropía. Sin

embargo, hay sistemas que, temporalmente, revierten esa tendencia (negentropía) a partir de la importación de energía del ambiente para incrementar sus estados de organización (Arnold y Osorio, 1998).

Una manera de generar su supervivencia es a través de procesos de retroalimentación, mediante los cuales el sistema absorbe información para regular su comportamiento. Igualmente, aplica el principio de recursividad, a partir del cual el sistema introduce en sí mismo sus propios resultados.

Según los postulados de la teoría, un sistema abierto llega al mismo estado final a partir de diferentes condiciones iniciales y diversas vías (equifinalidad) y ese estado final es siempre un estado de equilibrio que se alcanza a partir de intercambios de recursos con el ambiente (input) que pone marcha el ciclo de actividades del sistema con el fin de cumplir una función (output) (Arnold y Osorio, 1998).

Un sistema abierto tiene una organización que da cuenta del patrón de relaciones que definen sus estados posibles (variabilidad); producto de esta variabilidad, se originan las emergencias, es decir, otro sistema cualitativamente diferente producto de la descomposición de sistemas en unidades menores. Ante variaciones surgen también los procesos homeostáticos o compensaciones internas que bloquean, reemplazan o integran los cambios con el fin de mantener intacta la estructura del sistema (Arnold y Osorio, 1998).

Sin pretender ser exhaustivo, esta es la complejidad a la que alude el intento de realizar un abordaje sistémico de un fenómeno en estudio, en este caso, la seguridad operacional.

2.2 Sistemas Sociotécnicos Complejos

El concepto de sistemas sociotécnicos fue desarrollado por el Instituto Tavistock de Relaciones Humanas en Inglaterra en la década de los 50 y surgió ante la necesidad de diseñar organizaciones que integraran exitosamente los sistemas técnicos/tecnológicos con los sistemas sociales/humanos. Hoy en día, se asocia al diseño de lugares de trabajo que

promueven innovación, calidad de vida laboral, sistemas de trabajo de alto desempeño y sistemas de trabajo sostenible (Thomassen, Hegen y Strand, 2017).

Emery (1959, como se citó en Manrique y González, 2013) describe el sistema sociotécnico como un sistema abierto que, a pesar de su heterogeneidad y complejidad, tiene la capacidad de reorganizarse espontáneamente y retornar a su estabilidad funcional.

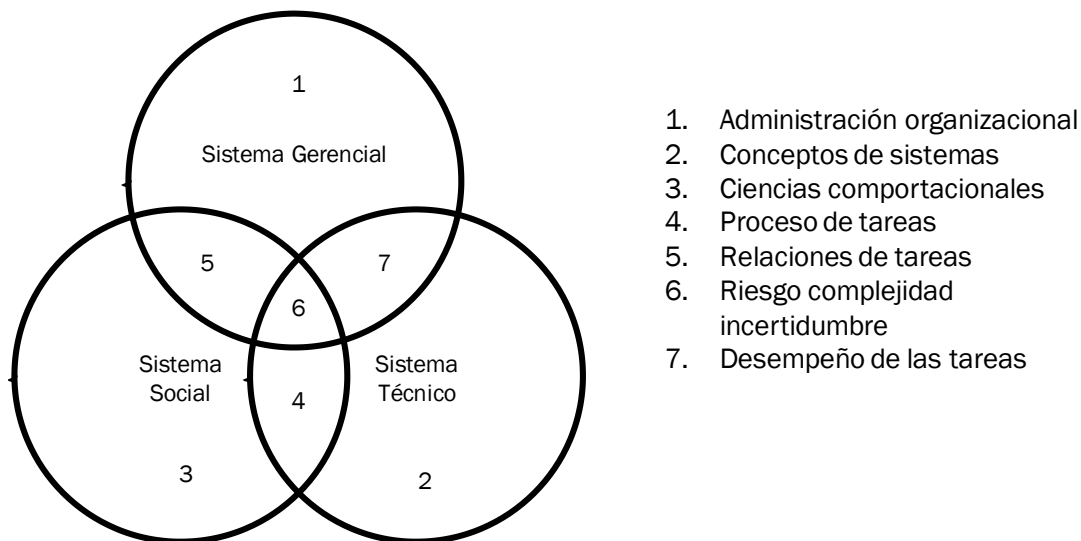
Esa condición y su dinámica interna es la que lo define como complejo. Concretamente, un sistema complejo es un conjunto de componentes que entran en interacción y crean propiedades que no se encuentran en los elementos aislados; esa complejidad es proporcional al número de elementos en interacción, al número de interacciones y a la complejidad intrínseca de los elementos y las interacciones (Torres, s.f.).

Al interactuar con los entornos físicos y regulatorios resulta en una dinámica compleja de retroalimentación. El efecto acumulativo de las interacciones no lineales e interconectadas entre las personas y el ambiente hace que estos sistemas sean potencialmente frágiles y susceptibles de fallas, generando condiciones emergentes difíciles de anticipar y controlar (Venkatasubramanian, Luo y Zhang, 2019).

Otro aspecto relacionado con el concepto de sistema sociotécnico es que fue concebido originalmente como un sistema operativo y no de regulación (Manrique y González, 2013). Esto significa que las necesidades del sistema y los trabajadores son interdependientes y que es importante capacitar y empoderar a los trabajadores para que participen en el diseño e implementación de los sistemas (Thomassen, Heggen y Strand, 2017).

Leal (2002) propone la existencia de tres aspectos necesarios para que una organización pueda ser considerada dentro del enfoque sociotécnico (Figura 1): (1) un sistema técnico o de tareas constituido por el flujo de trabajo, la tecnología y los procedimientos de operación tecnológica requeridos para el logro de los objetivos organizacionales; (2) un sistema gerencial/administrativo responsable de la organización y sus procesos de toma de decisiones

y (3), un sistema social que está relacionado con la cultura organizacional y la satisfacción de necesidades personales, en donde se desarrolla el soporte para el flujo de información que alimenta al sistema técnico.



Fuente: Tomado de Manrique y González, 2013

Figura 1. Interrelación recíproca de los tres sistemas. Modelo de Kingdon, 1973. Las organizaciones dentro de un enfoque sociotécnico están constituidas por tres subsistemas principales. Este enfoque sigue vigente y favorece la generación, transferencia e integración del conocimiento organizativo y, como consecuencia, mejora la eficiencia y efectividad de la gestión empresarial.

Una de las utilidades investigativas dadas a este concepto está relacionada con estudios para mejorar la seguridad dentro de los sistemas sociotécnicos con enfoque en los factores humanos y la ergonomía (HFE, Human Factors and Ergonomics) cuyo foco es la persona en su ambiente de trabajo y su influencia en las capacidades y aspiraciones del individuo para mejorar su desempeño (Murphy, Huang, Robertson, Jeffries y Danoff, 2018).

Murphy et al. (2018) consideran que existe evidencia investigativa sólida que muestra que el desempeño puede ser impactado de manera positiva a través de cambios en diversos componentes del sistema y esto plantea un claro cambio de enfoque de la seguridad por cuanto se deja de lado al operador y se centra en los elementos del sistema.

Con el fin de conocer cómo se provoca ese impacto, Trist (1981, como se cita en Manrique y González, 2013) sugiere seguir una secuencia de pasos ordenados que constituyen un método para analizar sistemas sociotécnicos (tabla 1).

Tabla 1

Método de Trist para el análisis de un sistema sociotécnico

Fase	Detalle
1. Descripción	Revisar los principales aspectos técnicos y sociales del sistema.
2. Proceso	Revisar las operaciones de la unidad hombre-máquina (transformaciones).
3. Indicadores	Examinar las diferencias clave y sus interrelaciones. (1) afecta la cantidad y calidad de la producción. (2) Funcionamiento social y costos de producción.
4. Sistema Social	Determinar hasta qué punto las diferencias clave son controladas por el sistema social (trabajadores, supervisores, gerentes).
5. Percepción de los trabajadores	Investigar la percepción social de los miembros acerca de sus roles y sus posibilidades.
6. Límite	Examinar sistemas vecinos.
7. Input y output	Considerar los sistemas de cruce en la entrada y salida, es decir, sistemas proveedores y usuarios.
8. Contexto	Analizar el sistema de destino y sus vecinos, en cuanto a los efectos de las políticas o planes de desarrollo de naturaleza técnico social.

Fuente: Tomado de Manrique y González, 2013.

Entender las organizaciones a través de este paradigma imprime una mecánica de orden y aporta una visión más amplia para abordar las situaciones particulares y desentrañar la íntima interrelación e interdependencia entre el sistema técnico, responsable de la eficiencia potencial de la organización, y el sistema social, que transforma esa eficiencia potencial en eficiencia real.

Capítulo

3. Seguridad Operacional en Organizaciones de Alto Riesgo

El objetivo de este capítulo es presentar la evolución de los abordajes de la seguridad operacional y para ello, en un primer apartado se presenta la perspectiva tradicional de la seguridad. Seguidamente, la visión de la seguridad operacional desde la perspectiva de los sistemas sociotécnicos complejos y, a modo de cierre, se describe el manejo de la seguridad en la institución militar que contextualiza el presente estudio y sus principales retos a partir del análisis de eventos ocurridos en un lapso específico.

Dentro de los sistemas complejos, una organización se cataloga como de alto riesgo o de alta fiabilidad cuando un accidente ocurrido durante su funcionamiento puede generar una catástrofe humana o ambiental de consecuencias difíciles de valorar. Organizaciones de este tipo son las plantas nucleares, químicas, petroleras y las industrias de transporte masivo, entre ellas, la aviación (Martínez, Gracia y Peiró, 2018).

Desastres ocurridos en estos sectores han trazado la evolución de la seguridad operacional. Por citar uno, el accidente en la planta nuclear Chernóbil llevó a incursionar en el concepto de cultura de la seguridad y dejó grandes enseñanzas; unas centradas en aspectos técnicos, tecnológicos y de ingeniería que están siendo aplicadas, otras, asociadas a las interacciones humanas y las condiciones del trabajo.

Los accidentes del transbordador espacial Challenger en 1986 llevaron a entender que al establecer los factores causales no es suficiente con mirar sólo fallas en el ámbito técnico o humano, se requiere incluir los factores organizativos a la fórmula explicativa para comprender el sistema en sí mismo y no sus eventos aislado (OACI, 2012).

Como se ha venido mostrando, en sus inicios la gestión de la seguridad operacional estaba centrada en la noción de error humano; sin embargo, la evolución tecnológica de la década de los 80 representada en la energía nuclear y la seguridad vial, hizo necesario sobrepasar el

análisis del error y entrar al problema científico del riesgo, lo que conllevó significativos avances en materia de seguridad operacional (Amalberti, 2009).

Los esfuerzos científicos y técnicos de este nuevo enfoque condujeron a una mejora significativa de la seguridad en la mayor parte de las empresas de riesgo; sin embargo, se redujeron eficientemente los problemas técnicos, pero aparecieron los retos asociados al factor humano (Amalberti, 2009).

Desde la perspectiva ergonómica, los factores humanos se refieren a una serie de principios que se aplican a cualquier operación en la que interactúen las personas con el medio de trabajo y, un sistema de trabajo se entiende como un conjunto de elementos interrelacionados y circunscritos a un espacio y un entorno organizado (Blaya, Abad, García y Sampedro, 2012).

En casi todo sistema, el centro es el operador que recibe información del ambiente y responde utilizando los medios de trabajo brindados para realizar su tarea. Un enfoque de factores humanos involucra el análisis de tareas, capacidades personales, condiciones de trabajo, la evaluación de la carga de trabajo y el establecimiento de medidas correctivas, todo ello con el fin de provocar mejoras en la productividad de los procesos productivos (Blaya et al., 2012).

Ahora bien, retomando el tema de los factores humanos, este fracaso relativo en mejorar la seguridad se puede explicar, entre otras cosas, por el rápido desarrollo de nuevas tecnologías lo cual transformó la naturaleza del trabajo y aportó mayor complejidad a las organizaciones y a los riesgos de operación, realidad que generó en los expertos la necesidad de ampliar el foco de intervención a diversos niveles en las organizaciones (Amalberti, 2009).

Así, el abordaje científico de la seguridad hizo un giro paradigmático en el que se abandonó el énfasis inicial dado a la perspectiva individual que se centraba en el error humano como causa de accidentes, para acoger la perspectiva sistémica según la cual, por un lado, el error humano no es causa sino consecuencia de una serie de concurrencias dentro de la organización

(Reason, 2010) y, por otro, que las personas aportan de un modo efectivo a la seguridad por su capacidad de adaptarse a los cambios y anticipar situaciones que potencialmente podrían dar lugar a fallos originados incluso en vacíos en el diseño de los sistemas o en los procedimientos (Cook, Renders y Woods, 2000).

Seguidamente se expone más en detalle el contraste entre dos posturas específicas: una que se conoce como tradicional a la que subyace una epistemología causal lineal y otra, sistémica, con una epistemología circular propia de la cibernética y los sistemas sociotécnicos. Cada una de ellas establece diferencias conceptuales profundas que trazan y delimitan el camino de la acción en seguridad operacional.

3.1 Evolución de los Modelos de Análisis de Accidentes

El enfoque tradicional de la seguridad operacional toma forma en la década de los setenta, cuando se enfatiza el error, su origen y control, corolario que inicia investigaciones sobre los aspectos psicológicos y fisiológicos vinculados a procesos cognitivos del individuo (Amalberti, 2009).

Básicamente, este paradigma de la seguridad se centró en buscar maneras en las que la actuación humana, concebida en su momento como limitada y tendiente al error, no pudiera abatir un sistema pensado como seguro y bien diseñado. Esto implicaba que la seguridad o los niveles deseables de seguridad, una vez establecidos, podían mantenerse siempre y cuando la actuación humana permaneciera dentro de unos límites o parámetros establecidos, para lo cual se establecían mecanismos que defendieran al sistema de las consecuencias derivadas del error humano (Woods y Hollnagel, 2006).

Dentro de esta perspectiva se enmarcan los modelos de accidentes que han sido utilizados durante décadas para explicar la génesis de los eventos adversos. Uno de los primeros es el modelo secuencial que plantea que el accidente es el resultado de una secuencia de eventos que ocurre en una relación causa-efecto y en un orden concreto; habitualmente el agente

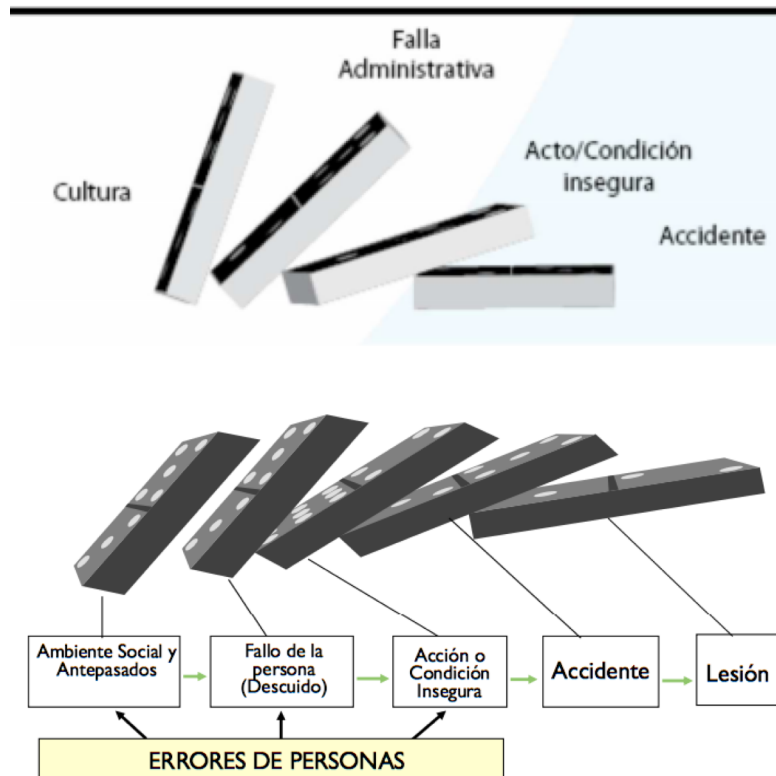
disparador es un acto arriesgado o equivocado del operador y/o la presencia de un riesgo físico o mecánico (Hollnagel, 2009).

En este modelo, un accidente es una perturbación causada a un sistema diseñado para funcionar de manera estable. El objetivo de la seguridad sería identificar esas relaciones causa-efecto desde el evento hasta sus causas últimas; por tanto, la seguridad del sistema puede incrementarse obstaculizando dicha secuencia lineal de eventos, bien sea retirando uno de los componentes de la secuencia o aumentando el espacio entre los componentes (Hollnagel, 2006).

Este tipo de modelos también incluyen varias secuencias de eventos y resultan atractivos porque generan reflexión sobre series causales y son fáciles de representar gráficamente; sin embargo, exige que las redes causales establecidas sean relativamente simples (Hollnagel, 2009).

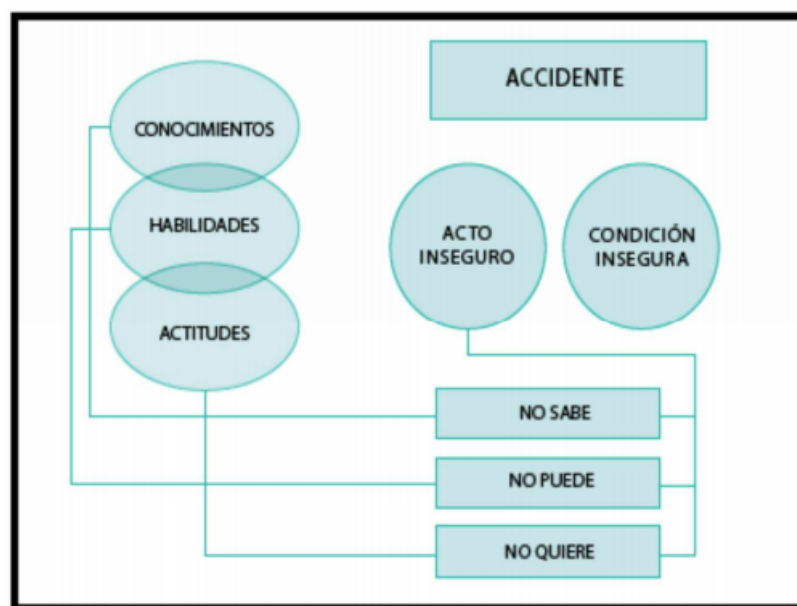
A este enfoque corresponde la teoría del dominó (figura 2) basada en la descripción de Heinrich (1980; como se cita en Hollnagel, 2009) y el modelo de evolución del accidente y barrera (Svenson, 1991, 2001; como cita Hollnagel, 2009).

Adicionalmente, Heinrich se pregunta las razones por las cuales las personas comenten actos inseguros y plantea tres respuestas posibles: por ahorrar tiempo, por ahorrar esfuerzo y por presión del grupo. A esto lo llama el factor actitudinal y lo presenta siguiendo la figura 3.



Fuente: Tomado de la Organización para la Aviación Civil Internacional, OACI.

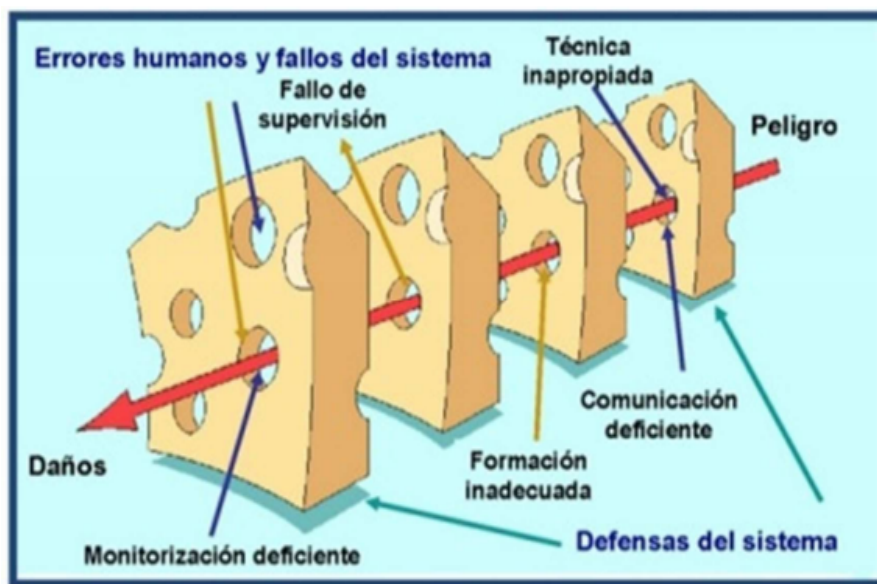
Figura 2. Teoría del dominó de Heinrich



Fuente: Tomado de la Organización para la Aviación Civil Internacional, OACI.

Figura 3. Modelo del factor actitudinal de Heinrich. En este modelo se aprecia que la capacitación y el entrenamiento afectan los conocimientos y la habilidad; es decir, la parte cognoscitiva y psicomotora. Sin embargo, las actitudes también juegan un papel crucial en la ocurrencia de accidentes.

La segunda categoría de modelo se conoce con el nombre de “modelo lineal complejo” o “modelo epidemiológico de accidentes”. Fue planteado inicialmente por Reason (1990, como se cita en Hollnagel, 2009) y conocido en el ámbito de la seguridad operacional como el modelo de “queso suizo” (figura 4). La idea central es que los accidentes pueden ser el resultado de una combinación de factores, unos explícitos otros latentes que coexisten en condiciones de tiempo y espacio.



Fuente Tomado de la Organización para la Aviación Civil Internacional, OACI.

Figura 4. Modelo de queso suizo. Las defensas, barreras y salvaguardas son claves en este modelo. Su filosofía se fundamenta en la creación y seguimiento de un sistema de defensa que tiene muchas capas o barreras, diseñadas para darse soporte mutuo con el fin de reducir la probabilidad de ocurrencia de un desastre.

Según Hollnagel (2009), este modelo se diferencia del secuencial en cuatro aspectos, a saber: no se habla de error humano sino de desviación en la actuación que puede hacer referencia a la tecnología o a la persona; toma en cuenta las condiciones ambientales que podían generar la desviación; aporta el concepto de barrera como mecanismos que podían incluso evitar un accidente; y, se plantea el concepto de condiciones latentes (patógeno residente) que son condiciones provenientes de procesos organizativos básicos y que están

presentes antes del inicio de la secuencia de accidente.

Amalberti (2009) sintetiza los paradigmas comunes de las construcciones científicas asociadas a los modelos secuenciales en lo siguiente: primero, los errores no son aceptables en las empresas porque perturban su funcionamiento, por tanto, es necesario reducirlos al máximo; segundo, como el error siempre estará presente, se deben desarrollar mecanismos de protección para una detección temprana, corregir e impedir sus consecuencias y; tercero, la causa real es la libertad del individuo en torno a los procedimientos y reglamentos, libertad que puede tolerarse dentro de un margen, pero que no justificará un descuido o la aceptación de riesgos en forma sistemática.

En esta misma línea, Woods y Hollnagel (2006) consideran que la seguridad operacional en el enfoque tradicional se centra, en primer lugar, en que es posible detallar completamente las condiciones de ejecución, por tanto, la seguridad se logra cuando la persona se ciñe al procedimiento/regulación/norma.

En segundo, un incidente de seguridad es resultado de un mal funcionamiento en algún componente, luego la gestión de la seguridad se basa en el análisis acerca de cómo pueden fallar los componentes, en la tabulación del error y en el cálculo de posibilidades de fallo para plantear acciones correctivas a partir de precisos informes y; por último, en este enfoque los responsables del objetivo de la seguridad realizan una gestión desarticulada de los objetivos estratégicos del sistema relacionados con la productividad y la eficiencia organizacional (Woods y Hollnagel, 2006).

Esta perspectiva tradicional, centrada en la necesidad de establecer las causas o causa raíz presenta importantes debilidades. Primero porque esta búsqueda lleva inmerso un carácter social y no sólo técnico, es decir, los investigadores contemplan qué causas serían aceptables para los propietarios del sistema. Segundo, es que esa búsqueda suele estar construida en torno a modelos de seguridad limitados o inexistentes que dejan de lado el rol que cumplen las

influencias culturales y organizacionales. Por último, habitualmente los modelos de seguridad se construyen al margen de otras actividades de gestión implicando la inexistencia de conexión integral entre seguridad y los procesos claves de la organización (Wreathall, 2006).

De otra parte, los métodos usuales de medición de la seguridad se basan en estadísticas y cálculos de probabilidades provenientes de análisis causa-raíz de eventos ocurridos, los cuales no dan cuenta de las influencias humanas y organizacionales, por lo que arrojan medidas estáticas del modo en que se originan los eventos y excluyen la complejidad y las interacciones al interior del sistema (Wreathall, 2006).

Una acción preventiva basada en el primer lugar de la pirámide de Bird (1969), a saber, las condiciones inseguras, no asegura que un evento mayor no vaya a suceder. Debe ocurrir una serie de hechos para que se produzca un accidente o pérdida, lo que plantea la necesidad de analizar factores principalmente relacionados con la responsabilidad que adquiere la administración a través del supervisor de los procesos o tareas y que se refiere a fallas en el control.

Otro aspecto importante tiene que ver con las medidas institucionales tomadas para mejorar la seguridad. Marais y Leveson (2003, como se cita en Sheridan, 2008) hacen un recuento de ellos: disciplinar a los trabajadores en respuesta a incidentes puede aislarlos; recompensar cuando informan la menor cantidad de incidentes es un incentivo para retener información valiosa para la seguridad; enfocarse en corregir lo inmediato puede dar una falsa sensación de seguridad y sofoca los esfuerzos por comprender las condiciones subyacentes que dieron lugar al evento; un enfoque excesivo a la prevención de la recurrencia del mismo tipo de eventos puede conducir a un examen insuficiente de otros problemas de seguridad latentes; las medidas de reducción de incidentes, tales como la redundancia, pueden mejorar inicialmente la seguridad, pero la ausencia de incidentes puede silenciar el sistema y reducir la conciencia situacional de los problemas de seguridad y, las bajas tasas de eventos pueden alentar el

sentimiento de autorregulación y caer en la trampa de la complacencia.

Un tercer enfoque de la seguridad es el llamado modelo sistémico que en lugar de descomponer estructuralmente el sistema en elementos o componentes y sus funciones, aborda los accidentes como fenómenos emergentes y, por tanto, eventos que pueden ocurrir.

3.2 Enfoque de la Seguridad desde los Sistemas Sociotécnicos Complejos

Partiendo de la complejidad en la tecnología y los riesgos asociados a su operación, las organizaciones requieren una articulación apropiada entre los subsistemas humano y técnico, lo cual representa un objetivo primordial en la seguridad por cuanto supone la posibilidad de que un evento ocurra no sólo en cada uno de ellos, sino también durante su interacción (Martínez, Gracia y Peiro, 2018).

Walker (2015) plantea que lo sociotécnico se refiere a la interrelación de los campos, el social y el técnico, pero la teoría sociotécnica se basa en dos principios. El primero es que esa interacción crea las condiciones para un desempeño (exitoso o no) del sistema. Los dos sistemas no se comportan de la misma manera, pero al trabajar juntos comienzan a generar interacciones de creciente complejidad e interdependencia y de allí el segundo principio: la optimización de las relaciones sociales o, más frecuentemente, las técnicas tienden a incrementar la cantidad de relaciones impredecibles o no diseñadas que son perjudiciales para el rendimiento del sistema.

Básicamente, la gestión de la seguridad en sistemas sociotécnicos complejos tiene dos tendencias: la primera, conocida como la teoría de accidentes normales propuesta por Perrow (1984, como se cita en Martínez et al. 2018) plantea la impredecibilidad de las interacciones y del resultado debido a la complejidad de la tecnología y la interdependencia entre tecnología y personas; la segunda, llamada teoría de las organizaciones de alta confiabilidad (HRO, High Reliability Organizations Theory) se fundamenta en la posibilidad de evitar los accidentes y llegar a ser entidades altamente confiables a partir de una adecuada gestión de la seguridad

(Martínez et al. 2018).

Desde el primer enfoque, los accidentes son resultado de fallas imprevistas en los componentes, pero no todas esas fallas se pueden anticipar debido a la complejidad interactiva y a la naturaleza estrechamente acoplada de los sistemas complejos, por tanto, es normal que ocurran accidentes (Stringfellow, 2010).

Desde el segundo enfoque, los accidentes pueden ser evitados si se tienen los siguientes elementos: personal experto, compromiso sólido con la seguridad, procesos técnicos estables y un compromiso organizacional con el aprendizaje; sin embargo, estas propiedades no pueden realmente garantizar la seguridad de un sistema y su efecto sobre la seguridad parece no contar con suficiente soporte científico (Stringfellow, 2010).

Algunos investigadores han abordado la seguridad desde un enfoque cultural, precisando dos atributos clave para que un sistema sociotécnico opere de manera segura: la cultura de la seguridad y la cultura justa. Una cultura de seguridad es producto de valores, actitudes, percepciones y patrones de comportamiento individuales y grupales que fijan el compromiso con una gestión en seguridad saludable. Cultura justa es un entorno que alienta y facilita la presentación de informes y el intercambio de información (Stringfellow, 2010).

Para Dekker (como se cita Stringfellow, 2010) una cultura de seguridad sana incluye el compromiso de la gerencia con la seguridad, la comprensión de la seguridad de operaciones y del riesgo, el empoderamiento de los operadores para influir en las políticas organizacionales, la conexión de las estructuras de incentivos con la seguridad y el aprendizaje de los informes de incidentes.

Cualquiera sea el punto de partida, es claro que tanto la seguridad como los accidentes se consideran propiedades emergentes de los sistemas. El sistema idealmente debe ser diseñado con criterios de seguridad desde el comienzo porque esta condición no puede ser adicionada una vez se ha completado el diseño del sistema. Para lograr esa integración, el diseño debe

contemplar las interacciones propias del sistema y no enfocarse solo en los procesos técnicos por cuanto estos, en sí mismos, no garantizan seguridad (Stringfellow, 2010).

No obstante, es un hecho que el elemento humano no puede ser diseñado, por lo tanto, el enfoque de diseño cuando se piensa en personas se refiere al diseño de sistemas de soporte humano tales como la modificación del contexto operacional, manejo de cargas de trabajo, gestionar las prioridades individuales a través de incentivos, gestionar la tolerancia al riesgo a través de una evaluación transparente y precisa de los riesgos y una toma de decisiones de apoyo (Stringfellow, 2010).

Walker (2015) cita algunos ejemplos exitosos en la aplicación de los principios de la teoría de sistemas sociotécnicos a organizaciones, entre ellos, destacar el papel de los equipos, promover la autonomía responsable, la adaptabilidad y las tareas significativas. La introducción de estos aspectos redundó en una mejora significativa y sostenida de la productividad.

En cuanto al control y la gestión de riesgos en sistemas sociotécnicos complejos, es un tema que plantea desafíos únicos de modelado y ejecución que van mucho más allá de los que se enfrentan en problemas de control regulatorio (Venkatasubramanian, et al. 2019).

Venkatasubramanian et al. (2019) consideran que para avanzar en el entendimiento de los accidentes, es necesario abandonar la tendencia de analizarlos como únicos e independientes para circunscribirlos en una perspectiva más amplia que contempla la fragilidad potencial del sistema, es decir, que la acumulación de efectos no lineales, la interconectividad y las interacciones entre las personas y su medio ambiente que pueden incrementar la fragilidad del sistema y hacerlo susceptible a fallas sistémicas.

Se entiende que un sistema sociotécnico complejo posee un gran número de componentes en interconexión con interacciones no lineales que pueden conducir a comportamientos emergentes, condición que puede dificultar la anticipación y el control; adicionalmente, estos

sistemas no están aislados, sino que interactúan con medio ambientes físicos, de mercadeo y regulatorios dando como resultado una compleja dinámica de retroalimentación (Venkatasubramanian et al., 2019).

Por esto, la ausencia de resultados no deseados (accidentes) no necesariamente significa que todo vaya bien. Si bien podría ser que cada cosa dentro del sistema está funcionando como debería y que la situación es normal con límites de desempeño de seguridad, es probable que el criterio de falla sea muy alto y/o la medida sea imprecisa o poco frecuente, caso en el cual se configura una condición latente en lugar de un resultado no deseado (Hollnagel, 2009).

Hay una diferencia importante entre una situación donde hay un resultado no deseado y otra donde el resultado no deseado no es detectado y esto también evidencia la existencia de una condición latente, en el sentido en que la define el modelo epidemiológico (Hollnagel, 2009).

Generalmente en el análisis de riesgo y la teoría de la decisión, se utiliza la tabla 2 para tener una categorización efectiva y abreviada de diferentes condiciones o situaciones y permite clarificar cuáles son las características de un accidente, disminuyendo el nivel de confusión (Hollnagel, 2009).

Tabla 2

Esquema para el análisis de riesgo y decisión

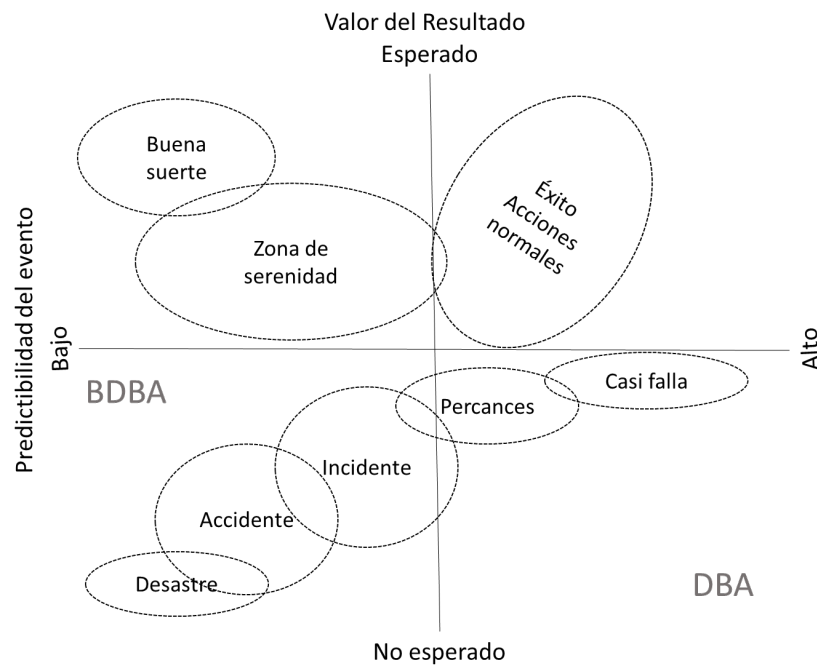
Evento	Resultado	Resultado no esperado	Resultado esperado o deseado
Evento no esperado e impredecible		Accidente	Golpe de suerte
Evento esperado y predecible		Mala suerte	Logro o cumplimiento de objetivo

Fuente: Tomado de Hollnagel, 2009.

Se aprecia que, aunque hay dos tipos de situaciones donde se dan resultados no esperados,

solo una de ellas podría llamarse accidente. Los accidentes siempre refieren a resultados no deseados y son siempre inesperados; sin embargo, esto no quiere decir que son inimaginables, por el contrario, es posible anticiparlos (Hollnagel 2009).

Hollnagel (2009), establece la posible relación entre diferentes categorías de resultados, como se ilustra en la figura 5.



Fuente: Tomado de Hollnagel, 2009.

Figura 5. Categorización de resultados operacionales.

El eje de la abscisa (X) describe la predictibilidad del evento, desde la más baja a la más alta. El eje de la ordenada (Y) describe la deseabilidad de los resultados desde lo no esperado hasta lo esperado.

El cuadrante superior derecho corresponde a la operación normal, es decir, eventos altamente predecibles con resultados esperados. El cuadrante inferior derecho corresponde a los eventos predecibles con resultados no esperados, serían los accidentes de diseño (DBA: design-base accident). El cuadrante inferior izquierdo involucra los eventos no predecibles con resultados no esperados y corresponde a lo que se llama “más allá del diseño” (BDDBA:

Beyond Design-Base Accidents) y, finalmente, el cuadrante superior izquierdo corresponde a los eventos no predecibles con resultados esperados o cuadrante de la serenidad o la buena suerte (Hollnagel, 2009).

La realidad parece ser que cuando ha ocurrido un evento inaceptable para el sistema, es frecuente que los actores, tanto operadores como gerencia, sean incapaces de 1) reconocer qué diseño, proceso o procedimiento condujo a una operación de alto riesgo; 2) entender el factor causal y las presiones que reforzaron el alto riesgo de operación y 3) encontrar soluciones al diseño que permitan o refuercen la seguridad de la operación (Stringfellow, 2010).

Otro gran desafío para la operación segura de sistemas sociotécnicos complejos es la migración del riesgo producto del dinamismo propio de los sistemas que los conduce a operar en los límites de lo que se considera seguro; esto quiere decir que la seguridad no es una propiedad estática, requiere de trabajo constante, pues los objetivos de eficiencia de la organización priman sobre los objetivos de seguridad (Dijkstra, 2006; Stringfellow, 2010).

Los expertos identifican también comportamientos problemáticos típicos en los sistemas sociotécnicos complejos. Uno de ellos es la tendencia del nivel gerencia de la seguridad y/o la organización a intervenir sobre los síntomas y no sobre los problemas de seguridad, actitud que es frecuente cuando la causa del problema no es obvia (Stringfellow, 2010).

Un sistema complejo es siempre un sistema variable, tanto en el sentido de su entorno inmediato como en su variabilidad endógena o de subsistemas constitutivos. Esta última es atribuible en alto porcentaje a las personas, pero no por ello se puede decir que los individuos son responsables sino, por el contrario, que esta variabilidad en la actuación es necesaria para hacer frente a las exigencias reales de la operación.

Desde la perspectiva sistémica, tanto los fallos como los éxitos se consideran fenómenos emergentes y de ninguna manera, los fallos pueden ser explicados por mal funcionamiento de partes específicas. Es probable que el resultado pueda diferir de lo que se esperaba, pero

esto se debe más a la variabilidad contextual que a fallos en la actuación (Hollnagel, 2006).

En este sentido, la actuación normal difiere de la actuación normativa: la primera representa el equilibrio que refleja la normalidad del ambiente operativo incluso cuando se han requerido ajustes por demandas cambiantes del entorno y la segunda, está constituida en el ajuste del comportamiento a las regulaciones (Hollnagel, 2006).

Pensar la seguridad desde un enfoque sistémico, significa que se es capaz de dar cuenta de las combinaciones o conjunto inesperado de sucesos que dan lugar a un evento no deseado y a esto se llama concurrencia; es decir, poder dilucidar que dos o más cosas pasaron al mismo tiempo y se influyeron mutuamente como parte del proceso comprensivo del evento no deseado (Hollnagel, 2006).

Una conclusión importante de la aplicación de modelos sistémicos en el análisis de los eventos, además de la profundidad de lo ya mencionado, es que esta manera de abordar los eventos aboga por buscar dependencias poco comunes y condiciones comunes asociadas a los accidentes. Esta actitud significa que el mejor camino para entender la variabilidad del sistema lo antes posible es controlar la actuación del sistema (Hollnagel, 2009).

Hasta aquí se han descrito los aspectos más relevantes de la gestión de la seguridad desde el enfoque de sistemas sociotécnicos. A continuación, se muestran los aspectos más relevantes del manual de gestión de seguridad operacional de la organización que sirve de contexto para este estudio, con el fin de dar cuenta de su enfoque y direccionamiento.

3.3 Seguridad Operacional en la Institución de Aviación Militar

La institución de aviación militar ha realizado un esfuerzo permanente por gestionar la seguridad operacional y adaptarse a los retos que plantea el contexto normal de operación, la realidad política nacional y las restricciones presupuestales que afectan la operación.

Pese a este escenario, la organización posee un sistema de gestión operacional documentado en un manual cuya última versión está próxima a ser legalizada. Allí se plantea

que el objetivo fundamental de la gestión en seguridad es mantener la capacidad operacional, para lo cual define fundamentos básicos, organización y elementos generales del sistema.

Para la organización, la seguridad operacional es un principio institucional de responsabilidad compartida que debe estar presente en todas las actividades y procesos. Su objetivo es mantener un proceso continuo de identificación de peligros a través de estrategias reactivas, proactivas y predictivas que permitan eliminar los riesgos de seguridad asociados a sus actividades. El fin es evitar sucesos no deseados de seguridad que impacten el normal desarrollo de su operación.

En su estructura, existe una Dirección como responsable de orientar los procesos de la organización para reducir, mitigar y controlar los riesgos, evitar la pérdida de recursos, preservar la capacidad operativa y prevenir el deterioro de la imagen de la organización. Sus acciones están enmarcadas en el ciclo planear, hacer, verificar y actuar.

El sistema plantea un esquema y procedimiento para identificación de peligros y gestión de riesgos a partir de la obtención de información válida, oportuna y precisa, cuyo fin es identificar peligros y aplicar medidas correctivas para mantener el nivel aceptable de seguridad con el fin de supervisar, evaluar y mejorar el desempeño en seguridad a través de estrategias reactivas, proactivas y predictivas.

Una vez identificados los peligros, se define la estrategia correspondiente de gestión: reducir, compartir, evitar, transferir o aceptar a partir de la evaluación de los criterios típicamente utilizados de probabilidad y severidad que definen el nivel de tolerancia del riesgo.

Adicionalmente, el sistema propone una garantía de seguridad (figura 6) cuya función es asegurar que los controles que han sido implementados mantengan los objetivos previstos. La gestión de riesgos habla de lo que ocurre en la operación del sistema y la garantía de calidad busca mantener los resultados. Un procedimiento de medición de rendimiento del sistema

sostiene su eficacia y mejoramiento.

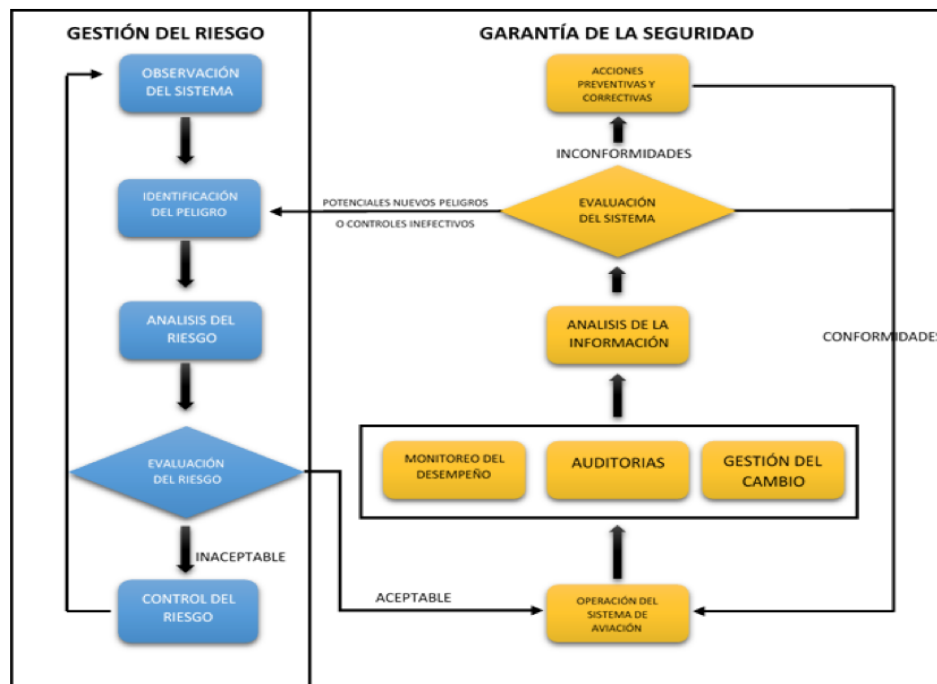


Figura 6. Relación gestión de riesgos y garantía de la seguridad. Esta interacción otorga continuidad al desempeño del sistema de seguridad. Manual de Gestión de Seguridad Operacional. Documento oficial en aprobación.

En términos generales, en este documento se resume la intención de la organización respecto de su sistema de gestión de la seguridad operacional. Sin embargo, es preciso tener en cuenta que la institución opera en condiciones *sui generis* de orden público y eso incrementa los riesgos a los que se enfrenta. Por ello, las estadísticas de eventos de seguridad son de importancia vital para la organización.

Como antecedente relevante para la investigación, se realizó el análisis descriptivo de 1.068 eventos de seguridad (Eveso) ocurridos entre los años 2015 y 2017 (Anexo B). Si bien desde la perspectiva de la ingeniería de la resiliencia, los eventos de seguridad operacional se comprenden superando la lectura de causalidades lineales y dirigiéndose específicamente a los procesos de la organización (Dallat, Salmón y Goode, 2017), esta aproximación descriptiva permite tener una primera perspectiva de los principales retos que enfrenta la

organización.

Los eventos así agrupan la clasificación definida en el manual de seguridad operacional de la organización donde se unifica la tipología (tabla 3) NOPER, INFO, EVOT, RECIL, RELES y accidente.

Tabla 3

Tipología de los eventos de seguridad operacional en la entidad

Tipología	
EVESO	Evento de seguridad operacional.
EVOT	Evento operacional en tierra
INFO	Evento en el que exista una de las siguientes condiciones: teniendo intención de vuelo no existan daños a la aeronave o lesiones a personas, afectación a la seguridad de interés para la prevención de accidentes o cuando se apliquen procedimientos anormales por un suceso en la aeronave.
NOPER	Novedad operacional.
RECIL	Suceso con intención de vuelo. Recuperable, ilesos.
RELES	Suceso con intención de vuelo. Recuperable, lesionados.
Accidente	Suceso operacional con o sin intención de vuelo en el que exista al menos una de las siguientes condiciones: la aeronave no es recuperable, existen lesiones fatales o algún tipo de incapacidad permanente, evento con fatalidades dentro de los noventa días calendario a su ocurrencia o aeronaves desaparecidas por más de noventa días.

Fuente: Manual de seguridad operacional institucional.

Durante el periodo de tiempo indicado, la organización asociaba las causas de eventos a tres factores: humano, operacional y técnico dentro del modelo HFACS (Human Factors Analysis and Classification System) planteado por Doug Weigman y Scott Shappel (2004) que parte del modelo de queso suizo (Reason, 2010) y provee una herramienta para asistir los procesos de investigación de accidentes y dirigir los esfuerzos en entrenamiento y prevención.

El HFACS tiene una estructura básica de cuatro niveles de falla: actos inseguros del operador, precondiciones para actos inseguros, supervisión insegura e influencia

organizacional. El modelo identifica categorías causales dentro de cada nivel a modo de fallas latentes o activas. En teoría, al menos una falla podría ocurrir en cada nivel en un evento adverso, de modo que, si se corrigen las fallas, se puede evitar el evento.

Particularmente en cuanto al análisis descriptivo de la data institucional se evidencia un comportamiento relativamente estable de los EVOT en los tres factores: operacional, técnico y humano. Sin embargo, los informes y reportes de novedades operacionales en el factor técnico presentan un incremento significativo entre los años 2016 y 2017. El número de reportes INFO y NOPER muestra una tendencia a disminuir en el factor operacional y, el factor humano, tiene un incremento significativo en los reportes NOPER.

No fue posible determinar si estos movimientos estadísticos responden a alguna variable interna, a coyunturas organizacionales o a cambios en las políticas de seguridad relacionadas con la rendición de informes de seguridad.

Los subtipos más significativos asociados al factor técnico estuvieron representados en fallas de los sistemas eléctrico y motores causados por: 1) humedad que ocasiona falla en las conexiones eléctricas para el primer caso y 2) desgaste normal de los componentes.

Los subtipos más significativos asociados al factor operacional fueron: 1) entorno operacional, BASH (bird aircraft strike hazard, 2) FOD (foreign object damage) y 3) factores ambientales asociados a condiciones meteorológicas de viento y humedad e inadecuado seguimiento de procedimientos de despacho (falta de procedimientos y normas).

Ahora bien, los subtipos más significativos para el factor humano fueron: Para acto inseguro de la tripulación relacionados con la toma de decisiones, 1) elección equivocada de un curso de acción durante la operación y 2) errores en la ejecución de procedimientos estandarizados.

Para acto inseguro de la tripulación relacionados con la habilidad, 1) sobrecontrol de la aeronave y 2) deficiente técnica de vuelo. Para acto inseguro de la tripulación relacionados

con percepción, 1) falta de atención y 2) percepción errada sobre la condición de la aeronave.

En factor humano para el subtipo precondiciones para actos inseguros en condiciones subestándar de operación, estado mental inadecuado, los aspectos más influyentes fueron complacencia y prisa. En prácticas subestándar de operación, CRM (crew resources management), el aspecto relevante fue la falla en el liderazgo y trabajo en equipo.

En factor humano para el subtipo supervisión insegura, se observó inadecuada supervisión relacionada con: 1) los trabajos de mantenimiento, 2) del piloto al mando sobre tareas rutinarias en vuelo y 3) la transmisión de prácticas inadecuadas de mantenimiento a través del modelamiento de errores.

En factor humano para el subtipo influencia organizacional, se encontró mayor frecuencia en proceso organizacional relacionado con la presión de la organización para el cumplimiento de la misión.

En cuanto a la fase de vuelo, se corrobora la literatura general de aviación que establece que el aterrizaje y el despegue son las fases más riesgosas del vuelo. Sin embargo, un alto índice de eventos de seguridad se observa también en la fase crucero, dato que merece la atención del sistema.

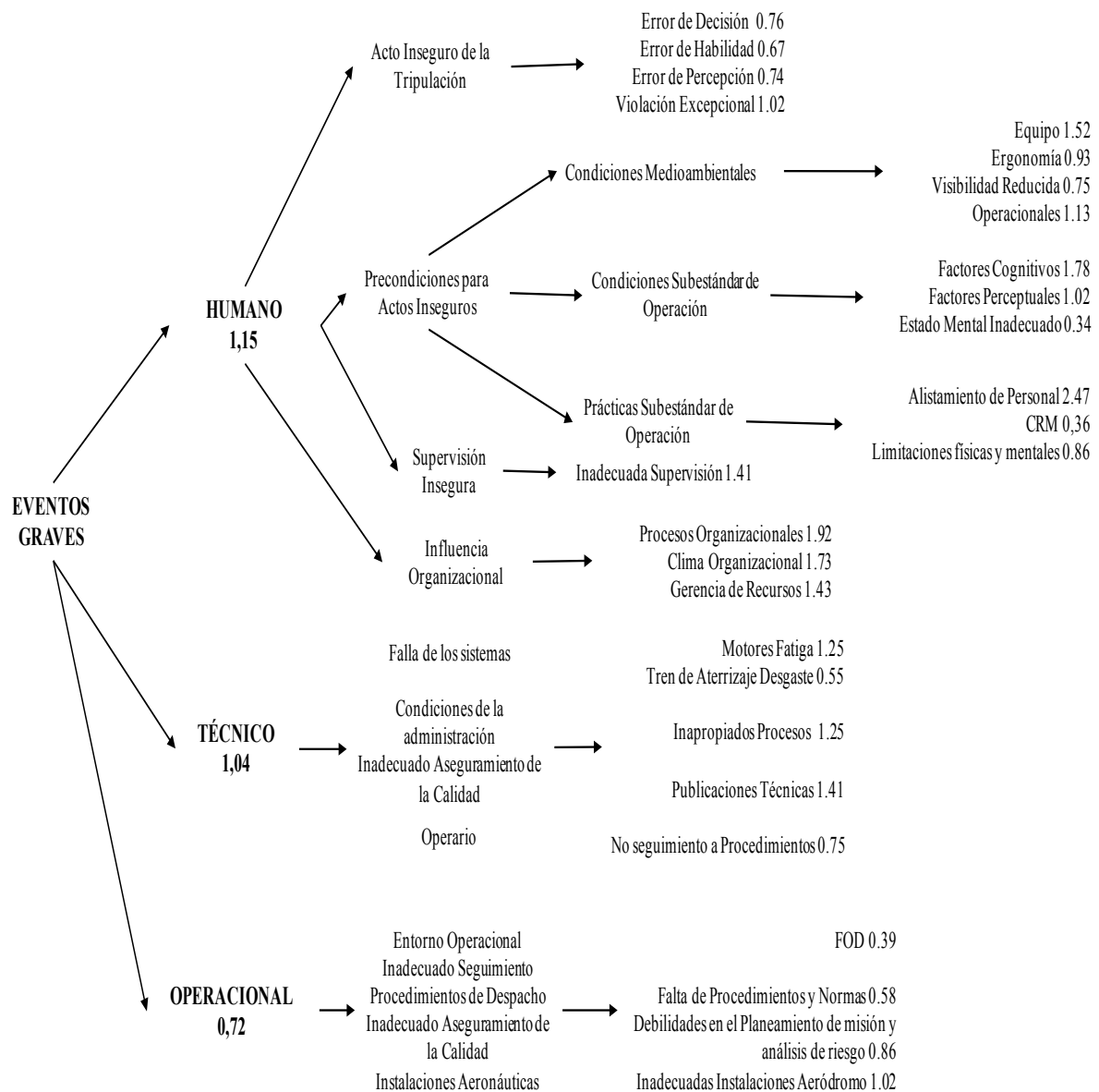
En este caso, el factor humano participa con mayor relevancia en la fase de aterrizaje. El factor técnico y humano son casi igualmente importantes en la fase de despegue; pero la fase de crucero está significativamente asociada al factor técnico.

Al considerar la misión, los datos significativos se aprecian en mayor participación del factor humano en misiones de instrucción y entrenamiento y transporte de personal y carga representados en las categorías 1) actos inseguros de la tripulación relacionados con errores de decisión, habilidad y percepción; 2) precondiciones para actos inseguros, condiciones subestándar de operación, estado mental inadecuado y 3) influencia organizacional, procesos organizacionales.

De otra parte, con la información entregada se realizó un estudio de las relaciones de riesgo de la incidentalidad en función de los factores situacionales y estructurales valorados y para el efecto se utilizó el estadístico de riesgo relativo (RR).

El análisis de RR tiene como objeto estimar la probabilidad de ocurrencia de un desenlace (evento de seguridad) dada una condición de riesgo. Para su interpretación el RR de 1,0 indica que no hay asociación entre la presencia de un factor y el evento. Si es $RR > 1,0$ quiere decir que la asociación es de riesgo y la presencia del factor está asociado con la ocurrencia del evento, es decir, que el factor sería un factor de riesgo para la ocurrencia del evento. Si $RR < 1,0$ entonces, la asociación es de protección y por ende la presencia del factor estaría asociada con la no ocurrencia de evento.

Para ello, se consideraron los accidentes y eventos de clasificación RECIL y RELES en función de los factores de exposición situacional y estructural dadas las tres categorías de análisis: factores técnicos, operacionales y humanos de la seguridad operacional, lo que permitió derivar el árbol de decisión relacional (figura 7).



Fuente: Elaboración propia de la autora.

Figura 7. Árbol relacional de los factores de riesgo y los eventos de seguridad operacional.

Se puede apreciar que el riesgo relativo es significativo para factor humano y técnico. El factor humano que se asocia con mayor probabilidad a la ocurrencia de un evento grave tiene relación con acto inseguro de la tripulación, violaciones excepcionales (omisión intencional de procedimientos estandarizados y acción humana equivocada y deliberada no corregida).

Desde la perspectiva individual este dato es interesante dado que los errores de habilidad,

decisión y percepción pueden ser intervenidos a través del entrenamiento, pero las violaciones aluden a aspectos vinculados a características más estables del individuo.

En precondiciones para actos inseguros, el mayor riesgo está en las condiciones medioambientales relacionadas con el equipo y la operación (diseño de los equipos y condiciones de meteorología que afectan el desempeño); condiciones subestándar de operación, tanto factores perceptuales (atención canalizada e inadecuada delegación de tareas) como factores cognitivos (atención canalizada, pérdida de conciencia situacional e insuficiente conocimiento de la aeronave) y; prácticas subestándar de operación, alistamiento de personal (inadecuada preparación del individuo para la ejecución de la tarea y complacencia).

En supervisión insegura, inadecuada supervisión, los valores de RR mayores a 1 fueron para supervisión de tareas y/o para la vigilancia y control operacional, y/o sobre las técnicas de instrucción en las escuelas. En influencia organizacional, el RR significativo estuvo relacionado con clima organizacional (alta carga laboral), procesos organizacionales (alta demanda de la instrucción y decisiones de personal que afectan los trabajos de mantenimiento) y gerencia de recursos (omisión de acciones organizacionales para mitigar riesgos en aeródromos no controlados y asignar personal no calificado para la ejecución de tareas).

En el factor técnico, por su parte, el RR se encuentra en falla de los motores por fatiga (falla en componente interno del motor); condiciones de la administración, inapropiados procesos (inadecuado proceso de certificación de los trabajos de mantenimiento) e inadecuado aseguramiento de la calidad, publicaciones técnicas (incumplimiento a lo establecido en procedimientos estandarizados).

Si bien el factor operacional, en general, no muestra un nivel riesgo relativo, se observa que el subtipo “inadecuada instalaciones del aeródromo” aparece con un riesgo relativo superior a 1,0 positivo en los eventos graves.

La importancia de este análisis de riesgo relativo radica en que lleva la mirada del sistema

a aspectos no observados como relevantes en el análisis descriptivo debido a que se está evaluando el grado de asociación entre los factores/subtipos y la ocurrencia de eventos graves en seguridad operacional.

Sin embargo, esta información evidencia que, hasta el momento, los datos institucionales recogidos por el sistema de gestión de la organización arrojan información centrada en el error, a cualquier nivel. Esto es esperado teniendo en cuenta que el modelo que se utiliza para clasificar la información de investigación de accidentes aéreos está basado en un enfoque tradicional de la seguridad operacional que difícilmente avanza a dar cuenta de procesos o concurrencias funcionales sistémicas involucradas en la ocurrencia de eventos.

El siguiente capítulo abre la discusión sobre las principales implicaciones de dar una mirada a la seguridad desde la perspectiva de los sistemas y, más específicamente, desde la ingeniería de la resiliencia.

Capítulo

4. Ingeniería de la Resiliencia

El objetivo de este capítulo es presentar los principios de la resiliencia organizativa que constituye el fundamento epistemológico de este trabajo de investigación, a partir de ejes temáticos que brinden una visión general del concepto.

En su sentido más amplio, la resiliencia es un proceso que ayuda a los sistemas para que tengan la capacidad de combatir con la desorganización, la pérdida y el daño de manera que puedan mantenerse y resistir a pesar de los obstáculos que surgen del entorno o de su propio funcionamiento (Said, Bouloiz, y Gallab, 2019).

Los desarrollos teóricos en sistemas sociotécnicos complejos dieron origen a esta disciplina cuyo objetivo, más que superar riesgos como se plantea en los métodos de gestión de la seguridad, es crear procesos robustos, pero flexibles que hagan frente a las interrupciones del funcionamiento normal y a las presiones propias de la operación a través del uso proactivo de sus recursos (Said, et al., 2019).

4.1 Aproximación Conceptual

El término resiliencia proviene de la física de los materiales y se refiere a su capacidad para absorber energía elástica cuando es deformado (antes de entrar en un régimen de fluencia o deformación irrecuperable) y cederla cuando cesa el esfuerzo de deformación. Su cuantificación implica una relación entre tensión-deformación por unidad de volumen y determina la resistencia o fragilidad del material; en términos simples, es la capacidad de memoria de un material para recuperarse de una deformación producida por un esfuerzo externo (Moreno, 2006).

Las ciencias humanas y sociales parten de este concepto y lo definen como la capacidad que tiene el ser humano, una organización o una comunidad para enfrentar situaciones adversas y resultar enriquecidos; se considera un estado producto de una interacción dinámica

entre factores protectores y factores de riesgo que puede ser desarrollados y promovidos (Fiorentino, 2008).

Este término fue aplicado a sistemas sociotécnicos complejos, entre otros teóricos, por Hollnagel (2006) quien la conceptualizó como la habilidad intrínseca de un sistema para ajustar su funcionamiento antes de, durante o después de cambios o perturbaciones con el fin de soportar las operaciones inclusive después de un contratiempo significativo o en presencia de presión continua.

Para McDonald (2006) “la resiliencia representa la capacidad (de un sistema organizativo) de anticipar y gestionar el riesgo de modo efectivo, mediante una adaptación apropiada de sus acciones, sistemas y procesos para garantizar que sus funciones esenciales sean llevadas a cabo en una relación estable y efectiva con el entorno” (p. 69).

La resiliencia se requiere, entonces, cuando los sistemas son desafiados a operar en condiciones no contempladas durante su diseño o en aquellas circunstancias que superan lo previsto originalmente en el diseño (Herrera, 2016), de manera que está presente antes y después de un evento inesperado (Hale y Heijer, 2006).

Esto quiere decir que la resiliencia apunta a una cualidad del sistema; es decir, es algo que el sistema hace y no algo que el sistema tiene, por tanto, es más pertinente hablar de potencial de resiliencia (Woods, 2015) o potencial de desempeño resiliente (Hollnagel, 2014).

Hale y Heijer (2006) plantean que la resiliencia es una habilidad que le permite a la organización operar muy cerca de la zona de riesgo de accidente, pero siempre fuera de ella, lo que significa que un sistema es resiliente cuando tiene conocimiento cierto de esa zona de peligro y esto implica hacer una evaluación compleja de las respuestas adaptativas a los diferentes tipos de alteraciones que le permite responder consistente y eficazmente cuando se detectan señales de peligro real, incluso si la situación es inesperada.

Para Hollnagel (2006), el enfoque de la seguridad basado en la ingeniería de la resiliencia

tiene unas premisas básicas: en primer lugar, es habitual que los procedimientos operativos estén especificados de manera exigua, de modo que los individuos deben adaptar lo que hacen durante la operación a lo requerido por la organización y a los recursos asignados. Son las personas quienes enfrentan los posibles vacíos procedimentales, de diseño y/o contingencias derivadas del ambiente operacional.

En realidad, las personas que ejecutan el trabajo técnico establecen estrategias para adelantarse a las diferentes situaciones que pueden conducir al fallo, de manera que aprenden y se adaptan para generar seguridad, pese a la presencia de riesgos explícitos y tácitos en el ambiente organizativo particular (Woods y Cooks, 2002; como se cita en Woods y Hollnagel, 2006).

Para De Keyser (1990), el hombre es un regulador por excelencia pues es quien analiza y decide en la incertidumbre, hace frente a situaciones inesperadas y llena los vacíos de múltiples carencias procedimentales. Sus posibilidades de diagnóstico exceden las de los sistemas más eficaces incluso con capacidades disminuidas por estrés o fatiga.

En segundo, algunos sucesos adversos quizá se puedan atribuir a fallos directos, pero la realidad es que la mayoría derivan de combinaciones inesperadas propias de la variabilidad de la ejecución. Muchas veces, el trabajo del individuo no se limita a ejecutar una acción frente a una situación determinada, sino que las situaciones devienen con la interacción de múltiples factores imprevistos.

En tercer lugar, la gestión de la seguridad operacional no puede basarse exclusivamente en la recolección de datos provenientes de incidentes ocurridos (reactiva) o en el cálculo de la probabilidad del error, sino que debe ser principalmente proactiva; es decir, desarrollar la capacidad de anticipar la posible ocurrencia de eventos para tomar las acciones preventivas planteadas para prevenir el evento o el resultado (Hollnagel, 2009).

Por último, la seguridad está íntimamente vinculada a la productividad de la organización.

Las empresas buscan ser productivas, pero también seguras, luego estos dos objetivos organizacionales se afectan mutuamente; por tanto, las mejoras o reingenierías en cualquiera de ellos deben estar en equilibrio con el otro, pues se consideran interdependientes.

Para Woods y Hollnagel (2006), la resiliencia tiene relación tanto con la habilidad del sistema para reconocer y dominar esas perturbaciones imprevistas que ponen en tela de juicio la competencia del sistema como con la capacidad de hacer cambios o reajustes en sus procesos. En ese sentido, gestionar la resiliencia significa entender cómo se adapta el sistema y a qué tipo de perturbaciones debe adaptarse para lo cual exhibe las siguientes propiedades:

Su capacidad de amortiguación, es decir, la cantidad de perturbaciones que el sistema puede enfrentar sin sufrir disfunciones estructurales; su flexibilidad o habilidad para reestructurarse frente a los cambios externos y las presiones; su margen o nivel de precariedad con que está funcionando en el momento; y, su tolerancia o capacidad para operar bajo estrés o presión sin degradar su funcionamiento (Woods y Hollnagel, 2006).

La resiliencia, entonces, tiene relación con estándares tales como el establecimiento de rutinas de funcionamiento, la eliminación de divergencias derivadas de las destrezas individuales, la supervisión del cumplimiento de estándares (McDonald, 2006).

Algunas de las características organizativas que muestran alta flexibilidad y adaptación son: la presencia de sistemas de decisión descentralizados y con autonomía local, prácticas de trabajo informales, tecnologías que no limitan la actuación humana apropiada y los modos de control y, por último, sistemas organizativos que pueden gestionar la retroalimentación, el aprendizaje y la mejora (McDonald, 2006).

Esta descripción general de características de un sistema resiliente lleva a preguntarse sobre cómo pueden entenderse los éxitos y fallos en un sistema resiliente.

4.2 Fallos y Éxitos

El enfoque de la resiliencia no señala causas de eventos adversos sino concurrencias

funcionales, las cuales son consideradas normales e inevitables y están presentes tanto en los éxitos como en los fracasos del sistema. El éxito (no accidente) muestra la habilidad del sistema para anticiparse a las formas variables en que se presenta el riesgo antes de que se produzcan los fallos; el fracaso (perturbación del sistema o fallo) es la ausencia temporal o permanente de esa habilidad (Hollnagel, 2006).

Los fallos y éxitos, entonces, se consideran caras de una misma moneda, lo que significa que los dos tipos de resultado se originan en la variabilidad de la actuación individual y en el ámbito del sistema. La diferencia estaría circunscrita al grado de eficacia de los mecanismos de control del sistema, de modo que no necesariamente el éxito refiere a la eficiencia organizacional, sino también a la combinación de una serie de condiciones (Woods y Hollnagel, 2006).

De esta manera, el fallo representa realmente una incapacidad temporal para enfrentar de manera eficaz la complejidad del sistema y/o un fracaso en la capacidad del individuo para anticiparse al fallo; de este modo el operador, lejos de ser el responsable de los eventos inesperados, realmente contribuye de modo positivo a la seguridad porque enfrenta continuamente y con éxito las situaciones imprevistas que surgen en el sistema (Hollnagel, 1983; como se cita en Woods y Hollnagel, 2006).

Se consideran los fallos, entonces, como fracasos de adaptación y, por tanto, la ingeniería de la resiliencia contribuye en la reestructuración del modelo de seguridad de una organización a partir del rediseño de métodos, herramientas e indicadores de factores que favorecen la resiliencia y los mecanismos de adaptación del sistema: amortiguación, margen, flexibilidad y tolerancia del sistema (Woods y Hollnagel, 2006).

Ahora bien, cualquier perturbación o fallo va a movilizar el sistema hacia la ejecución de una serie de reajustes que pueden tener derivaciones más allá de lo inmediato. Para que los reajustes no se salgan de control y detectar a tiempo una posible perturbación en el

funcionamiento, un sistema complejo requiere una tendencia a la estabilidad (Hollnagel, 2006).

En este sentido, debe admitir el cambio y la mejora a través del diseño de procesos que reaccionen lo más rápido posible a los desafíos del entorno, capacidad que es una propiedad emergente determinada por la capacidad del subsistema humano para anticipar, reconocer, adaptar y aprender de variaciones, cambios, disturbios, interrupciones y desastres que pueden causar consecuencias no deseadas al sistema (Said et al., 2019).

Este grado de adecuación a la estabilidad o al cambio frente a las demandas del entorno en el que maniobra el sistema (McDonald, 2006) es una condición que le permite operar de manera efectiva en contextos de complejidad en expansión y en medio de la incertidumbre propia del entorno (Said et al., 2019).

El grado de incertidumbre está definido por la capacidad del sistema para identificar y gestionar adecuadamente los riesgos propios de su operación capacidad que es el tema del siguiente apartado.

4.3 Gestión de Riesgos y Amenazas

Para Dekker (2006), un aporte fundamental de la ingeniería de la resiliencia es contribuir al mejoramiento de las capacidades adaptativas de la organización para responder efectivamente a las demandas de un entorno cambiante y a amenazas emergentes, de modo que puedan identificar modelos de riesgo obsoletos, evitar el exceso de confianza en la efectividad continuada de estrategias y gestionar mejor los procesos mediante los cuales deciden cómo controlar el riesgo.

En un sistema resiliente, la función de control responde adecuadamente para evitar que el riesgo aumente hasta niveles fuera de los límites de seguridad (Zipkin, Gershenfeld, Carrol, & Barret, 2006). La resiliencia requiere la capacidad de anticipar y gestionar los riesgos antes de que se conviertan en amenazas para su funcionamiento (McDonald, 2006).

El desafío del sistema para reaccionar ante situaciones potencialmente perturbadoras depende en mucho del tipo de amenaza. Si es frecuente, el sistema desarrolla una respuesta estándar para enfrentarla. Si es irregular, significa que surge excepcionalmente, luego es poco probable que el sistema cuente con una respuesta y sus consecuencias pueden ser sean catastróficas. La última situación es aquella que aparece de modo inesperado, requiriendo un alto grado de improvisación (Westrum, 2006).

Esto coloca sobre el tapete el papel primordial de la gestión de riesgos para el desarrollo del potencial de desempeño resiliente de una organización. Lo que se ha encontrado en cuanto a este tema es que la evaluación de riesgos en organizaciones de alto riesgo generalmente no sobrepasa la primera línea de operación, ni apoya la identificación de riesgos emergentes; es decir, la mayoría de los métodos de evaluación de riesgos adoptan una filosofía causal lineal (Dallat, et al. 2017).

Desde este paradigma se deja de lado la importancia de tener en cuenta que la certeza de que un riesgo está erradicado traerá comportamientos que introducirán una amenaza; el trabajo del responsable de la seguridad es mantener el riesgo vigente aun cuando parece que la operación está funcionando de manera segura: “el núcleo de una buena cultura de seguridad es una profecía autodestructiva, y el logro de quien da la voz de alarma es estar equivocado” (Pariés, 2006, p.28).

Básicamente, se plantea desde esta perspectiva dos tipos de previsión: de un lado la que se origina en procesos de aprendizaje pertinente derivado de las lecciones provenientes de la experiencia y de otro, la relacionada con lo que Westrum (2006) llama el procesamiento de señales débiles, que incluye la detección de situaciones sospechosas a juicio del operador e incluso, implica la identificación y eliminación de patógenos latentes que es posible en culturas que gestionan la capacidad para detectar, agrupar e integrar información.

Este rasgo cultural promueve la detección de sucesos ocultos y fomenta una respuesta

proactiva ante peligros que aún no se han cristalizado. Para Westrum (2006), las culturas que desarrollan un pensamiento grupal tienen dificultades para admitir señales de anomalías reales o potenciales al interior del sistema. Una organización resiliente debe fomentar el pensamiento crítico que supone el desarrollo de la capacidad de anticipación y de captura de las señales débiles.

Otro rasgo cultural que integra una organización resiliente es lo que Westrum (2006) llamó una cultura de indagación consciente y la describe como aquella en la que todas las personas a diversos niveles de la organización reconocen la posibilidad de una situación peligrosa.

Estos aspectos teóricos muestran que la capacidad de un sistema sociotécnico para gestionar sus riesgos está íntimamente relacionada con su cultura.

4.4 Responsabilidades de la Alta Dirección en el Enfoque de la Resiliencia

La resiliencia directiva puede definirse como la habilidad del alto nivel directivo para hacer frente a conflictos entre la seguridad y los objetivos de actuación de la organización.

Desde el nivel estratégico de la organización, Sheridan (2008) realiza un resumen de las principales responsabilidades de gestión necesarias para mantener un sistema resiliente:

- Hacer énfasis en anticipar posibles incidentes futuros y en las acciones que mitigaron y/o contribuyeron a la recuperación de incidentes pasados.
- Medir continuamente las variables del sistema para operar en los límites de seguridad.
- Acercar las políticas y procedimientos formales a las realidades de operación.
- Alentar el control en personas no por su estatus en la organización sino por su participación en los procesos.
- Considerar la carga de trabajo mental organizacional como predictor de falla para anticipar una disminución en el rendimiento.
- Flexibilizar el sistema para aprender y adaptarse.
- Equilibrar el objetivo de productividad con el objetivo de seguridad y relajar el objetivo

de eficiencia cuando la circunstancia así lo amerite.

- Desarrollar modelos abstractos comprensibles de las interacciones al interior del sistema que incluyan las entradas de control y resultados de desempeño, así como la relación entre ambos para mantener a las personas vinculadas.
- Tener la disposición para invertir en seguridad y mantener activa la imaginación, incluso sin un historial de eventos adversos.

Lograr estos objetivos desde la alta dirección implica un conocimiento preciso de los procesos que generan estas condiciones y la disposición para rediseñarlos alrededor de un modelo cuidadosamente diseñado y monitoreado. La eficacia de ese modelo está en la gestión de la información que, en cualquier caso, debe sobrepasar la simple recolección de datos y plantea otra serie de retos para el sistema, como se describe a continuación.

4.5 La Información

Un aspecto crítico para alcanzar altos niveles de resiliencia es la traducción de los datos a información. Para Hollnagel (1993, como se cita en Dijkstra, 2006) es habitual que los responsables de la seguridad se confundan al diferenciar los hechos de las causas, esto es, el fenotipo de un incidente que haría referencia a lo que ocurre, lo observable, lo que las personas hacen en realidad del genotipo o conjunto de factores que producen el fenotipo de un evento y que no son directamente observables.

Existen una serie de supuestos sobre los reportes de incidentes que cuestionan la eficiencia de este mecanismo como metodología para predecir posibles fracasos en la seguridad de sistemas complejos. Primero, la capacidad informática de la organización puede ser insuficiente para realizar un análisis lógico, significativo y oportuno a partir de la base de datos; es más, podría ser insuficiente para procesar la cantidad de reportes lo que dificulta la extracción de factores de riesgo o aproximarse a predecir cómo podrían combinarse estos factores nuevamente (Dekker, 2006).

En segundo lugar, Dekker (2006) plantea que no necesariamente los informes de incidentes tienen la información del próximo accidente, pues se ha observado que los accidentes ocurren durante el desarrollo de la operación normal a cargo de operadores calificados; en cambio, en la dinámica del sistema podrían darse algunas deficiencias organizativas no reportadas que se combinan para crear condiciones de riesgo.

Por último, el paradigma que subyace a los sistemas de reporte de incidentes parte de modelos lineales de accidentes que asumen un progreso lineal de fallos que, de interrumpirse, evitaría el evento no deseado; sin embargo, este modelo no es aplicable en sistemas complejos por cuanto la seguridad y los riesgos son fenómenos emergentes derivados de la interacción de componentes mientras se ejecuta el trabajo normal (Dekker, 2006).

Dijkstra (2006) aborda otros retos con respecto al manejo de información específicamente en organizaciones de aviación, entre ellos el efecto de la reducción de una situación compleja a un informe, con información superficial, ausencia de datos del contexto y falta de metodología para asignar una categoría, lo que hace que la categorización e interpretación sea un tema de carácter personal de quien administra los datos o quien investiga.

Menciona también el hecho de que las recomendaciones derivadas de las investigaciones y su aplicación quedan sujetas al nivel de la organización que corresponda, siendo probable que, a juicio de quien tome decisiones, las recomendaciones tengan un efecto negativo en la productividad y, por tanto, no se apliquen en la operación. Lo mismo puede ocurrir si contienen entrenamiento adicional para el personal operativo o cambio en procedimientos o limitaciones de equipamiento (Dijkstra, 2006).

De otra parte, para Dijkstra (2006) es probable que alguna entidad del sistema supervise que se implementen recomendaciones, pero puede no existir un proceso definido para saber si tuvieron el impacto que se esperaba, de manera que los esfuerzos organizacionales por investigar se pierden una vez que el sistema retorna a su estabilidad.

Los retrasos en los informes finales impactan negativamente la capacidad de aprender de la organización, así como la motivación por implementar las recomendaciones; en conclusión, la seguridad del sistema no presenta mejoras (Dijkstra, 2006).

Frente a esta complejidad, los expertos también hacen la salvedad de desarrollar un criterio que le permita a la organización determinar en qué eventos vale la pena realizar un análisis que muestra la complejidad sistémica y cómo se va a manejar la investigación de los incidentes y/o percances de manera que arrojen información oportuna y pertinente para alimentar la comprensión de las concurrencias funcionales del sistema (Woods y Hollnagel, 2006).

Al integrar los conceptos presentados en los apartados anteriores, se aprecia la complejidad de la mirada que hace la ingeniería de la resiliencia a la seguridad dentro de los sistemas sociotécnicos. Sin embargo, el nivel de resiliencia de un sistema no está asociado necesariamente a la no ocurrencia de eventos adversos. Esto plantea la necesidad de reunir la teoría referente a este foco central de la investigación.

4.6 Potencial de Desempeño Resiliente y Seguridad

Una vez descritos los principales planteamientos de la resiliencia organizativa, es oportuna establecer la conexión entre el enfoque de resiliencia y la seguridad operacional.

Desde el campo normativo en la aviación, la Organización de Aviación Civil Internacional (OACI, 2013), define la seguridad operacional como un “estado en el que la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable mediante un proceso continuo de identificación de peligros y gestión de riesgos de la seguridad operacional”.

En esta concepción, una organización es segura en la medida en que tiene menos resultados adversos y es dinámica en cuanto constantemente trabaja por identificar y mitigar riesgos. Sin embargo, esta manera de acercarse a la seguridad aparece lejana al paradigma de la resiliencia, no porque lo contradiga sino porque esta última la implica y la supera (Hollnagel, 2014).

Desde la perspectiva de la resiliencia, seguridad es la capacidad de operar con éxito en condiciones variables, lo que incluye tanto la protección y prevención de resultados no deseados como la capacidad del sistema para funcionar de modo que produzca resultados aceptables (Hollnagel, 2014).

Por tanto, la seguridad es una propiedad emergente de un sistema, es decir, es el resultado de la interacción entre los elementos del sistema. Esto significa que una organización es segura, no por tener menos eventos adversos, sino por la manera en que se comporta con respecto a sus metas de seguridad (Hollnagel, 2006).

Dijkstra (2006) plantea que las actuaciones de algunas organizaciones pueden tener resiliencia, pero fracasar en el sentido de sufrir un evento no deseado; en sentido contrario, algunas actuaciones pueden ser exitosas, pero no demostrar la conformación de un sistema resiliente. Esto se explica al observar los fallos y los éxitos como dos caras de la misma moneda.

Sin embargo, las características de un sistema resiliente, como se mostrará en este apartado, conducen a la conformación de un sistema seguro, en el sentido de definir prácticas, procesos y métodos que fortalecen la capacidad del sistema para sobreponerse a un malfuncionamiento e incluso, anticiparlo. Teniendo en cuenta este argumento teórico, es altamente probable que haya una relación directa y positiva entre potencial de desempeño resiliente y seguridad “(ver H1)” e incluso, estrechando más esa relación, se puede plantear que entre estas dos variables se puede establecer la existencia de una función predictiva “(ver H4)”.

Si las organizaciones, como propone Reason (2011), se mueven en un espacio de seguridad desde un extremo de resistencia hasta un extremo de vulnerabilidad, si siempre existirá la posibilidad de sufrir un evento no deseado por efecto de amenazas naturales, condiciones patógenas latentes, la falibilidad de la actuación humana y/o el azar, entonces es oportuno establecer cuál es la relación entre resiliencia y seguridad.

Para Woods y Hollnagel (2006), una organización resiliente reconoce las actuaciones que hacen explícitas las situaciones riesgosas, independientemente de que haya ocurrido o no algo que haga pensar que realmente se evitó un resultado adverso; es decir, es una organización que informa, que moviliza a las personas a reportar información pertinente en un proceso que cuida la confidencialidad de la información y cuyos resultados de investigación son accesibles, oportunos, útiles y confiables que permite conocer aspectos locales y organizacionales que promueven prácticas inseguras, así como las categorías de acción derivadas (Reason, 2010).

Una organización resiliente hace un adecuado equilibrio entre sus objetivos de producción y seguridad, con lo que demuestra que la seguridad es un valor esencial. Sin embargo, es frecuente encontrar que la productividad, como objetivo inmediato de supervivencia de una organización, se sobreponga a la seguridad generando tensión en el sistema (Woods y Hollnagel, 2006).

Este desequilibrio conduce a la necesidad de que la organización desarrolle un mecanismo que le permita establecer un criterio relajación/sacrificio en condiciones de incertidumbre para mantener un nivel de riesgo aceptable (Woods y Hollnagel, 2006).

Woods (2003, como cita Hale y Heijer, 2006) establece una lista de aspectos relacionados con la seguridad que caracterizan la falta de resiliencia en las organizaciones y que se constituyen en signos para diagnosticar el nivel de seguridad:

- Las defensas se deterioran por acción de la presión de la producción. Priman las decisiones relacionadas con la productividad y el cumplimiento de las operaciones y se sacrifica la seguridad.
- La buena actuación pasada genera confianza futura con respecto al control del riesgo. La organización confía en sus buenos resultados de seguridad (entendida como su baja frecuencia de eventos adversos) y cesa o detiene la inversión de recursos para la seguridad.
- El foco en la solución puntual de situaciones riesgosas no hace explícito el modelo global

de control de riesgo, situación que se evidencia en la pérdida de una visión integrada de la seguridad del sistema en todos sus componentes y una cultura cuyas prácticas erosiona los objetivos de seguridad.

- Las evaluaciones de riesgo no son sometidas a una revisión apropiada con base en la nueva información que ingresa al sistema. El sistema puede ser rígido y no incluir la comparación de los riesgos en los diferentes componentes, lo que indica que las prioridades no están totalmente abiertas a la reflexión sobre los riesgos.
- La comunicación formal y coordinación entre los diferentes niveles organizativos disminuye debido a la existencia de una grieta en las fronteras de seguridad. Canales de comunicación directos creados para informar riesgos se desvían de su fin, se mantienen los canales informales y pueden crearse nuevos canales de coordinación.
- Se pierde flexibilidad frente a las demandas del entorno y situaciones inesperadas. Se entiende la flexibilidad como la posibilidad de que varias personas puedan desempeñar una responsabilidad sin entrar en altos costes o el diseño y puesta en funcionamiento de puntos de control descentralizados.
- Se aprecia un compromiso por la seguridad casi de carácter nominal pues las decisiones rutinarias generan tensiones y riesgos al interior del sistema. O el interés está dirigido solo a un dominio del sistema de seguridad. O,
- La seguridad no está incorporada intrínsecamente en el sistema y tampoco en su modo de operación.

Hale y Heijer (2006) realizaron una investigación en el sistema ferroviario holandés utilizando esta lista y concluyeron que pareciera que el sistema tiene una baja resiliencia; sin embargo, consigue altos niveles de seguridad en ciertas áreas de funcionamiento, con lo que parece demostrar que las actuaciones en seguridad y resiliencia son relativamente independientes cuando se mira la seguridad como la ausencia de eventos no deseados.

Desde el punto de vista de Wreathall (2006) las organizaciones con alta resiliencia se caracterizan por un compromiso de alto nivel que da importancia a la actuación humana, una cultura justa que promueve la disposición de los operadores a informar, una cultura de aprendizaje que genera verdaderos cambios a favor de la seguridad, una conciencia que mueve al equipo de seguridad a recoger datos que muestren al equipo directivo lo que realmente está ocurriendo, hasta dónde es un problema y cuál es el estado de las defensas del sistema.

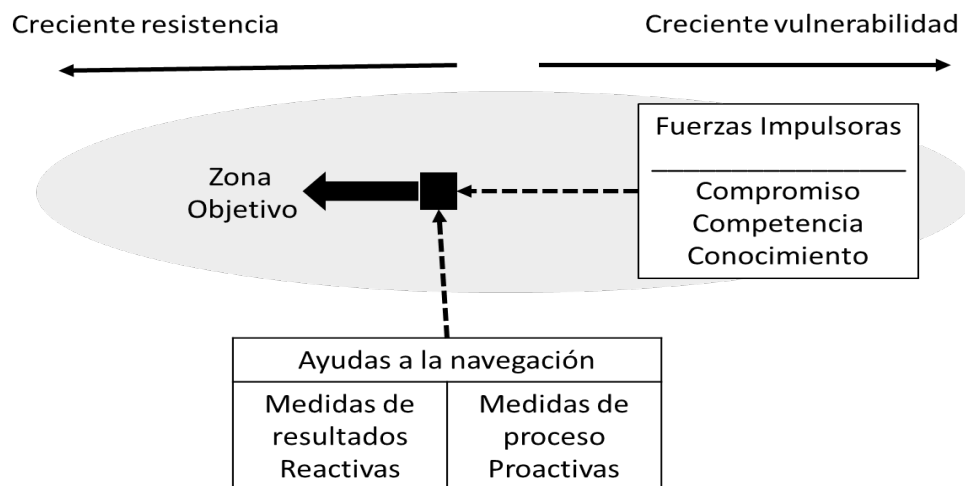
Además, está en estado de preparación para adelantarse a los problemas, es capaz de adaptarse a situaciones nuevas y complejas que retan al sistema a resolver problemas sin afectar su funcionamiento y desarrolla conciencia del límite, es decir, sabe cuándo se encuentra próximo a la zona frontera en lo que respecta a defensas y barreras degradadas.

Con respecto a la medición de la seguridad en organizaciones de alto riesgo, Reason (2010) plantea la necesidad de considerar varios aspectos. Aunque para encauzar el comportamiento organizacional hacia acciones seguras y productivas, se tiende a la procedimentalización y mejoramiento de procesos, la forma habitual de medir la seguridad es a través de los resultados no deseados que surgen durante la operación del sistema. Esto muestra que los datos de resultados no necesariamente hablan de la seguridad intrínseca del sistema.

Ahora bien, si esas estadísticas de resultados no esperados se mantienen estables en un nivel bajo, como en el caso de la aviación, entonces son insuficientes para guiar la gestión de la seguridad operacional. Las organizaciones de alto riesgo requieren conocer lo mejor posible aquellos factores desencadenantes y se dice lo mejor posible porque en el contexto en que operan este tipo de organizaciones, siempre habrá condiciones latentes, por tanto, la gestión de la seguridad debe ir enfocada a defender al sistema de las amenazas y reducir tanto como sea posible los actos peligrosos (Reason, 2010).

Para Reason (2010), tres son los motores de la seguridad: compromiso, competencia y conocimiento. Con el esquema de la figura 8 presenta la dinámica que da cuenta de la manera

en que una organización navega por el espacio de seguridad.



Fuente: Tomado de Reason (2010).

Figura 8. Esquematización de la dinámica de la seguridad

El compromiso está conformado por la motivación y los recursos. El primer componente está relacionado con el interés de la organización por ser un modelo en prácticas de seguridad o si solo busca ir con la normatividad del sector; el segundo hace referencia a la destinación de recursos presupuestales, logístico y humanos calificados para gestionar la seguridad. La competencia tiene que ver con la recolección, difusión y acción de la información que se origina desde los sistemas de recolección de datos (Reason, 2010).

El conocimiento se refiere a la conciencia de la organización sobre los peligros que amenazan su funcionamiento normal. Las organizaciones conocedoras entienden que la seguridad implica un producto y un proceso, luego las medidas de seguridad no se tratan como una lista de chequeo, deben ser observadas, evaluadas y ajustadas en un proceso continuo de aseguramiento (Reason, 2010).

Esos motores de seguridad fueron sometidos a evaluación en esta investigación para establecer la percepción de seguridad y las posibles relaciones entre esta y el potencial de desempeño resiliente. Se incluyeron además aspectos clave de la cultura de la seguridad tratados también por Reason (2010) por tratarse de un atributo clave para la gestión de la

seguridad contemplado también por el autor como eje de su modelo de subsistema de procesos primarios que subyacen a la seguridad operativa, del cual se tomaron algunos factores constitutivos.

Esta conjunción de aspectos constitutivos de la seguridad aportados por Reason (2010) dio como resultado el instrumento cuya estructura se presenta en la tabla 4.

Tabla 4

Estructura de la seguridad operacional

Componente de Seguridad	
Compromiso	Gestión de la Información
Motivación	Pertinencia
Interés por la seguridad	Aporte a procesos
Apoyo a la seguridad	Difusión oportuna
Decisiones sobre procesos	Foco sobre acciones individuales
	Conocimiento de peligros y amenazas
Componente de Gestión de la Seguridad y Operaciones	
Flexibilidad	Coherencia organizacional
Soporte logístico para las operaciones	Entrenamiento
Equilibrio entre objetivos	Estandarización
Nivel de supervisión	Calidad de los indicadores de seguridad
Cultura de la Seguridad	
Accesibilidad	Legitimidad
Estructura del informe	Consenso sobre aceptabilidad de la conducta
Confianza	Imparcialidad en aplicación de acciones correctivas
Autonomía para investigar	Oportunidad y logicidad de acciones correctivas
Oportunidad y accesibilidad a la retroalimentación	
Pertinencia de la información	
Adaptabilidad	Aprendizaje
Autonomía	
Entrenamiento del nivel supervisión	Calidad del aprendizaje
Confiabilidad del nivel supervisión	
Entrenamiento en detección de amenazas	

Fuente: Elaboración propia con base en Reason (2010)

Los atributos culturales abordados, muestran las principales características de una cultura de seguridad. Reason (2010) define la cultura de la seguridad como “el producto de valores, actitudes, competencias y patrones de comportamientos individuales y colectivos que

determinan el compromiso con, y el estilo y la competencia de, los programas de salud y seguridad de una organización... una cultura de la seguridad positiva se caracteriza por la existencia de comunicaciones que se basan en la confianza, por sus percepciones compartidas sobre la importancia de la seguridad y por su confianza en la eficacia de las medidas preventivas (p.251)”.

Sin embargo, a manera de reserva en el manejo de este concepto, es fundamental tener en cuenta que las personas en la organización ejecutan tareas complejas simplificando la manera en que interpretan la situación actual. Para Naevestad (2009) esas simplificaciones son potencialmente peligrosas para las organizaciones de alto riesgo porque limitan las precauciones que toman las personas, así como la capacidad de anticipar consecuencias no deseadas.

Weick (1999, como se cita en Naevestad, 2009) plantea que una cultura de seguridad en organizaciones de alto riesgo se caracteriza por una infraestructura cognitiva particular con ninguna o pocas simplificaciones culturales. Se trata de evaluar los significados que los miembros de una organización atribuyen a las advertencias y señales de peligro en situaciones mal estructuradas.

Para Turner (1978, como se cita en Naevestad, 2009), el modelo de evento no deseado provocado por el hombre se centra en una discrepancia entre un estado del sistema desmejorado dado por sentido y suposiciones y creencias del individuo para enfrentar los peligros. Esa discrepancia es un periodo de incubación del evento adverso en el que las señales de advertencia del sistema son ignoradas o mal interpretadas debido a creencias y expectativas compartidas.

Por lo tanto, una actitud de conciencia colectiva caracterizada por una preocupación constante por el fracaso, el rechazo a simplificar las interpretaciones y el compromiso con la resiliencia debilitan el efecto de las expectativas compartidas. La conciencia colectiva es una

forma eficiente de luchar contra la ignorancia culturalmente inducida a las señales de peligro.

Otro atributo importante en el modelo de cultura es el de cultura justa (legítima) que emerge como un punto medio entre dos formas extremas de responder a eventos adversos: la culpabilización y la no culpabilización. Este atributo implica la creencia de que habrá justicia dentro de los límites del sistema y para ello se debe reconocer que no es aceptable castigar todos los errores sin conocer las circunstancias de actuación y que no es posible hacer exenciones generales (Reason, 2010).

Lo cierto es que el punto de arranque es que todos los participantes están adheridos a una serie de reglas y principios que permite que el sistema funcione en beneficio de su misión. En función de esos principios, la cultura justa imparte acciones cuando existe una violación intencional a ese bagaje normativo preestablecido y compartido porque esa actuación trae un desequilibrio social: quien transgrede una norma obtiene una ventaja injusta sobre otros que no las trasgreden; manifiesta su menosprecio por ellas, por la autoridad y por los pares al colocarse por encima y provoca posibles lesiones como resultado de la violación (Reis-Dennis, 2018).

Un sistema de castigo justo tiene como objetivo restablecer el equilibrio perturbado por las irregularidades, distribuir de manera justa los beneficios para asegurar que las personas sientan que su inversión en la organización no es ingenua y manifestar que todas las personas merecen respeto y trato justo (Reis-Dennis, 2018).

Con base en lo expuesto, el instrumento elaborado para este estudio retomó los principales aspectos de la seguridad y la cultura de seguridad. Presentados estos elementos, en los siguientes apartados se presentan los argumentos teóricos que originaron las hipótesis 2 y 3.

4.7 Potencial de Desempeño Resiliente e Incidentalidad

Desde la perspectiva de la resiliencia, la capacidad de adaptación del sistema se evalúa observando cómo responde a las perturbaciones en su funcionamiento. Esa capacidad

adaptativa tiene límites y los incidentes proporcionan la información necesaria para marcar las fronteras de los mecanismos de adaptabilidad incorporadas dentro del diseño del sistema, mostrarle al sistema cómo se comporta frente a ellas, cómo se puede flexibilizar y cómo puede ampliar esos límites para enfrentar las perturbaciones (Woods y Hollnagel, 2006).

Por lo anterior, algunos autores sostienen que una mayor resiliencia no implica necesariamente una menor accidentalidad por cuanto existe un nivel de azar que puede combinarse con el riesgo inmerso en la operación, la variabilidad de la actuación y la posibilidad humana de fallar (Reason, 2010); un sistema transitará en un continuo entre fragilidad y resistencia de manera que organizaciones con bajos niveles de accidentalidad pueden ocupar lugares totalmente diferentes en ese continuo entre vulnerabilidad y resiliencia (Reason, 2010).

Sin embargo, las estadísticas de incidentalidad son una medida de resultado de casi todas las organizaciones de alto riesgo. Si la resiliencia es una capacidad que contribuye a anticipar la ocurrencia de eventos no deseados, podría pensarse que organizaciones con altos índices de incidentalidad tendrían un menor potencial de desempeño resiliente y una menor percepción de seguridad. Así mismo, organizaciones con menores índices de incidentalidad, tendrían mayor potencial de desempeño resiliente y seguridad “(ver H2)”.

4.8 Trabajo Diseñado vs. Trabajo Real

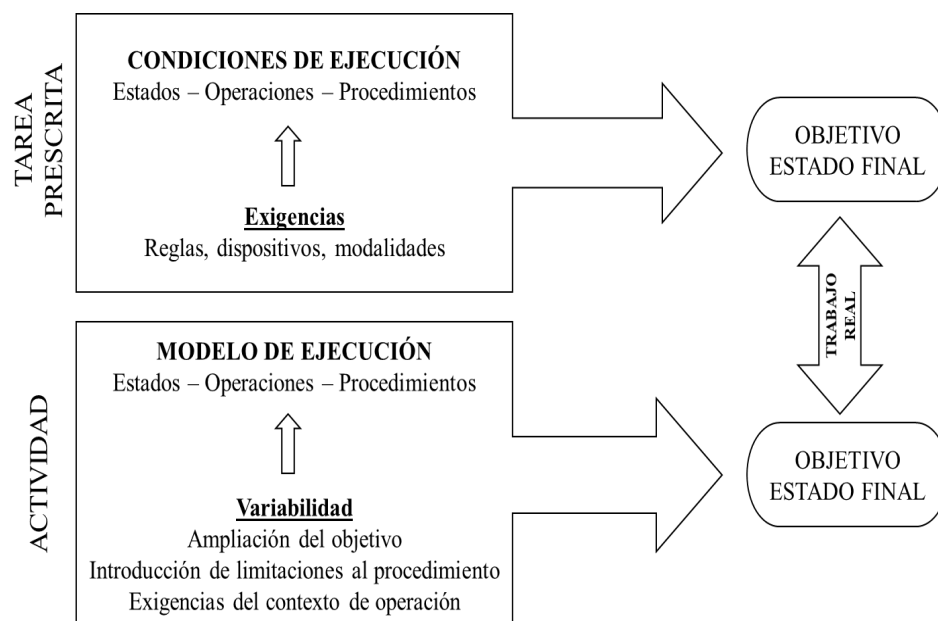
Otro indicador fundamental para los teóricos de la ingeniería de la resiliencia es la habitual brecha que existe entre lo que piensa la gerencia y lo que piensan los operadores respecto a lo que ocurre al interior del sistema. Leplat (1997, como se cita en Poy, Turjanski y Aslanides, 2005) plantea que una de las principales fuentes de variabilidad en el funcionamiento de un sistema tiene relación precisamente con esta brecha que parece existir entre el trabajo como ha sido diseñado y el trabajo tal y como realmente se realiza.

Poy et al. (2005) plantean que la aviación es uno de esos ambientes de alto riesgo que

fundamenta la seguridad en la estandarización de procedimientos para la mayoría de las situaciones posibles, de manera que quede muy poco margen para un imprevisto; sin embargo, lo imprevisto sorprende de manera continua la operación dando paso al criterio e idoneidad personal.

Esta realidad de los sistemas sociotécnicos complejos no es un problema menor: la gestión de riesgos debe tomar en cuenta que las normas y procedimientos formales son necesarios y preparan a los operadores para los riesgos visibles y permanentes de las situaciones de trabajo, pero los riesgos no pueden ser eliminados en su totalidad porque toda actividad es dinámica y, con alguna frecuencia, imprevisible, de modo que el operador es quien realiza de manera cotidiana los ajustes para el éxito de la operación (Poy, et al, 2005).

A esta incertidumbre es a la que aluden Leplat y Hoc (2009) cuando plantean que en todo ámbito laboral existe siempre una serie de tareas prescritas usualmente documentadas en procedimiento que representan lo que se debe hacer en el trabajo, pero también, la actividad, que correspondería a la manera en que se hacen las cosas en la realidad (Figura 9).



Fuente: Elaborada con base en Leplat y Hoc (2009)

Figura 9. Modelo de la tarea prescrita.

La tarea prescrita contiene la descripción de ejecuciones tal y como es concebida por la entidad o persona que asigna la ejecución y, en ese sentido, preexiste a la actividad y pretende encauzarla de la manera más precisa posible, pero casi nunca totalmente completa por cuanto normalmente en una descripción hay unidades implícitas más o menos amplias que desbordan el modelo planteado por la tarea prescrita y le otorgan un carácter relativo (Leplat y Hoc, 2009).

Pareciera entonces que fuera posible la existencia de una divergencia entre las operaciones tal y como los directivos suponen que marchan y el modo en que realmente acontecen, lo cual hace parte de la variabilidad en la ejecución de las tareas y, por tanto, de los éxitos y/o fracasos en la consecución de objetivos (Dekker, 2006). Lo anterior parece evidenciar dificultades en la alineación entre la gerencia y los retos y riesgos de la operación real, lo que genera tensiones durante la operación que podrían incrementar la vulnerabilidad del sistema “(ver H3)”.

Capítulo

5. Evaluación del Potencial de Desempeño Resiliente

Ahora bien, un aspecto que ha sido desarrollado por los expertos dentro del campo de la ingeniería de la resiliencia y que constituye el primer paso para poder introducir mejoras en el sistema, está relacionado con la manera de identificar y, por tanto, medir la resiliencia. En este capítulo se describe la herramienta base para realizar esta investigación y otras que se han desarrollado para perfilar el potencial de desempeño resiliente en una organización.

5.1 Rejilla para el Análisis de Resiliencia

La Rejilla para el Análisis de Resiliencia (*Resilience Analysis Grid / RAG*) fue planteada por Hollnagel (2018). La rejilla aporta una descripción del potencial de desempeño resiliente a partir de la observación de cuatro capacidades básicas interdependientes: la capacidad de responder (“saber qué hacer”), monitorear la situación (“saber qué buscar”), aprender (“saber qué ha ocurrido”) y anticipar (“saber qué esperar”).

Su objetivo no sólo es determinar la calidad en la ejecución de cada una de las cuatro capacidades del sistema sino también proveer una caracterización o perfil de un sistema que puede ser utilizado para desarrollar su potencial de desempeño resiliente (Hollnagel, 2018).

Se basa en un conjunto de preguntas que aborda aspectos funcionales de cada una de estas capacidades para la construcción de un perfil del potencial de desempeño resiliente; esas capacidades operan de manera interdependiente, de modo que para responder adecuadamente, un sistema debe monitorear tanto el contexto como su propio desempeño y, a no ser que el medio ambiente sea estable, la respuesta podría cambiar y desarrollarse sobre el tiempo, lo cual significa que el sistema debe ser capaz de aprender y anticiparse (Hollnagel, 2015).

Van der Vorm, Van der Beek, Bos, Steijger, Gallis y Zwetsloot (s.f.) aseguran que las cuatro capacidades planteadas en el RAG son piedras angulares de la resiliencia y funcionalidades centrales de la resiliencia operativa. Su modelo fue desarrollado con base en

ellas, agregando una estructura de apoyo, la cultura y un sistema de aprendizaje proporcionan elementos clave para el desarrollo de metamodelo que se presenta en la Figura 10.

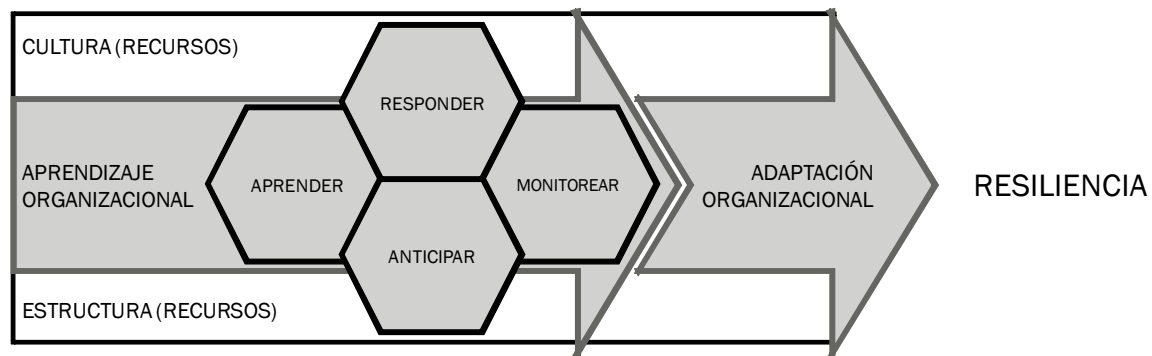


Figura 10. Modelo de Van der Vorm, et al. (s.f.).

Los elementos básicos son: la presencia de las cuatro habilidades de resiliencia, la necesidad de estructura y cultura de apoyo y la identificación y disponibilidad de recursos relevantes para promover y mantener la resiliencia.

Sin embargo, Van der Vorm et al. (s.f.) consideran que las cuatro capacidades resilientes deben analizarse con mayor detalle y traducirse en indicadores medibles junto con la identificación de recursos para el desempeño resiliente, trabajo que dejan como propuesta para futuras investigaciones.

A continuación, se describen cada una de las dimensiones que indaga la rejilla y que son un concepto central dentro del modelo que maneja esta investigación.

5.1.1 Capacidad para responder. Para Hollnagel (2015), esta capacidad consiste en saber qué hacer cuando se presentan cambios regulares/irregulares, disturbios y oportunidades activando acciones preparadas o ajustando el modo actual de funcionamiento. Un sistema, organización u organismo no sobrevive a menos que tenga esta capacidad y pueda ser activada de modo oportuno y efectivo para obtener los resultados deseados.

En este sentido, el sistema debe ser capaz de: (a) detectar que algo está pasando, (b) reconocer qué es, (c) determinar la respuesta necesaria y (d) implementar la respuesta estableciendo cuándo comenzar y cuándo detener la respuesta. Esto implica tener respuesta

preparada y recursos listos o, en su defecto, ser suficientemente flexible para reconfigurar la configuración actual de modo que los recursos necesarios estén disponibles (Hollnagel, 2015).

Para Hollnagel (2015) el potencial para responder no es un tema de reacciones instintivas, es una función que requiere algún tipo de condición o entrada que desencadene la respuesta. Esa entrada puede ser cambios en la situación, sucesos repentinos que interrumpen o desorganizan el flujo de actividades, bien sea una orden distinta, un requerimiento inesperado, un cambio de objetivo, una alerta como resultado de un monitoreo o un cambio interno en la organización.

Esa señal externa marca el momento exacto en que la respuesta es requerida, pero también hay un momento correcto interno en que debe detenerse siempre en función del efecto deseado. No puede detenerse antes, ni tarde, cuando su continuidad podría tener un efecto no previsto por lo que requiere un monitoreo de la condición o situación desencadenante para determinar si ha logrado el efecto deseado (Hollnagel, 2018).

Ese potencial de respuesta está estrechamente vinculado al tipo de amenaza que se enfrenta. No es lo mismo enfrentar una amenaza conocida y frecuente, para la cual el sistema puede desarrollar un procedimiento estándar a otra cuya ocurrencia es infrecuente y, quizá, totalmente nueva. En este caso, el operador actuará como factor de seguridad con base en su propia capacidad (Hollnagel, 2015).

Otra característica de la capacidad de respuesta es que, aunque las condiciones pueden ser obvias y la naturaleza de la respuesta conocida, la respuesta puede no empezar hasta que ciertas condiciones se hayan cumplido. Igualmente, para mantenerse puede requerir la presencia de recursos específicos y darse en el momento crítico, pues si comienza fuera de tiempo el resultado deseado puede no ser alcanzado y si se termina en la misma condición, podrían desperdiciarse valiosos recursos (Hollnagel, 2015).

La aplicación de las preguntas sugeridas por el modelo acerca de la capacidad de respuesta

del sistema, deben llevar al investigador a determinar cómo se establece ese potencial y cómo se puede mejorar o mantener. Algunas de las preguntas que hacen parte de la aproximación a esta capacidad se incluyen en la tabla 5.

Tabla 5

Capacidad para responder

Ítem	Pregunta
Lista de eventos	¿Cuáles son los eventos para los cuales el sistema tiene preparada una respuesta?
Antecedentes	¿Cómo fueron seleccionados estos eventos (tradicción, requerimientos del regulador, bases del diseño, experiencia, experticia, evaluación del riesgo, estándares industriales, etc.)?
Relevancia	¿Cuándo fue creada la lista?, ¿qué tan frecuentemente es revisada?, ¿con qué criterio es revisada?, ¿quién es responsable del mantenimiento y evaluación de la lista?
Límites	¿Cuándo es activada una respuesta?, ¿cuál es el criterio de activación o límite?, ¿el criterio es absoluto o tiene dependencia con factores internos y externos?, ¿hay un intercambio, por ejemplo, entre seguridad y productividad?
Lista de respuestas	¿Cómo se decidió el procedimiento de respuesta?, ¿cómo se determinó que es el adecuado (empíricamente o basado en análisis o modelos)?
Velocidad	¿Qué tan rápida es la capacidad de respuesta disponible?, ¿qué tan rápido puede implementarse una respuesta efectiva?
Duración	¿Por cuánto tiempo se puede mantener una respuesta eficaz al 100%?, ¿cuál es el mínimo aceptable nivel de respuesta y cuánto tiempo puede ser sostenido?
Reglas para detenerse	¿Cuál es el criterio para finalizar la respuesta y retornar al estado normal?
Capacidad de respuesta	¿Cuántos recursos son asignados para garantizar la respuesta preparada (personas, equipo, materiales) ?, ¿cuántos son exclusivos para el potencial de respuesta?, ¿quién es responsable del mantenimiento de esta capacidad?
Verificación	¿Cómo se mantiene la disposición para responder? ¿cómo y cuándo se verifica la disposición para responder?

Fuente: Adaptado de Hollnagel (2015).

5.1.2 Capacidad para monitorear. La capacidad para monitorear hace referencia a conocer qué buscar o ser capaz de monitorear y establecer qué sucesos están afectando o podrían afectar seriamente el desempeño del sistema en el corto plazo. Su desempeño se considera resiliente si la organización tiene la flexibilidad para monitorear tanto lo que pasa fuera del entorno operativo, como lo que sucede dentro de la organización, en su funcionamiento (Hollnagel, 2015).

La capacidad de responder está íntimamente vinculada a esta capacidad que permite evaluar si es necesario implementar acciones, así se trate de eventos menores, pues eso significa que se tiene la capacidad de observar y reconocer tendencias que pueden representar un cambio real con serias consecuencias (Hollnagel, 2018).

El propósito del monitoreo es mantener los ojos sobre lo que ocurre en el ambiente operativo y en la organización en sí misma. Sin esta actividad, el sistema estaría sometido a sorprenderse con cada cosa que ocurriera, situación que es claramente insostenible para una organización en el largo plazo y probablemente no deseable en el corto (Hollnagel, 2015).

En la práctica, una organización debería estar tan preparada tanto como le fuese posible para lo que pueda ocurrir y esto requiere monitoreo. No conocer el estado o preparación de una organización impediría el potencial para responder; sin embargo, este es un aspecto frecuentemente descuidado en las organizaciones (Hollnagel, 2015).

Esta capacidad se basa en indicadores o tendencias cuyo fin es informar si se ha alcanzado un umbral o si se alcanzará en un futuro próximo de continuar con la evolución actual de las cosas. Además del indicador, el potencial de monitorear requiere capacidad para interpretar con el fin de generar una alarma o una alerta. La alarma hace un llamado a una acción concreta, mientras la alerta inicia los preparativos de una respuesta, pero no la respuesta en sí misma. (Hollnagel, 2015).

De esta manera, un monitoreo eficiente contempla la metodología, la frecuencia, el foco, los

criterios y los umbrales. Su mejoramiento se fundamenta en lecciones aprendidas acerca del comportamiento de los indicadores y umbrales de operaciones seguras.

En cuanto a los indicadores, Hollnagel (2015) plantea la existencia de tres tipos: reactivos que se refieren a lo que ha ocurrido o el estado de la organización en el pasado tales como estadísticas de eventos, tendencias, etc., datos que habitualmente se utilizan para ajustar el funcionamiento del sistema y/o evitar disturbios futuros.

Los indicadores proactivos que se convierten en precursores válidos para los cambios y eventos que están por suceder, pero para su interpretación requieren de una descripción articulada o modelo del funcionamiento del sistema. De otro modo, podrían definirse por asociaciones o correlaciones falsas (Hollnagel, 2015).

Estos indicadores son resultado de la interpretación de medidas de los estados actuales y pasados con relación a lo que puede suceder en el futuro. En este sentido, las medidas son usadas como predictores más que como indicadores de estado o de desempeño. Entre ellos se puede citar la interpretación combinada de los recursos disponibles, el estatus técnico de los componentes críticos de la seguridad y el tiempo disponible (Hollnagel, 2015).

Los indicadores estándar se refieren a cosas que ocurren ahora o estados presentes de la organización; un ejemplo son los índices de producción, recursos o niveles de inventario, número de aviones en un sector y se usan para ajustar el desempeño durante la operación (Hollnagel, 2015).

Algunas de las preguntas que permiten sondear esta capacidad de la organización se presentan en la tabla 6.

Tabla 6

Capacidad para monitorear

Ítem	Pregunta
Lista de indicadores	¿Cómo han sido definidos los indicadores?: Por análisis, por tradición, por consenso industrial, por regulación, por estándares internacionales, etc.

Ítem	Pregunta
Relevancia	¿Cuándo fueron creadas estas listas de indicadores?, ¿qué tan frecuentemente son revisadas?, ¿sobre qué bases son revisadas?, ¿quién es responsable por el mantenimiento de la lista?
Indicadores tipo	¿Cuántos indicadores son de tipo conducción y cuántos de tipo rezago? ¿Los indicadores se refieren a medidas únicas o agregadas?
Validez	¿Cómo se establece la validez de un indicador?, ¿los indicadores se refieren a modelos de procesos articulados o simplemente al sentido común?
Retraso/rezago	Para los indicadores de rezago ¿qué tiempo es el retardo típico?, ¿es aceptable?
Tipos de medida	¿Cuál es la naturaleza de la medida (cuantitativa o cualitativa)? Si es cuantitativa ¿qué clase de escala se está usando?
Frecuencia de la medida	¿Qué tan frecuentemente se realizan las medidas?: Continuamente, regularmente, ¿cada cuánto?
Análisis / interpretación	¿Cuál es el retraso entre las medidas y el análisis/interpretación?, ¿cuántas de las medidas son directamente significativas y cuántas requieren análisis de algún tipo?, ¿cómo son comunicados y utilizados los resultados?
Estabilidad	¿Los efectos de las medidas son transitorios o permanentes?
Apoyo organizacional	¿Existe un plan de inspección o programa regular?, ¿tiene los recursos adecuados?

Fuente: Adaptado de Hollnagel (2015).

5.1.3 Capacidad para aprender. Esta capacidad implica los mecanismos del sistema para determinar qué ha pasado o ser capaz de aprender desde la experiencia adecuada las lecciones correctas con una apropiada comprensión de los eventos. A menos que el medio ambiente sea perfectamente estable y predecible, la capacidad para responder y para monitorear dependen de la capacidad para aprender: aprendizajes eficientes y sistemáticos desde la experiencia requieren una planeación cuidadosa y amplios recursos (Hollnagel, 2015).

El aprendizaje desde la experiencia es importante para diferenciar lo que es fácil de aprender de lo que es significativo aprender. El nivel de seguridad tradicionalmente se expresa en términos de los números y las frecuencias de ocurrencia de eventos adversos; sin embargo, la compilación de extensas estadísticas de accidentes no significa que alguien realmente aprenda

algo; es decir, contar cuántas veces sucede algo no es aprender (Hollnagel, 2015).

Adicionalmente, en gestión de la seguridad operacional, aprender se ha focalizado sobre las cosas que salen mal (accidentes, incidentes o eventos de seguridad) porque estos eventos son fáciles de capturar y son motivo de preocupación, pero desde el número de cosas que están bien, incluyendo casi fallas –cuya magnitud es mayor que el número de cosas que salen mal– habitualmente no se hacen aprendizajes aunque resulte lógico intentar aprender de eventos representativos (frecuencia) y no sólo de fallas (severidad) (Hollnagel, 2015).

No hay que olvidar que conocer cuántos eventos han ocurrido no dice nada acerca de por qué han ocurrido y mucho menos acerca de las muchas situaciones en las que no ocurrieron accidentes. Sin saber por qué sucede algo, así como por qué no sucede, es imposible proponer maneras efectivas de mejorar la seguridad (Hollnagel, 2015)

Hollnagel (2010) plantea que tres condiciones pueden dirigir a la organización hacia un aprendizaje significativo: 1) tener oportunidades de aprender; es decir, alta frecuencia de situaciones que pueden generar aprendizaje. Por eso es más pertinente aprender de eventos ordinarios que de eventos anormales. 2) las situaciones deben tener características similares para que sean comparables entre sí y 3) debe crearse un mecanismo que permita confirmar la realización de un aprendizaje correcto de los eventos entendiendo que una lección se ha aprendido cuando genera un cambio en el comportamiento. Si nada ha cambiado, no se ha aprendido algo (tabla 7).

Tabla 7

Capacidad para aprender

Ítem	Pregunta
Criterios de selección	¿Cuáles eventos son investigados y cuáles no (frecuencia, severidad, valor, etc.)?, ¿cómo se hace la selección?, ¿qué criterios son utilizados?, ¿quién realiza la selección?
Aprendizaje básico	¿El sistema intenta aprender desde sus éxitos (cosas que hace bien) así como de sus fallas (cosas que se hacen mal)?

Ítem	Pregunta
Clasificación	¿Cómo se describen los eventos?, ¿cómo se recolecta y categoriza la información?
Formalización	¿Hay algún procedimiento formal para la recolección, análisis y aprendizaje de información?
Entrenamiento	¿Hay algún procedimiento formal o soporte organizacional para la recolección de información, análisis y aprendizaje?
Estilo de aprendizaje	¿Es el aprendizaje una actividad continua o discreta (¿impulsada por eventos?
Recursos	¿Se dispone de recursos para la investigación y el aprendizaje?, ¿son adecuados?, ¿de qué criterio dependen ellos?
Retrasos	¿Cuál es el retraso entre el reporte y el aprendizaje?, ¿cómo se comunican interna y externamente los resultados?
Objetivos de aprendizaje	¿En qué nivel toma efecto el aprendizaje? ¿Individuos, colectivos, organización?
Implementación	¿Cómo se implementan las lecciones aprendidas: regulaciones, procedimientos, normas, entrenamiento, instrucción, rediseño, reorganización, etc.?

Fuente: Adaptado de Hollnagel (2015).

5.1.4 Capacidad para anticipar. Continuando la descripción de Hollnagel (2015), la capacidad para anticipar es saber qué esperar o ser capaz de anticipar desarrollos en el futuro, así como interrupciones potenciales, demandas nuevas, condiciones, amenazas y oportunidades futuras que podrían ser beneficiosas o causar detrimento del funcionamiento óptimo del sistema. La organización no puede limitarse a mirar lo que sucede dentro de ella misma, debe dirigirse a lo que ocurre en su entorno.

La evaluación del riesgo se focaliza en amenazas futuras y es adecuado para sistemas muy estables donde se conocen los principios de funcionamiento y en donde las descripciones pueden hacerse con relativa rapidez, no contienen demasiados detalles y permanecen válidas durante mucho tiempo (Hollnagel, 2015).

Sin embargo, muchos sistemas actuales no son así; en su lugar, existe alta variabilidad en el sistema de modo que las descripciones están frecuentemente desactualizadas y los

principios están subespecificados o son parcialmente conocidos. Si existen descripciones, contienen muchos detalles y toman largo tiempo para estructurarse. Por ello, tradicionalmente los métodos de evaluación de riesgos son inadecuados o francamente inapropiados.

La anticipación de las oportunidades futuras tiene poco soporte en los métodos actuales y esto debe considerarse tan importante como la búsqueda de amenazas futuras (tabla 8).

Tabla 8

Capacidad para anticipar

Ítem	Pregunta
Experticia	¿Qué clase de experticia se necesita para mirar al futuro?, ¿in house o subcontratado?
Frecuencia	¿Con qué frecuencia se evalúan las amenazas y oportunidades futuras?
Comunicación	¿Cómo se comunican o comparten las expectativas acerca de eventos futuros dentro del sistema?
Estrategia	¿El sistema tiene claramente formulados los modelos del futuro?
Modelos	¿El modelo o suposiciones acerca del futuro son explícitas o implícitas?, ¿cualitativas o cuantitativas?
Horizonte de tiempo	¿Cuánto tiempo tarda el sistema en mirar hacia el futuro?, ¿Es el horizonte de tiempo diferente para, por ejemplo, el negocio y la seguridad?
Aceptabilidad del riesgo	¿Cuál riesgo es considerado aceptable y cuál inaceptable? ¿Con base en qué?
Etiología	¿Cuál es la naturaleza asumida del futuro? Amenazas, oportunidades
Cultura	¿La conciencia del riesgo hace parte de la cultura organizacional?

Fuente: Adaptado de Hollnagel (2015).

Como recomendaciones finales, Hollnagel (2015) sugiere que los conjuntos de preguntas que se desarrollan para un uso específico deben ser formuladas de modo que puedan ser fácilmente evaluadas. Esto significa que deben referirse a relaciones concretas o características del desempeño del sistema, a algo con lo que los encuestados tienen experiencia o algo que se describe en la documentación del sistema.

Los temas abordados por las preguntas no pueden considerarse aisladamente. Un sistema no puede ser entendido simplemente como una combinación lineal de sus partes, sino que debe ser reconocido como un todo en el que las dependencias o acoplamientos entre las partes son críticos para el rendimiento global (Hollnagel, 2015).

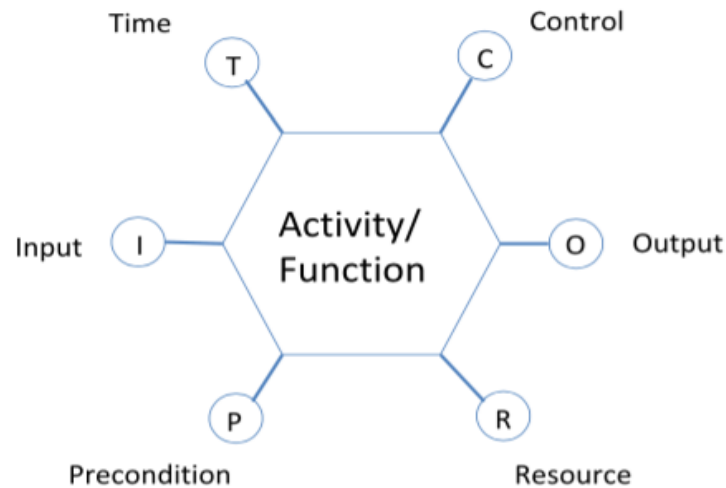
La anterior es una descripción general de las capacidades que definen la resiliencia desde la perspectiva de Hollnagel (2018). Esta herramienta fue construida con la flexibilidad de ser adaptada a contextos de acuerdo con las necesidades de investigación. Ljungberg y Lundh (2014) la usaron para identificar la capacidad de resiliencia con respecto a la ocurrencia de disturbios o eventos no planificados en controladores de tránsito aéreo. Los investigadores construyeron su propia versión del RAG y crearon a partir de allí un perfil de resiliencia.

5.2 Otros Métodos de Evaluación de la Resiliencia

A continuación, se presentan varias investigaciones en diversos dominios que muestran los abordajes distintos para evaluar la capacidad resiliente de una organización.

5.2.1 Método de análisis de resonancia funcional FRAM. Desarrollado por Hollnagel, el FRAM (Figura 11) tiene como objetivo capturar la dinámica de sistemas sociotécnicos complejos mediante el modelado de las dependencias no lineales y la variabilidad que experimentan las funciones y los comportamientos emergentes potencialmente relevantes para la resiliencia.

Este método tiene la capacidad de acomodar sucesos pasados que normalmente se abordan mediante análisis de accidentes, por lo que también se utiliza con este fin y para comprender sucesos futuros a los que normalmente se accede mediante métodos de evaluación de riesgos o modelos de sistemas (Hollnagel, 2004).



Fuente: Tomado de Bellini, Cocone y Nesi, (2018).

Figura 11. Método FRAM. El método no solo describe una función, sino que involucra la observancia de la variabilidad interna de la salida de la función X y en relación con otras funciones del sistema.

De acuerdo con este enfoque, una función se refiere a las actividades o conjunto de actividades que se ejecutan para producir un resultado esperado y está compuesta por seis aspectos: cinco entradas (input, tiempo, control, precondition y recursos) y una salida (resultado), como se mostró en la figura 11.

Para utilizar el modelo, el primer paso es la definición del propósito del análisis y seguidamente se identifican y describen las funciones del sistema que serán el foco de análisis, así como sus límites y el nivel de detalle o grado de resolución para la descripción de la función (Hollnagel, 2013).

El modelo define seis fuentes principales de variabilidad del desempeño humano y organizacional: 1) características fisiológicas y psicológicas, 2) fenómenos psicológicos de nivel superior utilizados para superar las limitaciones temporales y la subespecificación, 3) condiciones y requisitos de la organización, 4) factores psicológicos sociales o de equipo, 5) variabilidad de las condiciones del trabajo y 6) variabilidad del entorno (Hollnagel, 2013).

El modelo FRAM que ha sido usado habitualmente para analizar los accidentes y para la evaluación de riesgos, ha sido empleado por otros autores para recoger resultados exitosos y

ganar efectividad (Furniss, Curzon & Blandford, 2016).

5.2.2 Otros métodos y modelos. Un acercamiento cuantitativo para medir la resiliencia de un sistema fue presentado por Shirali, Mohammadfam y Ebrahimipour (2013) quienes evaluaron la resiliencia en una planta de procesos industriales a partir de un cuestionario con seis dimensiones: compromiso de la alta dirección, cultura justa, cultura de aprendizaje, conciencia y opacidad, preparación y flexibilidad. El cuestionario incluyó un total de 61 preguntas tipo Likert que fueron validadas en un estudio piloto y la información se analizó utilizando el análisis de componentes principales (PCA) y la taxonomía numérica (NT Approach).

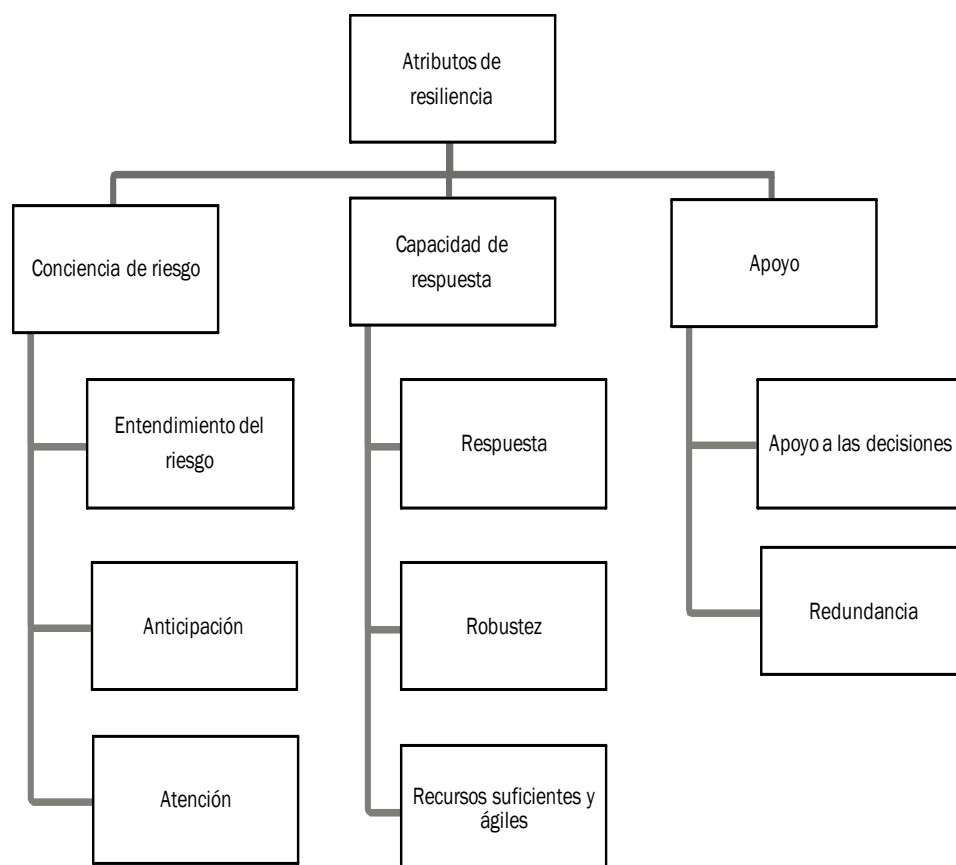
Los autores encontraron que el PCA permitió identificar las unidades con bajos indicadores de resiliencia y plantear medidas para mejorar: crear un sistema de informes de incidentes, accidentes y casi accidentes, mejorar la capacitación con base en enfoques proactivos, cambiar las ideas tradicionales sobre accidentes y reemplazarlas con previsión, cambiar el sistema de investigación de accidentes dirigiéndola hacia procesos y funciones, considerar la seguridad y la resiliencia como un valor establecer un sistema de retroalimentación eficiente e invertir en la mejora de la seguridad.

Posteriormente, Shirali, Motamedzade, Mohammadfam, Ebrahimipour y Moghimbeigi (2015) realizaron otra investigación en procesos industriales utilizando los mismos estadísticos. En esta investigación se evaluaron nueve factores asociados a la resiliencia: capacidad de amortiguación, margen, tolerancia, interacción entre escalas, cultura de aprendizaje, flexibilidad, anticipación, atención y respuesta. Los datos se recopilaron mediante entrevistas semiestructuradas con preguntas de opción múltiple, análisis de documentos, grupos focales y conversaciones informales.

Para Shirali et al. (2015) los resultados de evaluaciones cualitativas son difíciles de emplear por cuanto generan una gran cantidad de hipótesis que dificultan su nivel de precisión. Sin

embargo, la posibilidad de construir modelos numéricos para aproximarse a resultados intangibles también lo es, pero se constituye en un camino legítimo para plantear potenciales interacciones de variables en un sistema que contribuyan al mejoramiento de su resiliencia.

Oien, Massaiu, Tinmannsvik y Storseth (2010) demostraron que es posible desarrollar un sistema de indicadores a manera de alertas tempranas para el sistema con base en la ingeniería de la resiliencia. La investigación se realizó en una organización dedicada a la exploración de petróleo y gas y parte de un método desarrollado por el Instituto de Energía Eléctrica de Estados Unidos conocido como “Indicadores Principales de Salud Organizacional, LIOH”. Como un primer paso para su desarrollo, los autores plantearon el modelo que se ilustra en la figura 12.



Fuente: Tomado de Oien, Massaiu, Tinmannsvik y Storseth (2010).

Figura 12. Factores contribuyentes de éxito modelo REWI. Criterios utilizados para operativizar el concepto de resiliente basado en el supuesto de que una característica clave de la idea de resiliencia es la interacción e intercambio entre diferentes capas del sistema, niveles y puntos focales. Los factores que presenta el modelo pueden especificarse en cualquier capa organizativa.

A cada uno de ellos se le plantearon problemas generales con propuesta de indicadores de alerta temprana con la opción de poder incluir nuevos problemas e indicadores según la evolución del diseño. El modelo demostró funcionar apropiadamente para los objetivos de la compañía y su aplicación fue sencilla al contemplar un solo nivel de problemas, pues el método LIOH propone plantear un problema general y objetivos específicos.

El método, denominado por los autores “Resiliencia basada en Indicadores de Alerta Temprana, REWI (Resilience Based Early Warning Indicator)”, proporcionó un lenguaje común para hablar de seguridad, moviliza recursos para monitorear y evaluar la seguridad y promueve el diálogo entre unidades, áreas y personas sobre temas de seguridad.

Azadeh, Salehi, Arvan y Dolatkah (2013) realizaron una investigación en una planta petroquímica cuyo objetivo fue evaluar los factores que afectan el nivel de resiliencia a través de la aplicación de mapas cognitivos difusos. Los autores encontraron que los factores de resiliencia con mayor influencia son la conciencia, la preparación y la flexibilidad, el de menor influencia es el factor redundancia.

Carvalho, dos Santos, Gomes y Borges (2007) realizaron una investigación en la que diseñaron una vista esquemática de un sistema de control en una planta nuclear que contribuyera al análisis de microincidentes. Este marco pretendía ofrecer una visión anticipada de las acciones de control de los operadores y proporcionar elementos para el análisis sobre la posibilidad de que situaciones problemáticas relativamente pequeñas en las capas del sistema débilmente acopladas puedan conducir a resultados negativos en algún momento futuro.

Los autores encontraron que, para lograr un desempeño resiliente, los operadores no pueden confiar solo en las construcciones organizacionales formales (normativas). Los operadores negocian compensaciones entre objetivos en conflicto, toma de decisiones y

resuelven problemas a través de adaptaciones locales utilizando bucles de retroalimentación recursiva.

Goldbeck, Angeloudis y Ochieng (2019) propusieron una medida genérica de evaluación de la capacidad de resiliencia que puede ser utilizada en sistemas de infraestructura críticos. Este modelo combina el paradigma de modelado de flujo de red con una representación novedosa de activos de infraestructura reparables y considera las dependencias relacionadas con la propagación de fallas, la arquitectura del sistema de sistemas y los recursos necesarios para operar y reparar activos.

Huber, Gomes y Rodrigues (2012) diseñaron un método para el desarrollo de indicadores capaces de informar a una organización sobre el estado de su resiliencia a través de un proceso cíclico de identificación de factores de resiliencia, medición a partir de indicadores, evaluación y mejoramiento. El método fue probado por los autores en una compañía de taxis aéreos en la que se desarrollaron indicadores a tres niveles: 1) operadores de campo, 2) gerentes de operaciones de campo y 3) investigadores y desarrolladores de sistemas. En la investigación, los expertos comprobaron la eficiencia del método.

Estas investigaciones muestran la variedad de enfoques utilizados para medir la resiliencia de la organización. En este estudio se utiliza el RAG como herramienta para diagnosticar la capacidad de resiliencia de la organización y señalar los escenarios de mejora organizacional, debido a que la adaptabilidad de su estructura facilita su adaptación a la realidad de la organización para hacer un mapeo general y efectivo de las principales capacidades resilientes y puede ajustarse para ser aplicada dentro del marco de investigación cuantitativo.

Sección Empírica

Capítulo

6. Marco Metodológico

Seguidamente se definen los elementos metodológicos básicos para este estudio desde una perspectiva de investigación científica como garantía de validez interna y externa (Hernández, Fernández y Baptista, 2014) en el marco disciplinar de la psicología como área del conocimiento científico y, en particular, de la psicología del trabajo como campo teórico-práctico del ejercicio profesional (Gómez, 2016).

6.1 Objetivo General

Analizar la relación entre el potencial de desempeño resiliente y la seguridad operacional en una organización de aviación militar colombiana, así como describir factores organizacionales asociados.

6.2 Objetivos Específicos

Objetivo específico 1. Determinar la relación que existe entre potencial de desempeño resiliente y seguridad operacional.

Objetivo específico 2. Analizar las diferencias en el potencial de desempeño resiliente entre clúster de incidentalidad¹ que homogenizan las unidades operacionales de la organización.

Objetivo específico 3. Analizar las diferencias en el potencial de desempeño resiliente entre los niveles gerencial y operador de la organización de aviación.

Objetivo específico 4. Formular una relación predictiva que permita establecer el grado de seguridad operacional en función del potencial de desempeño resiliente.

Objetivo específico 5. Describir factores organizacionales que contextualizan la relación

¹ En el marco de esta investigación, las unidades aéreas operativas se agruparon en clúster de muestras homogéneas con base en un criterio de nivel relativo de incidentalidad (Horas de vuelo / incidente) según consulta a la entidad aérea (Ver ecuación 1, pág. 106). Lo anterior con el propósito de hacer comparaciones válidas de acuerdo con el grado de exposición al riesgo. (N. de la A.).

entre potencial de desempeño resiliente y la seguridad operacional en el ámbito de la organización.

6.3 Hipótesis

1. Se espera encontrar correlación significativa directa entre el potencial de desempeño resiliente y la seguridad operacional, de manera que un mayor potencial de desempeño resiliente se relacione con un mayor nivel de seguridad operacional y viceversa.
2. Se espera que existan diferencias en el potencial de desempeño resiliente entre clúster de incidentalidad, de manera que los clúster de mayor incidentalidad tengan promedios significativamente menores en los puntajes de seguridad operacional y potencial de desempeño resiliente y viceversa.
3. Se espera que existan diferencias estadísticamente significativas en el potencial de desempeño resiliente entre el nivel gerencial estratégico de la seguridad operacional y los nivel táctico y operacional de la organización de aviación.
4. Se espera establecer una función predictiva que permita estimar el nivel de seguridad operacional en función del potencial de desempeño resiliente.
5. Se espera encontrar configuraciones organizacionales imperantes que den cuenta de los hallazgos de la investigación, desde un enfoque comprensivo.

6.4 Método

A continuación, se desarrollan puntualmente los aspectos metodológicos para abordar el problema de investigación, lograr los objetivos y someter a prueba las hipótesis propuestas, definiendo desde el tipo de investigación y el diseño hasta la precisión del procedimiento, el plan de análisis y los respectivos referentes éticos de la investigación.

6.4.1 Tipo de estudio. El método de investigación de este estudio fue de tipo mixto que combina los enfoques cuantitativo y cualitativo de la investigación científica. La fase cuantitativa fue de tipo correlacional y de comparación de grupos (Hernández et al. 2014) y la

segunda fase, de tipo cualitativa, planteó un análisis de tipo fenomenológico cuyo objetivo fue obtener una visión comprensiva de las relaciones entre el potencial de desempeño resiliente de la entidad militar y la seguridad operacional según el análisis aportado por un grupo de personas de diferentes niveles de la organización (Hernández et al. 2014).

Con ello se buscó acceder con una visión más holística e integral al objeto de estudio para obtener mayor riqueza interpretativa (Hernández et al. 2014).

6.4.2 Tipo de diseño. Esta investigación se realizó con base en un diseño secuencial explicativo (Hernández et al., 2014). En la fase cuantitativa inicial se planteó un estudio no experimental de tipo correlacional y comparativo de grupos. También se analizaron las decisiones secuenciales y las probabilidades asociadas al entendimiento de una determinada acción relacionada con el potencial de desempeño resiliente.

En la fase cualitativa se realizó un estudio fenomenológico a partir de la realización de dos grupos focales y entrevista personal a cinco sujetos de la organización. Con la información recolectada se buscó comprender con mayor amplitud los resultados obtenidos del análisis correlacional y comparativo de la fase cuantitativa inicial.

La utilidad, tanto de los grupos focales como de las entrevistas como técnica de investigación para este estudio, fue explorar la problemática revelada en la fase cuantitativa de manera que las discusiones fueron semiestructuradas a partir de los hallazgos para generar posibles argumentos explicativos a los datos.

6.5 Muestra

La muestra en la fase cuantitativa estuvo conformada por 545 pilotos, algunos de ellos con formación previa en seguridad operacional.

En la fase cualitativa, la muestra incidental fue de 14 oficiales que accedieron voluntariamente a participar en las sesiones de grupo focal y entrevistas.

6.5.1 Elegibilidad de los participantes. Como criterio de inclusión se estableció que fueran

pilotos militares, pertenecientes a la organización, con cargos asignados en el sistema de seguridad operacional o sin tal condición, que aceptaran participar libre y voluntariamente en la investigación, quienes previa manifestación del consentimiento informado, procedieron a realizar el diligenciamiento de los cuestionarios (Anexos C y E).

Como criterio de exclusión se estableció que no se incluirían pilotos que presentaran una evidente aprehensión al tema o a los procedimientos del estudio, así como también se excluirían aquellos formatos que, al ser diligenciados, tuvieran un número significativo de ítems sin responder (>50% en alguna de las dos pruebas).

6.5.2 Diseño de la muestra. Los participantes se obtuvieron mediante un modelo de muestreo probabilístico aleatorio simple no estratificado de la lista general de pilotos de la entidad, quienes fueron convocados por correo electrónico institucional.

Para efecto de proteger la validez estadística, el tamaño de muestreo mínimo para tener una potencia esperada (*power*) (capacidad probabilística para no cometer errores I y II [Daniel, 2002]) de 0,80, bajo un nivel de significancia alfa de 0,05 y una hipótesis unilateral, se toma como estimador el parámetro poblacional $\gamma > 0,5$ (hipótesis alternativa) de la correlación entre el potencial de desempeño resiliente y la seguridad operacional vs. una correlación de nulidad $\gamma \leq 0,35$ (hipótesis de nulidad) entre tales variables.

Con base en ello se alimentó el aplicativo de software “Tamaño de la Muestra” versión 1.1 (Pérez, Rodríguez, Gil y Ramírez, 2001) arrojando el resultado puntual que se presenta en la figura 13.

Prueba de hipótesis para el coeficiente de correlación

Toma de datos

-Error tipo I: .05

-Error tipo II: .2

-Coef. correlación poblacional: .5

-Valor de prueba en la hipótesis nula: .35

Calcular... Cerrar

Resultados

Tamaño muestra: 369

Tipo de cálculo

☒ 1 Cola ☐ 2 Colas

☒ Tamaño muestra ☐ Poder

Fuente: Elaborada con aplicativo de software Tamaño de la Muestra. Versión 1.1 (Pérez et al. 2001).

Figura 13. Cálculo del tamaño muestral

El tamaño de muestra calculado como mínimo requerido fue de 369 sujetos; no obstante, por previsión metodológica, en la aplicación de estudios psicosociales se puede agregar un 5% para efecto de prever pérdida de muestra por factores de abandono, diligenciamiento inadecuado de instrumentos o similares. Así, el tamaño de muestra establecido para el estudio como mínimo requerido fue de 409 sujetos; sin embargo, se recibió mayor participación y el tamaño de la muestra final fue de 545 pilotos participantes, de un total de 870 que componen la población, lo cual da una participación del 62,6% de la población.

Con esto se garantiza a priori un poder del 0,80, lo cual indica que la significancia de las pruebas de hipótesis de las correlaciones estaría dentro de límites estadísticamente permisibles para ser significativas, con lo cual se puede afirmar que la evidencia obtenida tiene la debida validez externa y validez estadística (Kerlinger y Lee, 2002; Suárez, 2015; Vera, 2018).

No obstante, luego de obtenidos los datos se procedió a estimar a posteriori el poder final del estudio, lo que se describe como parte de cierre del capítulo de Resultados. Esta es una

manera de certificar que el estudio no fuese falso positivo (Error I) o falso negativo (Error II) (Pérez et al., 2001).

6.6 Variables de Investigación

Para efectos de este estudio, en la tabla 9 se definen operacionalmente las variables que fueron consideradas.

Tabla 9

Definición operacional de variables

Nombre	Definición	Medición / Itto.	Unidades / Categorías
Variables Predictoras			
Potencial de Desempeño Resiliente:	Capacidad intrínseca de la Institución para reajustar su funcionamiento antes, durante o después de cambios o perturbaciones que permita desarrollar las operaciones luego de un contratiempo significativo o en presencia de presión continua (Hollnagel, 2014). Contempla las siguientes capacidades:	Numérica ordinal con métrica intervalar. Itto: Escala PoDeRe y sus subescalas.	Puntaje %. [(Categorías: Baja (0-70) / Media (>7-85) / Alta (>85-100)]
Capacidad de responder	“Saber qué hacer” con base en la experiencia y en consideración de los efectos previos obtenidos.		Puntaje %
Capacidad de monitorear	“Saber qué buscar” al momento de valorar continuamente las operaciones de la entidad en su propósito misional.		Puntaje %
Capacidad de aprender	“Saber qué ha ocurrido” y qué puede mejorar para futuras situaciones.		Puntaje %
Capacidad de anticipar	“Saber qué esperar” ante la demanda operacional y con la consideración de la experiencia previa.		Puntaje %
Escenarios: Contextos y ámbitos institucionales en los que se expresa el potencial de desempeño resiliente. Se consideraron los siguientes escenarios:			
Escenario 1.	Ejecución de operaciones (mantenimiento, vuelo y entrenamiento)	Cualitativa Ordinal.	Puntaje %
Escenario 2.	Entrenamiento de personal operativo (pilotos, controladores, operarios de mantenimiento)	Itto: Escala PoDeRe	Puntaje %
Escenario 3.	Supervisión de procesos operativos (mantenimiento, operaciones y entrenamiento).		Puntaje %
Clúster eventos de seguridad operacional	Agrupación de unidades operativas que comparten características de incidentalidad ² lo que supone situaciones similares en gestión del	Cualitativa Ordinal. Registro de	Menor Intermedio Mayor

² Se consideraron “incidentes” a aquellos eventos ocurridos que podrían potencialmente incidir en la operación aérea (N. de la A.).

Nombre	Definición	Medición / Itto.	Unidades / Categorías
	riesgo/acción de la seguridad operacional. Se tomó en consideración la relación funcional: $\text{Incidentalidad} = (\# \text{ horas de vuelo}) / \text{Incidente}$	incidentes.	
Variable Criterio			
Seguridad operacional:	Dinámica de acción en que la posibilidad de afectar a personas, equipos o instalaciones se reduce y/o mantiene mediante un proceso continuo de identificación de peligros y gestión de riesgos (OACI, 2013). Da cuenta de la capacidad del sistema para operar con éxito en condiciones variables, que incluye protección y prevención de resultado no deseado. Es la capacidad para funcionar de modo que se produzcan resultados aceptables (Hollnagel, 2014). Contempla los siguientes componentes:	Numérica ordinal con métrica intervalar. Itto: Escala SegOp y subescalas.	Puntaje % [Categorías: Baja (0-70) / Media (>71-85) / Alta (>85-100)]
I. Componente de Seguridad	1.1 Compromiso 1.2 Gestión información		Puntaje % Puntaje %
II. Componente gestión de seguridad y operaciones			Puntaje %
III. Componente Cultura de la Seguridad	3.1 Accesibilidad 3.2 Legitimidad 3.3 Adaptabilidad 3.4 Aprendizaje		Puntaje % Puntaje % Puntaje % Puntaje %
Otras variables			
Unidad operativa	Unidad organizacional con funciones operacionales y responsabilidad de gestión operacional.	Cualitativa nominal	(según reporte de asignación de cada piloto)
Nivel de participación en las operaciones	Grado de responsabilidad y decisión en la cotidianidad del accionar misional de la entidad.	Cualitativa Ordinal.	1. 1° Nivel 2. 2° Nivel 3. 3° Nivel
Tiempo experiencia de vuelo	Tiempo de desempeño en las actividades de vuelo, como piloto.	Autoreporte	1. <5 años 2. 5-10a. 3. 10,1-20a. 4. >20a.
Oficial seguridad operacional	Funcionario de la entidad con formación básica, intermedia y/o avanzada en seguridad operacional.	Cualitativa nominal	Sí No
Tiempo de desempeño en cargo seguridad	Tiempo de desempeño en cargos directamente relacionados con la gestión de la seguridad operacional.	Cualitativa Ordinal.	1. <5 años 2. 5-10a. 3. 10,1-20a. 4. >20a.
Tiempo de desempeño en sistema seguridad	Tiempo de desempeño en cargos, funciones o tareas de operaciones, entrenamiento y/o mantenimiento.	Cualitativa Ordinal.	1. <5 años 2. 5-10a. 3. 10,1-20a. 4. >20a.

Fuente: Elaboración propia de la autora.

6.7 Instrumentos de Medición

Seguidamente se describen los instrumentos que fueron utilizados en el desarrollo de esta investigación.

6.7.1 Escala potencial de desempeño resiliente -PoDeRe-. Esta escala (Anexo B) se elaboró con base en la estructura y los contenidos de la rejilla genérica (Resilience Analysis Grid -RAG-) propuesta por Hollnagel (2015), como desarrollo para Colombia y específicamente para organizaciones de aviación militar.

6.7.1.1 Validación de contenido. Los ítems fueron sometidos a validación de contenido con un panel conformado por dos psicólogas militares con conocimientos de psicometría y cuatro pilotos militares con experiencia operacional, quienes actuaron como jueces expertos. En los 51 ítems se encontró en promedio un nivel de acuerdo en la validez de contenido (concordancia interevaluadores) de 98,0% ($\pm 5,4\%$) y en la claridad idiomática (redacción) de 90,2% (10,1%) (tabla 10), aunque se hace notar que, en esta última, la divergencia entre los expertos fue mayor y llegó incluso a un mínimo de 66,7% en el ítem 13, el cual fue debidamente ajustado para formularlo de manera más explícita.

Tabla 10

Validación de contenido escala PoDeRe: concordancia de jueces y claridad de los ítems

Aspecto	N	Media	Desviación estándar	Mínimo	Máximo
%Concordancia	51	98,039	5,4233	83,3	100,0
%Claridad	51	90,196	10,0976	66,7	100,0

Adicionalmente, la validación de contenido se complementó con el índice de Haynes mediante el análisis de acuerdos y desacuerdos de los expertos, con la división de los acuerdos entre la suma de acuerdos y desacuerdos (Sabogal, Barraza, Hernández y Zapata, 2011). Se obtuvo un índice de Haynes de 0,882 /1,0, lo cual da confianza sobre la estructura de la escala.

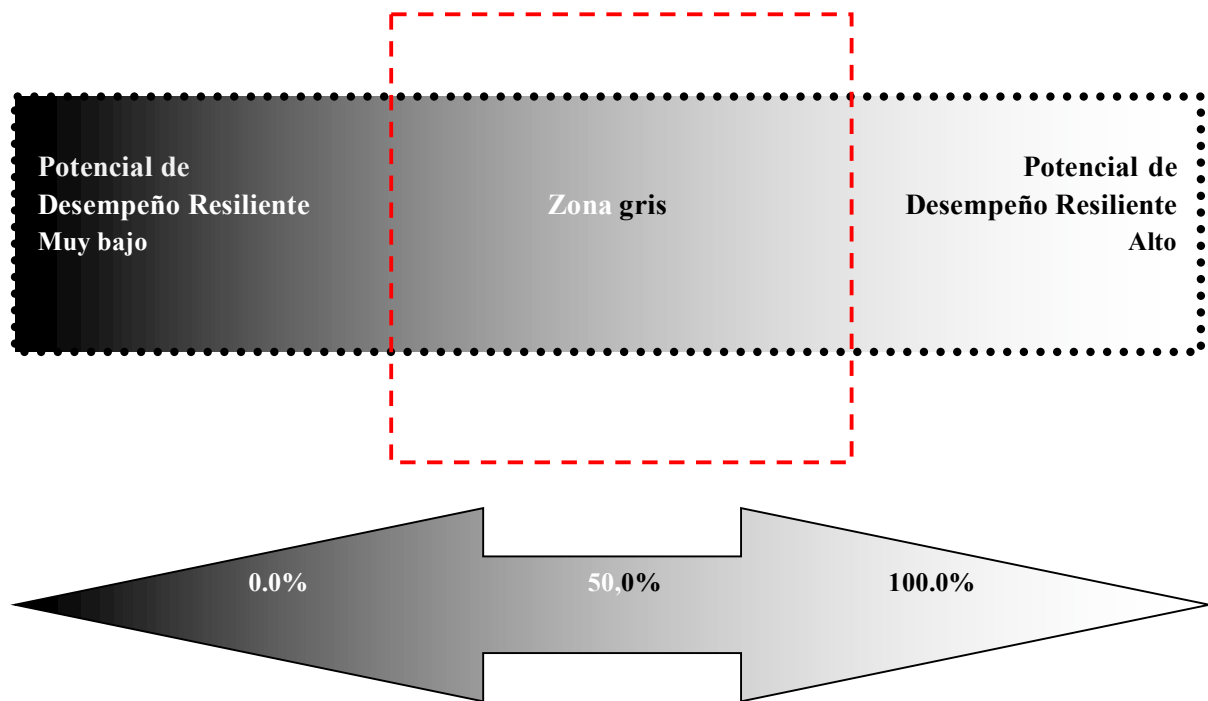
Luego, en conjunto se consideró que el instrumento tenía la requerida validez de contenido escalar.

Así entonces, la estructura del cuestionario quedó conformada por 51 ítems distribuidos en cuatro subdimensiones: capacidad de responder (saber qué hacer), capacidad de monitorear (saber qué buscar), capacidad de aprender (saber qué ha ocurrido) y capacidad de anticipar (saber qué esperar); con ítems tipo Likert de cinco opciones de respuesta, todos ellos de calificación directa positiva, que incluyeron criterios de ocurrencia porcentual para minimizar el sesgo subjetivo "apreciativo" y unificar la percepción de las alternativas de respuesta con un referente externo, como son las posibles frecuencias de ocurrencia, así:

0. No sabe, no conoce; 1. En ningún caso se presenta; 2. Casi nunca, en máximo el 25% de los casos; 3. Parcialmente, aprox. en la mitad de los casos; 4. Casi totalmente, en más del 70% de los casos, y 5. Sí, en todos los casos se presenta.

Se hace notar que la opción "0. No sabe, no conoce" no se consideró dentro de la posibilidad de cálculo de la escala ni tampoco de las subescalas, al entenderse que la respuesta a ello no era indicadora de un potencial de desempeño resiliente de la entidad. Sin embargo, en el capítulo de Resultados se hizo un análisis estadístico específico de los casos que en la calificación directa fuesen cero.

Comportamiento escalar. El potencial de desempeño resiliente valorado con esta escala se asumió como una dimensión continua con ordinalidad en la medición, como se ilustra en la figura 14.



Fuente: Adaptación de la autora.

Figura 14. Esquematización del comportamiento del constructo escalar potencial de desempeño resiliente

Consistente con ello, se hace notar que los valores numéricos dados por los 51 ítems del instrumento no configuran una escala numérica con monotonía intervalar, aun cuando a las calificaciones directas se les aplicó una transformación lineal a puntajes porcentuales como referente operacional dentro del rango numérico derivado de los ítems de las subescalas y la escala total y se comporta como una escala ordinal continua (Jakobsson, y Westergren, 2005), lo cual conforma su dominio conceptual.

Interpretación escalar. Un menor valor directo obtenido en la escala indica menor potencial de desempeño resiliente de la institución y un mayor valor sugiere un mayor nivel en esta variable.

Luego de la calibración a cero de la escala, el cero (0,0%) no necesariamente configura “ausencia de” potencial de desempeño resiliente y el cien (100,0%) tampoco indica un “total de” o máximo nivel de potencial de desempeño resiliente, valores que, aunque numéricamente

son posibles en la escala, no son conceptualmente viables en la realidad operacional de la gestión del riesgo en la institución.

6.7.1.2 Pilotaje. Antes de la aplicación muestral, la escala fue sometida a prueba en fase piloto con una muestra incidental no aleatoria de 34 participantes, en la cual la escala arrojó un nivel de consistencia interna (confiabilidad) en términos del Alpha de Cronbach de 0,956, que se interpretó como de “alta fiabilidad” (Cervantes, 2005) y con ello se procedió a la aplicación a la muestra general de la investigación con los pilotos militares.

6.7.1.3 Fiabilidad. Obtenidos ya los datos finales se re-calculó el nivel de confiabilidad de la escala PoDeRe estimando la consistencia interna con el mismo alpha de Cronbach tanto a las subescalas como a la escala total, según se reporta en la tabla 11.

Tabla 11

Análisis de consistencia interna: Alpha de Cronbach de las subescalas y la escala PoDeRe

Subescala (Dimensión)	# ítems	# de participantes [§]	Alpha de Cronbach	Menor alpha si algún ítem se elimina
Capacidad responder	18*	500	0.956	0,952
Capacidad monitorear	21*	479	0.972	0,970
Capacidad institucional para aprender	6	504	0,833	0,800
Capacidad institucional para anticipar	6	504	0,913	0,889
Escala PoDeRe (Total)	51	439	0,982	0.981

*En esta dimensión se consideraron los escenarios (Operaciones, entrenamiento y supervisión operacional).

[§] El n de cada subescala varía en función de quienes contestaron todos los ítems correspondientes.

La consistencia interna más baja se dio en la “capacidad para aprender” con *alpha* de 0,83 (que, no obstante, es considerado “muy bueno” en este estadístico psicométrico, según el criterio de Murphy y Davishofer [citados por Hogan, 2004] que advierten que un *alpha* de 0,6 es lo mínimamente aceptable, de 0,8 o más es muy bueno y superior a 0,9 es muy elevado), mientras que en la escala total llegó a ser de 0,981, lo que en general indica que el instrumento PoDeRe tiene un nivel de consistencia interna muy alto, lo que hace a la escala

psicométricamente fiable y tiene una alta intercorrelación entre los ítems.

6.7.1.4 Validación. Para analizar la validez de la escala se realizó un análisis factorial de componentes principales aplicando la rotación de maximización de varianza (varimax) con normalización de Kaiser (Hair, et al., 2000) y para la solución factorial final se consideraron solo los coeficientes con carga factorial superiores a 0,4. En la tabla 12 se aprecia la obtención de un KMO óptimo y una prueba de Bartlett significativa, lo cual garantiza que la proporción de varianza común entre las variables (ítems) es “muy bueno” y el modelo presenta un buen nivel de ajuste, indicando que el análisis factorial es adecuado y se valida el resultado obtenido respecto a los constructos valorados en la prueba.

Tabla 12

Estadísticos de validación del análisis factorial de componentes principales de las escalas

Indicador	Escala PoDeRe	Escala SegOp
Medida adecuación del muestreo Kaiser-Meyer-Olkin	0,967	,974
Prueba esfericidad de Bartlett	<i>Chi²:</i> 23281.7	10217,9
	<i>gl:</i> 1275	435
	<i>Sig. p</i> ≤ 0,001	<i>p</i> ≤ 0,001

6.7.2 Escala de seguridad operacional -SegOp-. La escala de seguridad operacional (Anexo D) se desarrolló con base en la estructura conceptual y los contenidos propuestos por Reason (2010).

6.7.2.1 Validación de contenido. La escala de SegOp (Anexo E) también fue debidamente revisada para la respectiva validación de contenido por parte del panel de jueces expertos. En los 30 ítems se encontró un nivel de acuerdo en la validez de contenido (concordancia interevaluadores) de 97,2 % ($\pm 7,7\%$) y en la claridad idiomática (redacción) de 90,0% ($\pm 14,9\%$) (tabla 13), aunque se hace notar que en este último indicador (claridad) la divergencia entre los expertos fue mayor y llegó incluso a un mínimo de 50,0% en los ítems

cinco y ocho, los cuales fue revisados en su construcción gramatical para plantearlos con mayor claridad.

Tabla 13

Validación de contenido escala SegOp: concordancia de jueces y claridad de los ítems

Aspecto	N	Media	Desviación estándar	Mínimo	Máximo
%Pertinencia	30	97,220	7,6872	66,7	100,0
%Claridad	30	89,993	14,9076	50,0	100,0

La validación de contenido también se complementó con el índice de Haynes con la relación en pertinencia entre los acuerdos y el total acuerdos y desacuerdos (Sabogal, et al. 2011), obteniéndose un índice de Haynes de 0,867 /1,0, con lo cual se pudo aceptar como adecuada la estructura escalar y con ello asumir que el instrumento SegOp tiene una buena validez de contenido.

Así, la escala SegOp quedó conformado por 30 ítems que se distribuyen como se había definido en la tabla 9: el componente de seguridad (con las subescalas de compromiso y gestión de información), el componente de gestión de seguridad y operaciones y el componente de cultura de la seguridad (con las subescalas de accesibilidad, legitimidad, adaptabilidad y aprendizaje).

Los 30 ítems tipo Likert se diseñaron de cinco opciones de respuesta en las cuales también se incluyeron criterios de ocurrencia porcentual que igualmente buscaban minimizar el sesgo subjetivo y unificar la percepción de las alternativas de respuesta tomando un referente externo (frecuencias de ocurrencia). Así: “0. No sabe, no conoce; 1. En ningún caso se presenta; 2. Casi nunca, en no más del 25% de los casos; 3. Parcialmente, aprox. en la mitad de los casos; 4. Casi totalmente, en más del 70% de los casos y 5. Sí. en todos los casos se presenta”. Se hace notar que la construcción de los ítems fue orientada a una calificación positiva (directa), excepto uno (ítem 8) cuyo modo de calificación es inverso en la polaridad de la escala.

6.7.2.2 Pilotaje. Esta escala también fue sometida a prueba en la fase piloto con una muestra incidental no aleatoria y participaron voluntariamente 31 pilotos militares, encontrándose que la escala SegOp arrojó un nivel de consistencia interna (confiabilidad) según el Alpha de Cronbach de 0,939, que también se interpretó como de “alta fiabilidad” (Cervantes, 2005) y con ello se dio paso a la fase de aplicación a la muestra general de la investigación.

Se hace notar que para efectos del comportamiento y la interpretación escalar en la escala SegOp se toman como referencia los mismos criterios establecidos para la escala PoDeRe.

6.7.2.3 Fiabilidad de SegOp. Con la muestra final, la confiabilidad de la escala se estimó dando los índices que se e reporta en la tabla 14.

Tabla 14

Análisis de consistencia interna: Alpha de Cronbach de las subescalas y la escala PoDeRe

Subescala (Dimensión)	# ítems	# de Participantes*	Alpha de Cronbach	Menor <i>alpha</i> si algún ítem se elimina
Componente Seguridad	9	486	0.815	0,765
Componente Gestión de seguridad y operación	8	502	0.894	0,873
Componente Cultura de la seguridad	13	452	0,948	0,941
Escala SegOp (Total)	30	431	0,964	0.962

* El n de cada subescala varía en función de los pilotos que contestaron todos los ítems correspondientes.

La consistencia interna más baja se dio en el “componente seguridad” con *alpha* de 0,815 (considerado “muy bueno” según Murphy y Davishofer [citados por Hogan, 2004]), mientras que en la escala total llegó a ser de 0,964, que indica que el instrumento SegOp tiene un nivel de consistencia interna “elevada” que también hace que esta escala sea psicométricamente confiable.

6.7.2.4 Validación. Para la validación de las escala SegOp, el análisis factorial exploratorio de componentes principales aplicando la rotación de maximización de varianza (varimax) con

normalización de Kaiser (Hair, et al., 2000) que ya se reportó en la tabla 12 donde se mostró un KMO óptimo y una prueba de Bartlett significativa ($p < 0.001$), lo que indica que la proporción de varianza común entre los ítems es “muy buena” y el modelo factorial ajusta indicando que es adecuado, con lo que se validan los constructos valorados en la escala.

6.7.3. Cuestionario de caracterización demográfica. En el formato de valoración se incluyó la información sociodemográfica de caracterización que permitió identificar variables de respuesta de identificación y otras categorías como la pertenencia a una unidad operativa, el tiempo de experiencia en la aviación y si ha recibido capacitación en seguridad operacional. Estas variables tenían como propósito permitir la ubicación de los sujetos en la estructura organizacional de la entidad como se previó en la tabla 9 de definición de variables.

6.7.4 Guía para la intervención en grupo focal y la realización de entrevistas. Para la fase cualitativa se utilizó una guía semiestructurada de preguntas de profundización orientadas a la temática según el criterio experto de la investigadora y considerando los resultados de la fase cuantitativa. Se buscó de manera comprensiva identificar las configuraciones organizacionales en torno a la seguridad operacional y al potencial de desempeño resiliente (Anexo G).

6.8 Procedimiento

En la parte empírica de esta investigación aplicada se desarrollaron los siguientes procedimientos.

Fase 1. Contactos institucionales. Dada la condición de “alto valor nacional” de la institución se contactó a oficiales del Alto Mando con el propósito exponer la temática de investigación y los procesos metodológicos con el fin de obtener los debidos permisos para el acceso a la población de pilotos, además de allegar la información para conformar los clúster de incidentalidad.

Se tuvo acceso al registro institucional de los eventos de seguridad operacional en los

periodos de tiempo establecidos en esta investigación, con lo cual se estableció la categorización y segmentación de las bases operativas en clúster según el nivel de incidentalidad (según la ecuación 1 [pág. 109]) para definir la comparabilidad necesaria para someter a prueba la hipótesis 2 del estudio.

Fase 2. Diseño y elaboración de las escalas PoDeRe y SegOp. Se desarrollaron para valorar las variables desempeño resiliente y seguridad operacional junto con las otras variables de interés operacionalizadas en la tabla 9, tomando en consideración la estructura de la rejilla Resilience Analysis Grid propuesta por Hollnagel (2006) y los presupuestos de Reason (2010), respectivamente.

Fase 3. Validación de contenido y apariencia, y pilotaje de las escalas. En esta fase se consultaron como jueces expertos a 2 psicólogas militares con conocimientos del contexto organizacional y de la operación de la institución y 4 pilotos expertos en seguridad operacional y con experiencia en situaciones tácticas y operacionales (Anexo C y Anexo E).

Para el pilotaje, se gestionó con la entidad encargada el vaciamiento de los formatos de la encuesta PoDeRe y SegOp en la herramienta web de comunicación interna para respuesta en línea y generación de la base de datos. Los instrumentos preliminares se remitieron vía intranet a 34 pilotos que voluntariamente aceptaron participar en este proceso. Con base en los resultados descritos, se definió la estructura final de las escalas (Anexo B y Anexo D), cuyos formatos también fueron cargados en la herramienta definida por la institución para su aplicación.

Fase 4. Muestreo y aplicación de las Escalas PoDeRe y SegOp. Mediante proceso de muestreo aleatorio probabilístico se seleccionaron los pilotos (545) a partir de la base de datos interna del personal de la institución durante el segundo semestre del año 2019.

Vía correo electrónico se remitió el consentimiento informado (Anexo H) y los enlaces de los formatos de las escalas PoDeRe y SegOp para respuesta individual en línea y el aplicativo

de software almacenaba las respuestas digitadas. La investigadora previó el ocultamiento de la información de identificación y de cualquier elemento que, a su juicio, permitiese acceder al origen de las respuestas o a su autor para proteger la confidencialidad de la aplicación.

Fase 5. Análisis Cualitativo: Obtenidos los resultados y establecidos los hallazgos de la fase cuantitativa, se procedió a realizar la intervención cualitativa del diseño secuencial explicativo (Hernández et. al 2014), a través de realizar dos grupos focales y entrevistas individuales a cinco participantes con conocimiento y experticia en aviación militar, las cuales fueron grabadas digitalmente (previa autorización expresa) y transcritas a texto, generando datos cualitativos flexibles e inductivos (Mendizábal 2006), buscando “construir una imagen compleja y holística para presentar diversas perspectivas de la realidad según los informantes en su situación natural” (Valsilachis, 2006; pág. 24).

Esta información permitió ampliar sintéticamente la comprensión de la situación institucional y de los resultados obtenidos en el primer momento investigativo de acuerdo con la visión propia de personas en diferentes niveles de la organización.

Fase 6. Recopilación, tabulación y análisis de los resultados obtenidos. Dado que la aplicación se desarrolló en línea vía correo electrónico, luego de dos semanas de estar disponible para respuesta, se cerró la opción de captura y se procedió a la descarga de la base de datos en formato de Microsoft Excel, para su posterior exportación a formato .sav de IBM SPSS Statistic™.

En general, se siguió el procedimiento investigativo que se presenta en la esquematización del proceso de aplicación del estudio ilustrado en la figura 15.

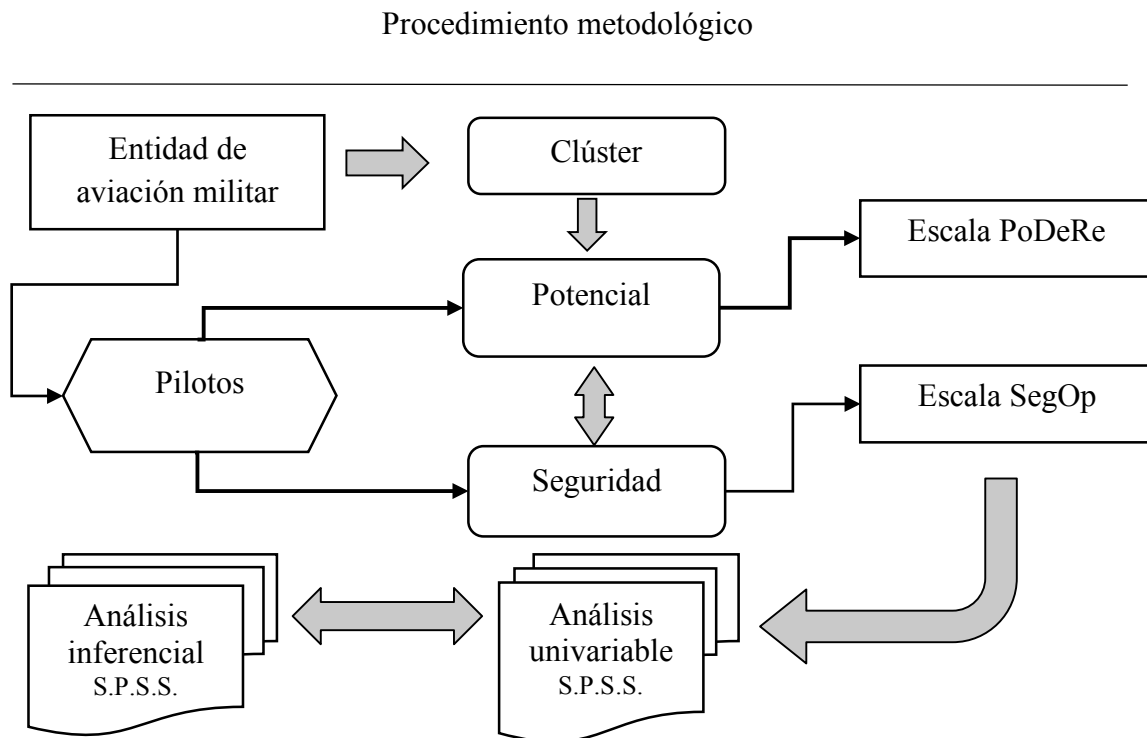


Figura 15. Esquematzación del plan aplicado de la investigación

6.9 Plan de Análisis de los Datos

Una vez obtenidos los archivos de datos originales y realizada su debida concatenación con la variable llave con el programa Excel[®] de Microsoft Office[®] bajo Windows 10.0[®], la base de datos maestra fue exportada al programa de análisis estadístico IBM SPSS Statistic[™] versión 23.0, previa depuración y crítica de datos para detección de inconsistencias y posibles errores en la información o en su digitación y así proceder al respectivo análisis.

6.9.1 Análisis descriptivo univariado. Se realizó un análisis descriptivo univariado construyendo tablas y figuras, elaboradas con los estadísticos de tendencia central y dispersión según el nivel de medición de las variables, de manera que para las variables cuantitativas (puntajes de la escala PoDeRe y de la escala SegOp, así como de sus respectivas subescalas) se calculó la media, la mediana y la desviación estándar, junto con el error estándar de la media; mientras que para las variables cualitativas (vg. grado, clúster, etc.) se obtuvo la distribución porcentual de frecuencias en presentación tipo tablas y/o de gráficas (Daniel, 2002).

6.9.2 Análisis inferencial comparativo. Dado que las variables de respuesta son de tipo numérico ordinal evaluadas con métrica intervalar (Jakobsson, y Westergren, 2005) se analizaron las distribuciones de frecuencias para verificar la normalidad en términos de la distribución probabilística de gauss considerando el estadístico de Levene, tomando un nivel $\alpha \leq 0,05$ como criterio de aceptación/rechazo del supuesto de homocedasticidad de varianzas y de normalidad de la variables, que validan el uso de pruebas paramétricas como criterio de referencia inferencial.

Así entonces, para el análisis inferencial comparativo que permitió poner a prueba las hipótesis de nulidad de diferencias de medias se utilizó el modelo de análisis de varianza de una factor de clasificación de efectos fijos para grupos independientes no relacionados (Daniel, 2002) para someter a prueba las comparaciones intergrupos definidas en función de variables categóricas como tipo de clúster (hipótesis 2), rango jerárquico y nivel de participación en las operaciones (hipótesis 3) y demás variables del ámbito institucional. En las pruebas estadísticas inferenciales realizadas también se tomó como criterio de significancia una $p \leq 0,05$.

Se hace notar además que el *teorema del límite central* indica que a medida que el tamaño de la muestra es mayor (en esta investigación fueron 545 sujetos en el grupo estudiado), la distribución tiende a comportarse de manera aproximadamente normal. De manera que ante un mayor tamaño muestral, el Anova es un modelo “robusto” para los supuestos de normalidad y homogeneidad de varianzas (Hair, Anderson, Tatham & Black, 1999).

De manera complementaria, para las variables numéricas también se construyeron los intervalos del 95% de confianza respecto de la media (Daniel, 2002); lo que permite referentes comparativos entre promedios, de manera que un traslapamiento del recorrido de los intervalos se entendía como indicador de diferencias no significativas, mientras que la no sobreposición indicaba diferencias significativas con ese nivel de confianza asociado (Ferrán, 1996).

De manera accesoria, para estas docimias con el modelo de Anova de una vía se calculó

el tamaño del efecto mediante el estadístico *eta parcial*² (Domínguez-Lara, 2017) que considera la diferencia de medias entre los grupos con el propósito de aportar evidencia acerca de si una significancia estadística ($p \leq 0,05$) corresponde también con una relevancia temática (“relevancia clínica”), ya que las diferencias específicas entre grupos pueden ser estadísticamente significativas, pero no necesariamente ser temáticamente (“clínicamente”) relevantes. De hecho, “el tamaño del efecto es la diferencia más pequeña que el investigador está dispuesto a aceptar como ‘clínicamente’ relevante e indica cuánto de la variable dependiente se puede explicar, predecir o controlar por la variable independiente” (Cárdenas y Arancibia, 2014, p. 213).

Para su interpretación se consideró el criterio de Cohen: 0,01 = pequeño, 0,06 = mediano, 0,13 = grande (Cohen, 1988; Cohen, 1992, Domínguez, 2017). Por demás, el *eta parcial*² es la varianza explicada por una variable dada de la varianza después de excluir la varianza explicada por otros predictores” que en el caso de un solo factor de clasificación está controlado (Domínguez, 2017), de manera que indica cuánto de la variable dependiente es controlado (aunque no indica causalidad) por la variable independiente, luego el valor más alto (aunque decimal) que se puede obtener es 1,0.

Los valores más altos (los más cercanos a 1.0) significan un mayor control. (v.g. un *eta cuadrado* de 0,73 significa que la variable independiente explica el 73% de la variable dependiente) (Domínguez, 2017),

6.9.3 Análisis correlacional. Se realizó un análisis correlacional con el coeficiente de correlación producto-momento de Pearson previa verificación de los supuestos de medición intervalar, tamaño muestral y normalidad para identificar las relaciones significativas entre las variables, en particular con y entre las escalas y subescalas del potencial de desempeño resiliente y de la seguridad operacional (hipótesis 1), con ello seguidamente se construyó la respectiva matriz de correlaciones.

Para efectos del análisis correlacional con la r de Pearson, el tamaño del efecto se deriva del mismo coeficiente de correlación que indica la fuerza de la relación entre dos variables, además de su polaridad. De manera que una r entre 0,10 y 0,30 se suele considerar un tamaño del efecto pequeño. Entre 0,30 y 0,50 se considera un tamaño del efecto medio, y si es mayor que 0,50 un tamaño del efecto grande (Ledesma, Macbeth, y Cortada, 2008).

6.9.4 Modelamiento regresional. Para realizar el modelamiento de predicción multivariable que requiere la hipótesis 4, se utilizó un modelo de regresión múltiple con la técnica step waise forward (Hair, Anderson, Tatham y Black, 2000), en el que se va adicionando por pasos cada variable predictora para potenciar la capacidad predictiva.

Para ello, se indica el panel de predictores y el modelo selecciona las variables de mayor significancia para su inclusión en el modelo predictivo. Luego se van incluyendo progresivamente otros predictores que le siguen a la anterior en capacidad predictiva aumentando la variabilidad explicada por el modelo. La seguridad operacional de la institución fue tratada como la “variable criterio” objeto de predicción. Igualmente, el nivel de significancia para la regresión, así como para los coeficientes de regresión fue $p \leq 0,05$.

6.9.5 Análisis cualitativo. Con el propósito de analizar la evidencia interpretativa (datos flexibles (Mendizábal, 2006) obtenida en grupos focales y entrevistas, cuyos audios fueron grabadas en formato digital y transcritos a formato de texto, se recurrió al software MAXQDA 2020 (Qualitative Data Analysis Software); (Verbi Software, 2019; Rädiker y ori.Kuckartz, 2020) como herramienta para el análisis categorial a posteriori, aunque teniendo en consideración la estructura conceptual de Hollnagel (2015).

En el software (Verbi Software, 2019) se utilizó la rutina de codificación (asignación de códigos a conceptos y pasajes de texto) para identificar categorías inductivas y segmentaciones asociadas, lo cual permitió construir el sistema jerárquico de categorías (ordenamiento escalonado de categorías y subcategorías) para establecer la estructura conceptual que se mapea

en un pictograma que muestra las relaciones e interdependencias de las categorías y sus respectivas capas (subcategorías).

Adicionalmente, como otro producto gráfico descriptivo, se construyó la nube de códigos (Rädiker y Kuckartz, 2020) que proporciona una representación visual de la lingüística discursiva imperante en el análisis apreciativo de los expertos que sintetiza los recursos argumentativos con una visión accesible y fácilmente entendible para legos y expertos, en virtud de las suposiciones e hipótesis planteadas alrededor del tema de estudio.

6.10 Consideraciones Éticas

Para efectos de esta investigación, se entendió que la vinculación al proceso de investigación tanto de la autora y la entidad militar colaboradora, como de las personas participantes se hizo bajo las debidas consideraciones éticas. Así, este estudio de acuerdo con la clasificación de riesgo investigativo para participantes e investigadores que establece el Ministerio de Salud de Colombia, en el artículo 011 de la Resolución 8430 de 1993, se cataloga como una “investigación sin riesgo” (Ministerio de Salud de la República de Colombia, 1993):

Investigación sin riesgo: Estudios que emplean técnicas y métodos de investigación documental retrospectivos y aquellos en los que no se realiza ninguna intervención o modificación intencionada de las variables biológicas, fisiológicas, psicológicas o sociales de los individuos que participan en el estudio, entre los que se consideran: revisión de historias clínicas, entrevistas, cuestionarios y otros en los que no se le identifique ni se traten aspectos sensitivos de su conducta (Resolución 8430 de 1993, artículo 11, literal a.)

Adicionalmente, se asumió el compromiso de la voluntariedad de la participación, la reserva de información e identidad y, además, se preservó la privacidad de los documentos y datos que fueron conocidos durante las actividades investigativas mediante la codificación de las identificaciones y la debida custodia de los documentos y las bases de datos.

A los participantes se les dio a conocer previamente el consentimiento informado (Anexo

G) y se les brindó opciones de terminar y/o abandonar el proceso valorativo si así lo consideraban personalmente, a lo largo de todo el procedimiento.

Dado que los sujetos de interés configuraban una población de alto valor nacional, se previeron las deferencias respectivas para la participación en términos de aceptación / rechazo o retiro del consentimiento informado y la certeza de no tener afectaciones de la situación laboral y/o militar de cada voluntario, así como la garantía de que los resultados fueron debidamente anónimos, reservados y sin contingencia de prejuicio individual o grupal (Resolución 8430 de 1993, art. 46 literales a y b.)

Se tuvieron en cuenta todas las demás consideraciones éticas propias de la investigación con sujeto humano según la ley colombiana y las declaraciones internacionales de bioética y ética investigativa.

Adicionalmente, se contó con el aval académico del programa de Doctorado en Psicología de la Universidad de Palermo (Buenos Aires, Argentina).

Capítulo

7. Resultados

En esta investigación se pretendió examinar la relación que existe entre el potencial de desempeño resiliente y la seguridad operacional en el contexto de una organización de aviación militar colombiana, así como también describir factores organizacionales que puedan estar involucrados en esta relación.

7.1 Caracterización Muestral

En el estudio fueron invitados a participar 548 pilotos militares, de los cuales tres (0,55%) en ejercicio de su derecho personal negaron el consentimiento informado (Anexo G) por lo cual fueron excluidos, quedando finalmente la muestra conformada por 545 oficiales que aceptaron voluntariamente participar dando respuesta a los instrumentos del estudio (Anexos C y E) luego de conocer los objetivos y características puntuales de la investigación.

7.1.1 Aspectos demográficos e institucionales. En términos de la caracterización de la muestra participante en la figura 16 se presenta la distribución según el rango jerárquico en la institución, donde se puede apreciar que sobresale el 52,7% en el rango del primer nivel (1°) que corresponde a la base táctica de la entidad, dándose una relación de 6,4 funcionarios del nivel 1 por cada participante del 3° nivel o de mayor rango jerárquico. En conjunto se refleja la característica piramidal que es usual en las entidades militares. De hecho, conjuntamente los niveles 1°-2° llegan a ser el 91,7% del total de los participantes.

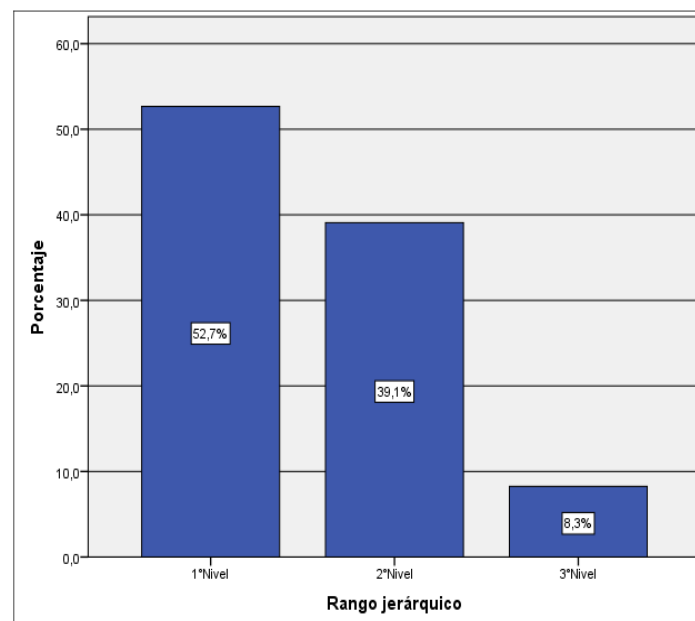


Figura 16. Distribución muestral según el rango jerárquico de los oficiales participantes

Seguidamente, la figura 17 presenta la distribución de los 545 participantes según las unidades organizacionales de la organización a las que se encontraban asignados. Sobresalen las bases 9, 4 y 2 con mayores aportes, que en conjunto llegan al 38,2%, lo cual se explica por el tamaño censal de cada unidad.

Por previsión ética y por requerimiento de seguridad de la entidad, los nombres de las unidades organizacionales se codificaron para preservar la reserva de su ubicación y de su denominación real.

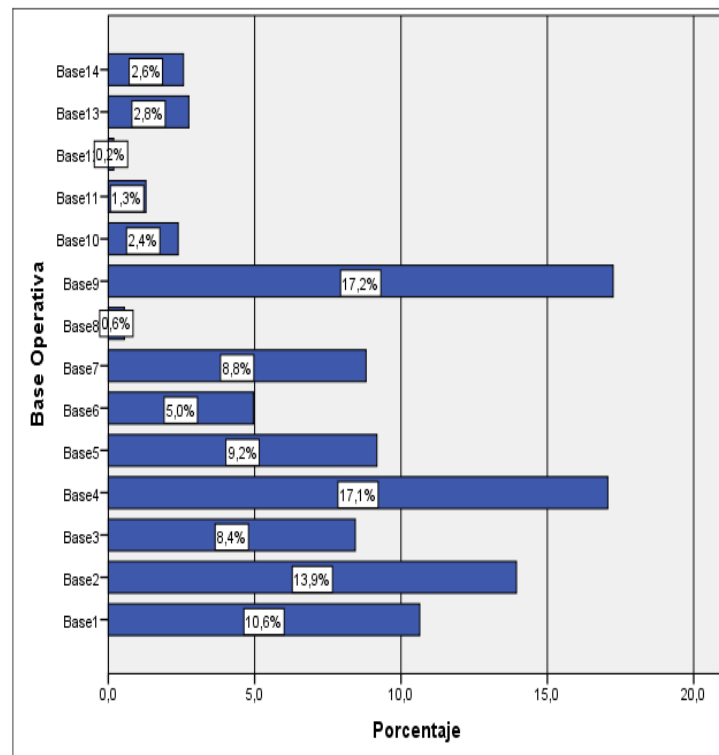


Figura 17. Distribución muestral de las unidades organizacionales de procedencia

Así mismo, se encontró que en el tiempo de desempeño (figura 18) en la especialidad de vuelo, sobresalen los oficiales con menos de 10,0 años de experiencia que en conjunto llegan a ser el 67,0%. Solo el 6,4% superan los 20 años de experiencia. Esto se explica también por la estructura piramidal de la organización.

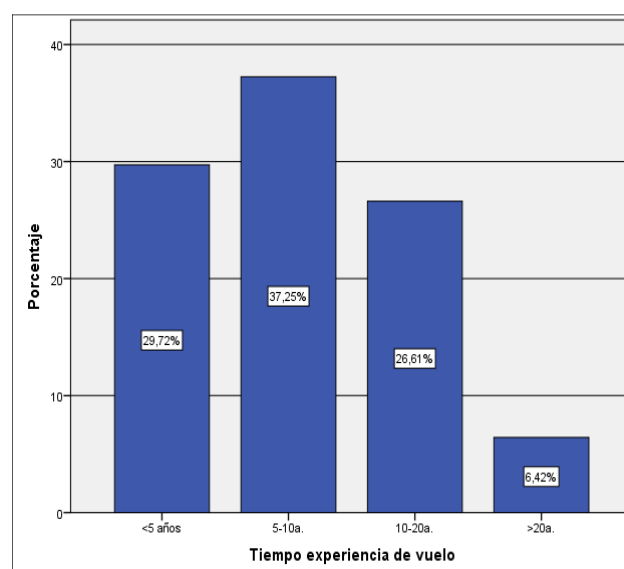


Figura 18. Distribución muestral según el tiempo de experiencia de vuelo

Del total de la muestra, se encontró que el 26,2% reportaron ser oficiales de seguridad operacional como se ve en la figura 19.

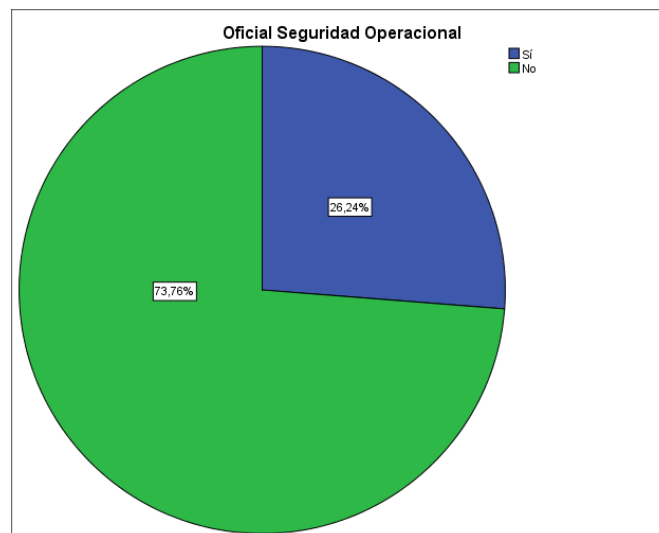


Figura 19. Distribución muestral de la experticia en seguridad operacional

De ese total de participantes, que corresponde al 26,2%, el 75,2% indicó haber ejercido durante menos de 5 años, cargos de seguridad operacional (figura 20) dentro de la estructura de la institución.

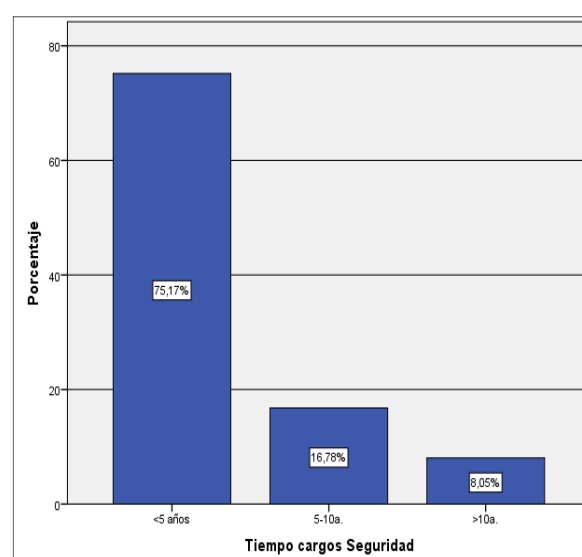


Figura 20. Distribución muestral según el tiempo de experiencia en cargos de seguridad

7.2 Definición de Clúster: Niveles de Incidentalidad Aérea

Para efectos de probar la hipótesis 2 de diferencias entre clúster de muestras homogéneas en el nivel de ocurrencia de la incidentalidad se obtuvo de la entidad la base de datos del reporte de los eventos ocurridos entre 2015-2017, con la cual se calculó la relación que se presenta en la ecuación 1.

$$\text{Incidentalidad} = \frac{\# \text{ horas de vuelo}}{\text{Incidente}}$$

Sí... Incidentalidad ≥ 200 = Clúster de baja

Incidentalidad $> 140 - \leq 200$ = Clúster de media

Incidentalidad > 140 = Clúster de alta

Ec. 1.

Con base en ello y para el marco de esta investigación, las unidades organizacionales se agruparon en clúster de muestras homogéneas tomando un criterio de nivel relativo de incidentalidad, arrojando la distribución que se presenta en la tabla 15, donde se diferencian clúster de alta, intermedia y bajos niveles de incidentalidad relativa según las horas de vuelo por incidente.

Tabla 15

Ordenamiento de las unidades según horas de vuelo / incidente para la conformación de clúster de incidentalidad

Clúster	Base	Horas vuelo/evento	%	Base	Clúster	Horas vuelo/evento	%
Alta	Base1	11,0	0,4	Base9	Media	172,7	6,8
Alta	Base2	29,1	1,1	Base10	Media	180,8	7,1
Alta	Base3	123,3	4,8	Base11	Media	190,5	7,5
Alta	Base4	132,5	5,2	Base12	Media	196,0	7,7
Alta	Base5	134,2	5,3	Base13	Baja	210,7	8,2
Media	Base6	145,2	5,7	Base14	Baja	264,4	10,4
Media	Base7	146,8	5,7	Base15	Baja	465,0	18,2
Media	Base8	152,1	6,0				

De hecho, si se consideran los valores extremos dados en la tabla 15 se podría afirmar que mientras en la unidad quince del clúster de baja incidentalidad ocurrió un incidente cada 465 horas sumativas de vuelo, en la unidad uno del clúster de alta incidentalidad se registró un incidente cada 11 horas sumativas de vuelo, aunque es claro que las distintas tipologías de incidentes no siempre compromete gravemente a equipos ni tampoco a personas y está estrechamente relacionada con el tamaño de la unidad, los equipos asignados y la misión (exposición al riesgo). Esta construcción de clúster bien diferenciados permitió hacer comparaciones válidas para poner a prueba la hipótesis de diferencias (hipótesis 2).

Al respecto, la muestra de participantes diferenciados por la correspondencia a clúster de incidentalidad dio la distribución que se presenta en la figura 21, donde se puede apreciar que mientras al clúster de mayor incidentalidad corresponden el 33,6% de los pilotos participantes, al de menor incidentalidad pertenece el 20,7% de la muestra.

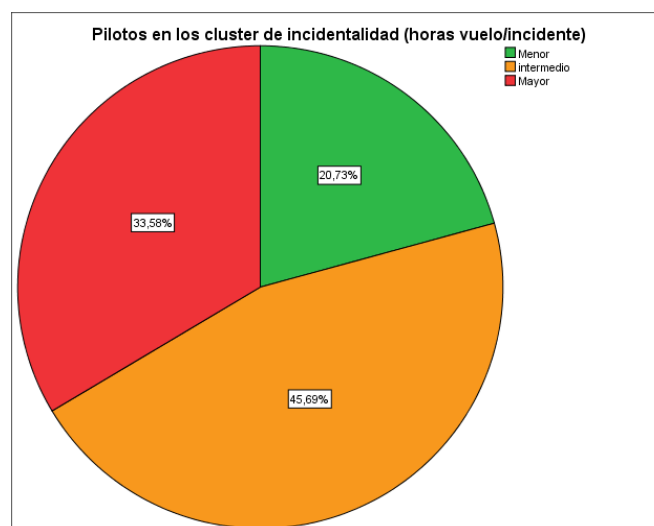


Figura 21. Distribución de la muestra de pilotos en clúster de incidentalidad

7.3 Potencial de Desempeño Resiliente: Comportamiento Muestral

Seguidamente se describen los resultados en la escala PoDeRe con el fin de caracterizar el nivel de potencial de desempeño resiliente en la organización de aviación militar colombiana.

En el anexo I se presentan las distribuciones proporcionales directas de las respuestas originales dadas a todos los ítems de la escala de potencial de desempeño resiliente.

7.3.1 Previsión sobre el comportamiento escalar. Con base en lo anterior, se hace notar que al analizar las respuestas originales de los ítems (Anexo I) se detectó un porcentaje de respuestas en la categoría “no sabe” que osciló entre 0.9% (5 pilotos) en el ítem 19 y 8,4% (46) en el ítem 8 que plantea: “La persona responsable de los indicadores verifica y/o revisa esta lista regularmente” (en el escenario de entrenamiento de personal operativo y en el escenario de supervisión de procesos operativos).

Luego, se optó por realizar un análisis de la frecuencia de repuestas en la categoría “0” (“no sabe”), obteniendo las distribuciones que se presentan en la tabla 16 y la Figura 22.

Tabla 16

Frecuencia de respuesta en la categoría “No sabe” de las escalas

Aspecto	Ninguno		1-5		6 o más		Total
	n	%	n	%	n	%	n
# 0 (No sabe) PoDeRe	439	80,6%	66	12,1%	40	7,3%	545
# 0 (No sabe) SegOp	431	79,1%	92	16,9%	22	4,0%	545

Se encontró que en la escala PoDeRe el 80,6% de los pilotos dieron respuesta completa a los ítems de la prueba e incluso 40 (7,3%) dejaron 6 o más preguntas contestadas como “no sabe, no conoce”, lo cual podría estar reflejando una actitud de reserva de los sujetos o un no comprometerse con las opciones de respuesta, aunque también podría indicar un margen de desconocimiento de condiciones operacionales que, por su cargo, deberían conocer.

Se hace notar que para evitar un efecto no deseado en la valoración del nivel de resiliencia para los cálculos de los puntajes parciales y totales de las subescalas y las escalas se previó su no inclusión al codificarlos como valores perdidos (missing value) sin efecto de cuantificación.

Seguidamente se describe la tendencia muestral del potencial de desempeño resiliente y luego se pasa a presentar las debidas desagregaciones según los aspectos categóricos

institucionales.

7.3.2 Descripción del nivel de potencial de desempeño resiliente. Con base en las respuestas originales se obtuvieron las estadísticas para las subescalas capacidad de respuesta, capacidad de monitoreo, capacidad de aprender y capacidad de anticipar que conforman el nivel del potencial de desempeño resiliente (tabla 17), según el diseño de la escala (Anexo B), lo que permite mostrar el perfil de desempeño resiliente que se observa en la figura 22).

Tabla 17

Estadísticas de la escala y subescalas de potencial de desempeño resiliente PoDeRe en la entidad militar

	N	Media	Mediana	Desviación		
				estándar	Mínimo	Máximo
Capacidad Rpta Esc1	541	71,271	75,000	17,5120	,0	100,0
Capacidad Rpta Esc2	541	71,178	75,000	17,9450	,0	100,0
Capacidad Rpta Esc3	541	70,407	70,833	18,3890	,0	100,0
Capacidad Respuesta	541	70,952	72,222	17,4220	,0	100,0
Capacidad Monitoreo Esc1	541	72,879	75,000	18,7704	,0	100,0
Capacidad Monitoreo Esc2	540	70,584	71,429	18,6819	,0	100,0
Capacidad Monitoreo Esc3	540	72,306	75,000	19,0911	,0	100,0
Capacidad Monitorear	542	71,702	73,810	18,8931	,0	100,0
Capacidad Aprender	543	68,970	70,833	17,8008	4,2	100,0
Capacidad Anticipar	542	65,314	70,833	21,0026	,0	100,0
Potencial Desempeño Resiliente	543	70,414	72,059	16,7155	7,4	100,0

En conjunto, respecto al total del potencial de desempeño resiliente (tabla 17) se encontró, en un rango máximo posible de 100, que el promedio general fue de $70,4 \pm 16,7$, variando desde una capacidad resiliente mínima de 7,4 hasta una máxima de 100,0 puntos porcentuales, lo que permite afirmar que globalmente la institución de aviación militar tiene un nivel de desempeño resiliente calificable como medio bajo.

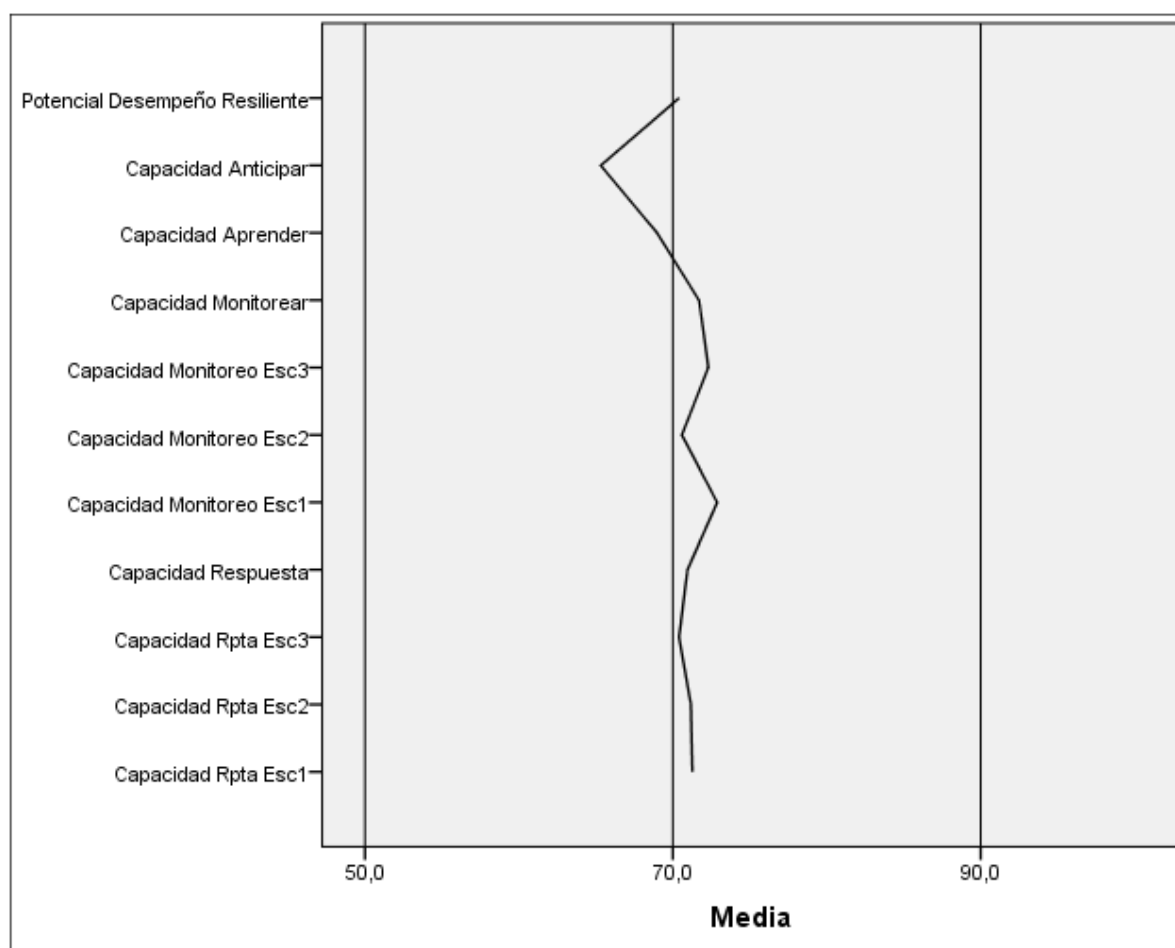


Figura 22. Perfil de desempeño resiliente de la entidad

Respecto a las subescalas, en promedio la que presentó un menor puntaje fue la capacidad de anticipar con un $65,3 \pm 21,0$ mientras la que puntuó más alto fue la capacidad de monitoreo, específicamente en el escenario de ejecución de operaciones (mantenimiento, vuelo y entrenamiento) con $72,9 \pm 18,8$.

Seguidamente, en la tabla 18, con base en los valores dimensionales de la escala se categorizaron las distribuciones muestrales de los puntajes porcentuales de manera que un puntaje abajo del 70 se consideró bajo, de 70 o 85 medio y más de 85 de alta capacidad resiliente (según se definió en la operacionalización de variables que se estableció en la tabla 9, página 84), que correspondería a un criterio cualitativo de potencial de desempeño resiliente de la organización.

Tabla 18

Categorías de escala y subescalas del potencial de desempeño resiliente en la entidad militar

Sub escala	Baja		Media		Alta		Total
	N	%	N	%	N	%	N
Capacidad Responder Esc1	221	40,9	205	37,9	115	21,3	541
Capacidad Responder Esc2	207	38,3	210	38,8	124	22,9	541
Capacidad Responder Esc3	223	41,2	205	37,9	113	20,9	541
Capacidad de Responder	234	43,3	192	35,5	115	21,3	541
Capacidad Monitorear Esc1	206	38,1	184	34,0	151	27,9	541
Capacidad Monitorear Esc2	225	41,7	183	33,9	132	24,4	540
Capacidad Monitorear Esc3	210	38,9	181	33,5	149	27,6	540
Capacidad de Monitorear	229	42,3	180	33,2	133	24,5	542
Capacidad institucional de Aprender	250	46,0	205	37,8	88	16,2	543
Capacidad institucional de Anticipar	270	49,8	193	35,6	79	14,6	542
Potencial Desempeño Resiliente	241	44,4	201	37,0	101	18,6	543

Se puede observar que en la escala total sobresale un bajo potencial de desempeño resiliente con un 44,4%. En términos de las subescalas sobresalen las capacidades de anticipar, aprender y responder como aquellas con mayor afectación y por ende con el más bajo potencial de desempeño resiliente de la entidad (figura 23). Solo el 18,6% de la muestra considera que el potencial de desempeño resiliente está en un alto nivel.

En cuanto a la capacidad de monitorear, es la subescala con mejor consideración de alto potencial resiliente en los tres escenarios contemplados, mostrando resultados que sobresalen en relación con las otras subescalas de la prueba, aunque los niveles proporcionales apreciados en cada dimensión no lograron superar las categorías de media y baja capacidad.

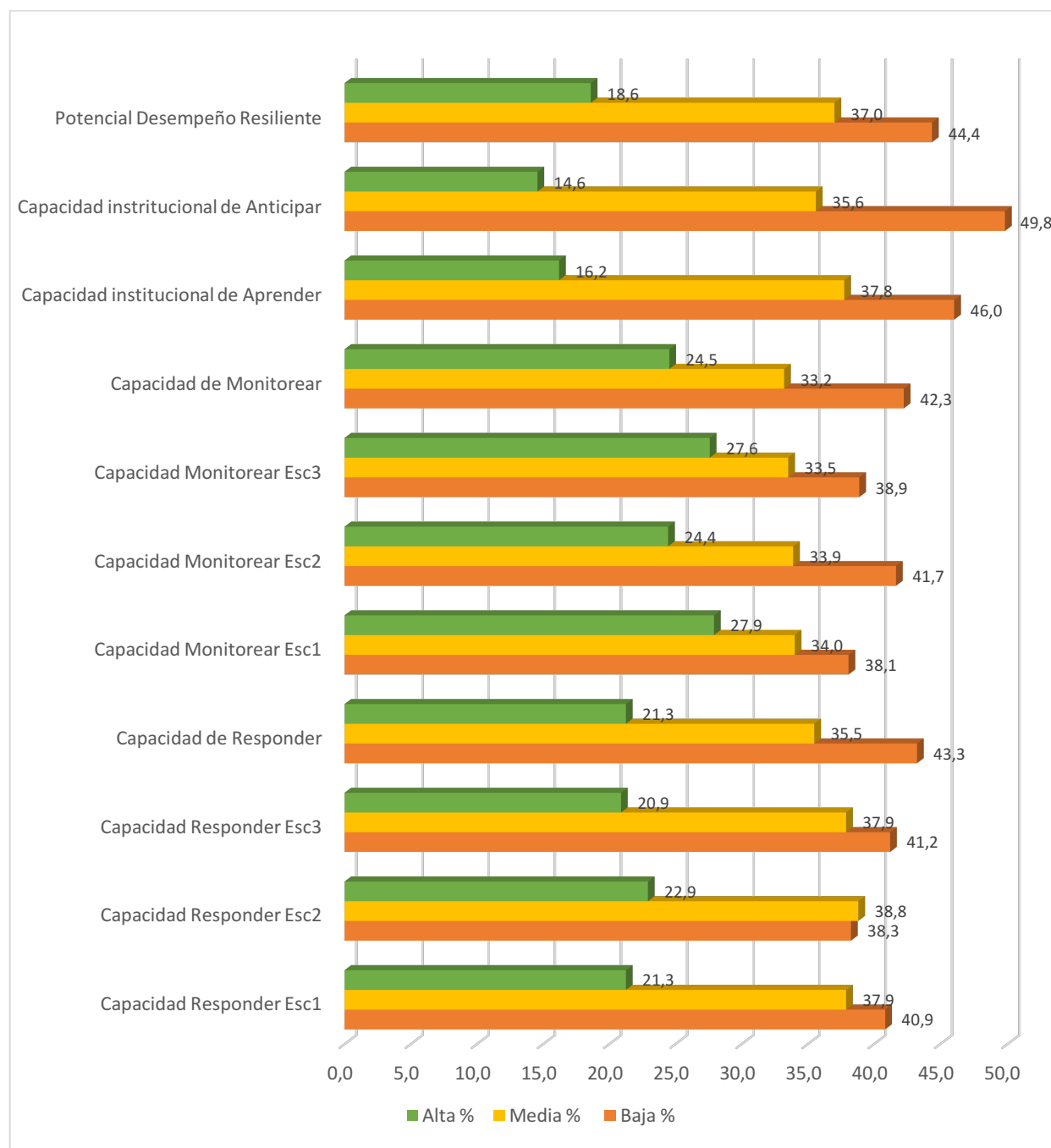


Figura 23. Categorías de escala y subescalas del potencial de desempeño resiliente de la entidad

La figura 23 permitió observar la alta agrupación de respuesta en la categoría de baja, en contraposición a la cantidad de respuestas que se encuentran en categoría alta. Esto evidencia la necesidad de la organización de trabajar en su potencial de desempeño resiliente de manera sistemática, holística y armónica.

7.4 Seguridad Operacional: Comportamiento Muestral

Pasando ahora a la descripción muestral del nivel de seguridad operacional según el concepto de los participantes, en el Anexo I se presentan las distribuciones proporcionales de las respuestas originales dadas a todos los ítems clasificados según los componentes y sus respectivas subescalas. Seguidamente se describe la tendencia muestral de la organización, para luego presentar también la desagregación muestral según los aspectos categóricos institucionales.

7.4.1 Previsión sobre el comportamiento escalar SegOp. De igual manera que la escala anterior, se encontró en las respuestas de los ítems (Anexo J), un porcentaje de respuestas en la categoría de “no sabe” ya mostradas en la tabla 17, que osciló entre 0.4% (2 pilotos) en el ítem 15 y 6,1% (33 pilotos) en el ítem 20 (“La dependencia que recopila y analiza los informes tiene autonomía respecto de aquella que determina las acciones correctivas o sanciones”).

En la escala SegOp, el 79,1% respondieron completamente los ítems e incluso 22 pilotos (4,0%) dejaron 6 o más preguntas como “no sabe, no conoce”. También podrían reflejar una actitud inhibitoria de los pilotos o una inclinación a no comprometerse con la respuesta. En esta escala sería más severo si llegare a ser desconocimiento de las condiciones de la seguridad operacional.

Igualmente, en la seguridad operacional no se incluyeron los “no sabe, no conoce” en el cálculo de los puntajes parciales y totales, siendo codificados como valores perdidos (missing value) sin cuantificación.

Seguidamente se describe la tendencia muestral de la seguridad operacional de la organización para luego presentar también la desagregación muestral según los aspectos categóricos institucionales.

7.4.2 Descripción del nivel de seguridad operacional: Escala SegOp. Se obtuvieron las estadísticas de los componentes de seguridad, gestión de la seguridad y las operaciones y

cultura de la seguridad que conforman el nivel de seguridad operacional (tabla 19), según el diseño de la escala (Anexo D) que a su vez permite mostrar el perfil de seguridad operacional que se observa en la figura 24.

Tabla 19

Estadísticas de la escala de seguridad operacional SegOp y sus componentes

Subescala	Desviación					
	N	Media	Mediana	estándar	Mínimo	Máximo
Compromiso	541	72,173	75,000	18,7097	6,3	100,0
Gestión Información	542	61,246	65,000	13,7018	8,3	100,0
Componentes Seguridad	542	66,097	66,667	14,9291	4,2	91,7
Comp. Gestión seg. y oper.	542	71,506	75,000	17,1506	3,1	100,0
Accesibilidad	540	62,997	65,000	21,3686	5,0	100,0
Legitimidad	536	71,121	75,000	19,7995	8,3	100,0
Adaptabilidad	538	70,950	75,000	18,8414	6,3	100,0
Aprendizaje	531	74,576	75,000	19,2687	25,0	100,0
Cultura de la Seguridad	541	68,077	70,833	18,2166	2,8	100,0
Seguridad Operacional	543	68,223	70,833	16,3245	2,6	96,7

Así, respecto al nivel de seguridad operacional (tabla 19) se encontró que el promedio general fue de $68,2 \pm 16,3$, variando desde una seguridad operacional mínima de 2,6 hasta una alta de 74,6 puntos porcentuales, lo que permite afirmar que la organización tiene en promedio una seguridad operacional calificable como medio bajo.

Respecto a los componentes de la seguridad operacional, por su parte, en promedio el que presentó un menor puntaje fue el de gestión de información con un $61,2 \pm 13,7$ mientras que el componente que puntuó más alto fue el de aprendizaje que en promedio fue de 74,6 con una variación de 19,3 puntos porcentuales.

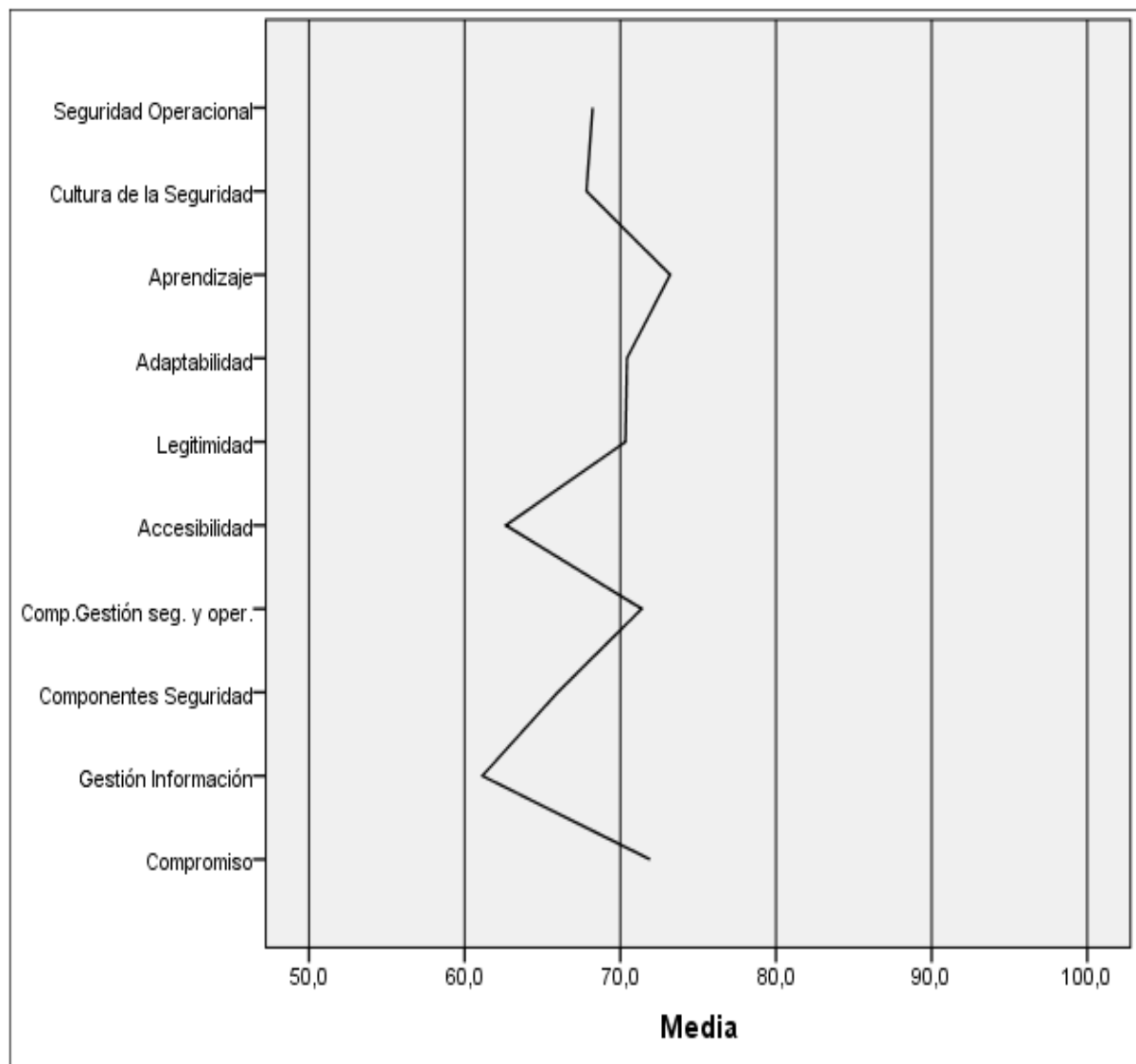


Figura 24. Perfil de componentes de la seguridad operacional

Seguidamente, en la tabla 20 con base en los valores dimensionales de la escala SegOp de manera que un puntaje abajo del 70 se consideró baja, de 70 o 85 media y más de 85 de alta seguridad operacional (según también se definió en la operacionalización de variables de la tabla 9), que correspondería a un criterio cualitativo de la seguridad operacional en entidad militar según el concepto con que los pilotos calificaron el contexto operacional, que se puede ver gráficamente en la figura 25.

Tabla 20

Categorías de escala y subescalas de seguridad operacional en la entidad militar

Subescala	Baja		Media		Alta		Total N
	N	%	N	%	N	%	
Compromiso	223	41,1%	181	33,3%	139	25,6%	543
Gestión Información	431	79,4%	103	19,0%	9	1,7%	543
Componentes Seguridad	354	65,2%	123	22,7%	66	12,2%	543
Comp. Gestión seg. y oper.	217	40,0%	220	40,5%	106	19,5%	543
Accesibilidad	343	63,2%	128	23,6%	72	13,3%	543
Legitimidad	227	41,9%	200	36,9%	115	21,2%	542
Adaptabilidad	242	44,6%	180	33,2%	120	22,1%	542
Aprendizaje	136	25,1%	270	49,9%	135	25,0%	541
Cultura de la Seguridad	271	49,9%	187	34,4%	85	15,7%	543
Seguridad Operacional	267	49,2%	198	36,5%	78	14,4%	543

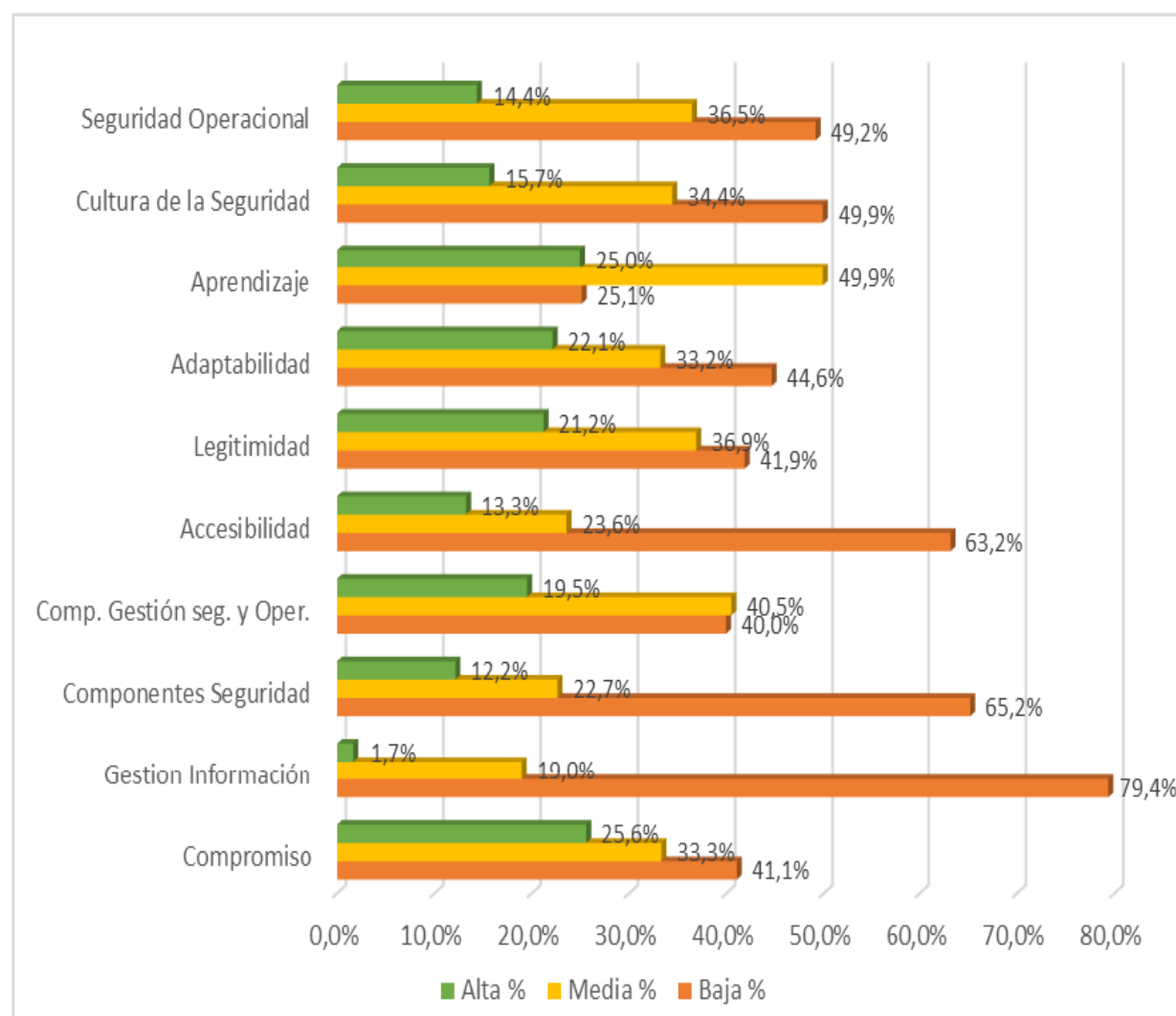


Figura 25. Categorías de subescalas y escala de seguridad operacional en la entidad

Se puede apreciar que en la escala total sobresale proporcionalmente un nivel de seguridad operacional bajo con un 49,2%, indicando que el sistema presenta, en general, un bajo nivel de seguridad operacional.

El componente de seguridad dentro de la escala fue el que puntuó más bajo (65,2%), seguido del componente de cultura de seguridad (49,9%). Los subcomponentes de gestión de información (79,4%) y accesibilidad (63,2%) que presentaron la mayor afectación, podrían servir para optimizar la previsión de seguridad operacional. Solo el 14,4% de la muestra consideró la seguridad operacional total en un alto nivel.

Se hace notar que las mayores consideraciones de alta seguridad operacional se dieron en los subcomponentes de compromiso, aprendizaje y adaptabilidad donde se pudo apreciar la mayor respuesta de seguridad de la entidad, sobresaliendo sobre los otros componentes de la escala, aunque los niveles proporcionales apreciados en estas subescalas tampoco lograron superar las categorías de media y alta seguridad operacional.

En seguida se presentan los análisis relacionados con los puntajes en las escalas de resiliencia y seguridad diferenciados con base en clúster de incidentalidad establecidos con ese fin.

7.5 Análisis Diferencial en Función de Clúster de Incidentalidad

Para efecto de los análisis diferenciales tanto del potencial de desempeño resiliente como de la seguridad operacional, previamente se valoró la normalidad de los datos muestrales, donde se hipotetiza su distribución aleatoria y se probó la homogeneidad de varianzas (homocedasticidad) con la prueba de Levene (Ferrán, 1996), arrojando los estadísticos que se presentan en la tabla 21, donde se aprecia que efectivamente las variables de respuesta, potencial de desempeño resiliente y seguridad operacional presentan distribuciones de muestreo con las debidas homogeneidades de las varianzas al no llegar a rechazar la hipótesis

nula respectiva con $p > 0,05$, lo cual valida el uso de la pruebas paramétricas (Daniel, 2002).

Tabla 21

Distribución y prueba de homogeneidad de varianza de las variables de medida

Variables	Media	Intervalo de confianza 95%		Desviación estándar	Coeficiente Asimetría	Estadístico de Levene	<i>p</i>
		Límite inferior	Límite superior				
Potencial Desempeño Resiliente	70,414	69,005	71,823	16,7155	-0,553	0,750	,473 _{NS}
Seguridad Operacional	68,223	66,847	69,599	16,3245	-0,634	0,376	,687 _{NS}

^{ns} $P > 0,05$. No significativa

Así entonces, se procedió a desarrollar los análisis diferenciales previstos en las hipótesis investigativas y, como previamente se había describió, la muestra de pilotos participantes se diferenció entre clúster de alta (mayor), intermedia y baja (menor) incidentalidad relativa según las horas de vuelo/incidente en las bases operacionales a las que se encuentra asignado cada piloto, para efectos de someter a prueba estadística la hipótesis 2 que pronosticaba diferencias significativas en el desempeño resiliente y la seguridad operacional entre los clústeres.

7.5.1 Potencial de desempeño resiliente según clúster de incidentalidad. Para el efecto, la tabla 22 muestra los promedios e intervalos de confianza de las subescalas y la escala PoDeRe diferenciados según clúster de incidentalidad en que se clasificó la muestra de pilotos participantes, hallazgos que además se ilustran en la figura 26 y la figura 27 y se someten a prueba estadística en la tabla 23 con la prueba de Anova de una vía y los respectivos valores de *p* y del tamaño de efecto según el *eta parcial*² que estima la proporción de desempeño resiliente que se podría atribuir al factor independiente clúster de incidentalidad.

Tabla 22

Promedios de la escala PoDeRe diferenciados según clúster de incidentalidad

Subescalas	Clúster	N	Media	Desviación estándar	95% del intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Capacidad	Menor	113	72,3	14,9	69,5	75,0	29,2	100,0
Rpta Esc1	intermedio	248	69,6	17,8	67,4	71,9	8,3	100,0
	Mayor	180	72,9	18,5	70,2	75,6	,0	100,0
Capacidad	Menor	113	72,0	14,8	69,2	74,8	25,0	100,0
Rpta Esc2	intermedio	248	69,2	18,7	66,9	71,5	4,2	100,0
	Mayor	180	73,4	18,5	70,7	76,1	,0	100,0
Capacidad	Menor	113	71,3	15,2	68,4	74,1	20,8	100,0
Rpta Esc3	intermedio	248	68,5	18,6	66,2	70,8	,0	100,0
	Mayor	180	72,5	19,7	69,6	75,4	,0	100,0
Capacidad	Menor	113	71,8	14,5	69,1	74,6	25,0	100,0
Respuesta	intermedio	248	69,1	17,8	66,9	71,3	6,1	100,0
	Mayor	180	72,9	18,4	70,2	75,6	,0	100,0
Capacidad	Menor	113	74,4	17,3	71,1	77,6	21,4	100,0
Monitoreo	intermedio	247	70,8	19,3	68,4	73,3	,0	100,0
Esc1	Mayor	181	74,7	18,7	72,0	77,5	17,9	100,0
Capacidad	Menor	113	71,6	17,9	68,3	74,9	17,9	100,0
Monitoreo	intermedio	246	68,3	18,8	65,9	70,7	,0	100,0
Esc2	Mayor	181	73,1	18,8	70,3	75,8	10,7	100,0
Capacidad	Menor	113	74,6	17,5	71,3	77,9	25,0	100,0
Monitoreo	intermedio	246	69,8	19,3	67,3	72,2	,0	100,0
Esc3	Mayor	181	74,3	19,4	71,5	77,2	,0	100,0
Capacidad	Menor	113	73,5	17,3	70,3	76,7	21,4	100,0
Monitorear	intermedio	248	69,2	19,5	66,7	71,6	,0	100,0
	Mayor	181	74,0	18,6	71,3	76,8	15,5	100,0
Capacidad	Menor	113	69,0	18,1	65,6	72,4	16,7	100,0
Aprender	intermedio	249	67,7	17,1	65,5	69,8	4,2	100,0
	Mayor	181	70,7	18,4	68,0	73,4	12,5	100,0
Capacidad	Menor	113	64,7	22,1	60,6	68,9	,0	100,0
Anticipar	intermedio	248	64,3	20,3	61,8	66,9	,0	100,0
	Mayor	181	67,0	21,2	63,9	70,2	8,3	100,0
Potencial	Menor	113	71,4	15,6	68,5	74,3	28,6	99,5
Desempeño	intermedio	249	68,5	16,6	66,4	70,6	7,4	100,0
Resiliente	Mayor	181	72,5	17,4	69,9	75,0	18,6	100,0

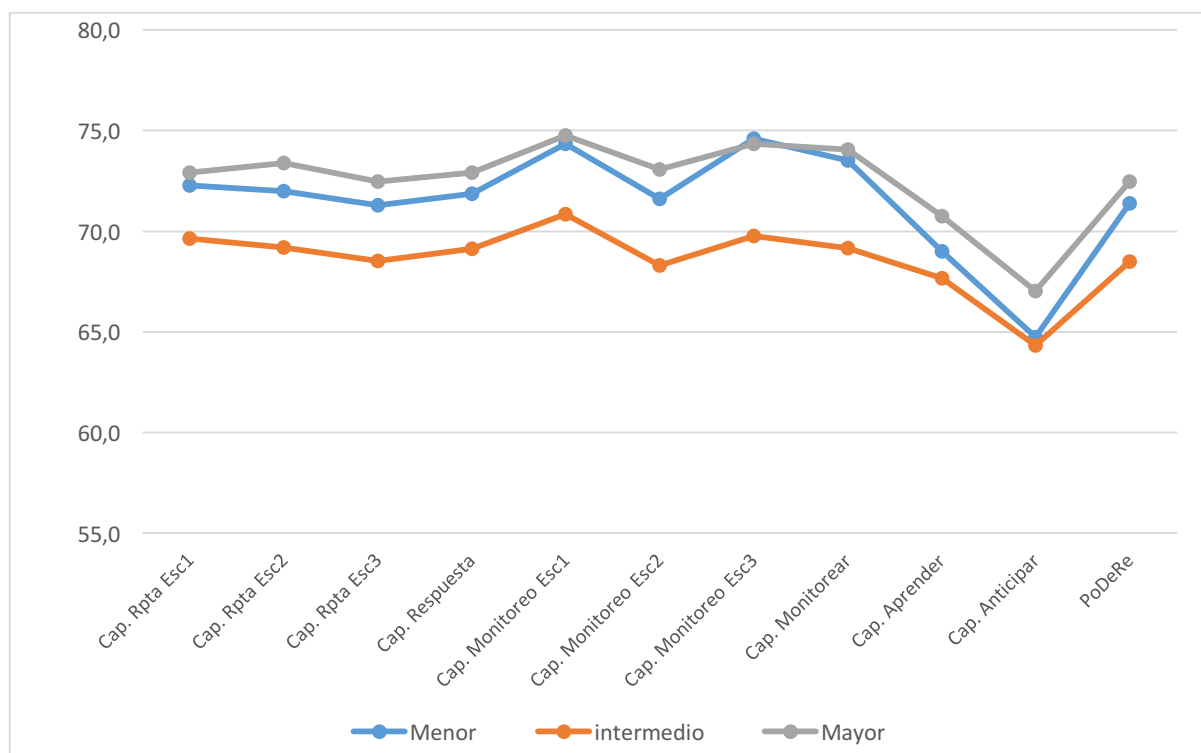


Figura 26. Subescalas de la escala PoDeRe según clúster de incidentalidad

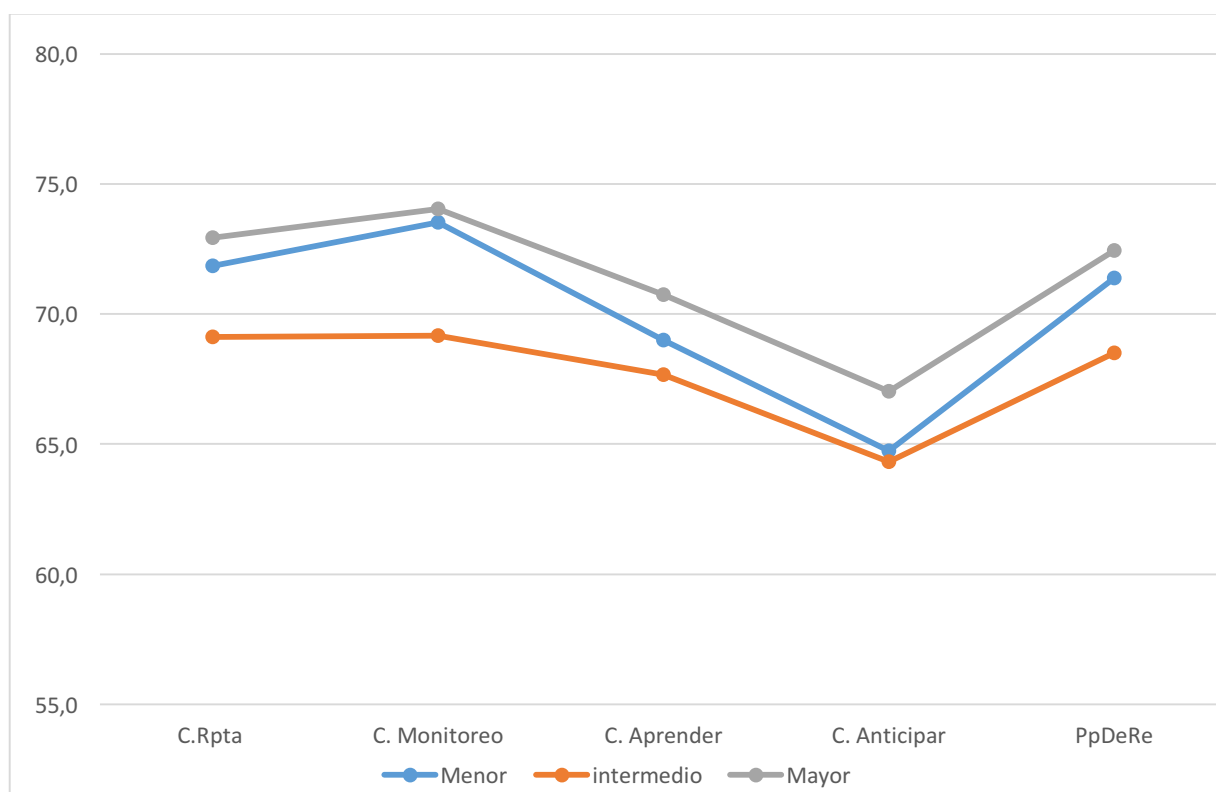


Figura 27. Promedios de las subescalas de la escala PoDeRe según clúster de incidentalidad

Tabla 23

Pruebas de Anova para los promedios de la escala PoDeRe según clúster de incidentalidad y los respectivos tamaños del efecto

Variables de respuesta	<i>F</i>	Sig.	Tamaño del efecto [§] (<i>Eta parcial</i> ²)
Capacidad Rpta Esc1	2,067	,128	,008
Capacidad Rpta Esc2	3,033	,049*	,011 [⊗]
Capacidad Rpta Esc3	2,589	,076	,010 [⊗]
Capacidad Respuesta	2,703	,068	,010 [⊗]
Capacidad Monitoreo Esc1	2,716	,067	,010 [⊗]
Capacidad Monitoreo Esc2	3,639	,027*	,013 [⊗]
Capacidad Monitoreo Esc3	4,097	,017*	,015 [⊗]
Capacidad Monitorear	4,208	,015*	,015 [⊗]
Capacidad Aprender	1,551	,213	,006
Capacidad Anticipar	,930	,395	,003
Potencial Desempeño Resiliente	3,200	,042*	,012 [⊗]

* $p < 0,05$; ** $p < 0,01$.

[§]Nota: *Eta parcial*²: [⊗]pequeño=0.01; ^{⊗⊗}mediano=0.06; ^{⊗⊗⊗}grande=0.13 (Domínguez-Lara, 2017).

Se puede apreciar que los promedios de las capacidades del potencial de desempeño resiliente se ubican alrededor del puntaje 70 que correspondería a un nivel medio dentro del dominio escalar, lo cual indicaría la existencia moderada de recursos instrumentales y actitudinales de la entidad para enfrentarse a contingencias fortuitas de la actividad operacional. Sobresale que la capacidad de monitoreo, en particular en los escenarios tres (supervisión de procesos operativos) y uno (ejecución de operaciones) mostraron puntajes que repuntan, seguidos de la capacidad de aprendizaje.

Los promedios más bajos se observaron consistentemente en la capacidad de anticipación (tanto previsibles como fortuitos) que estuvieron alrededor de 64,0 puntos porcentuales, siendo la dimensión de resiliencia con menor capacidad en los tres clúster.

La pruebas inferenciales con los Anova de la tabla 23 mostraron que las diferencias del potencial de desempeño resiliente entre los clúster de incidentalidad se hicieron significativas con $p < 0,05$ en las subescalas de capacidad de responder (escenario 2: entrenamiento de personal operativo), capacidad de monitoreo (escenario 2: entrenamiento de personal operativo

y escenario 3: supervisión de procesos operativos) y en la escala total de PoDeRe, particularmente en la comparación entre los clúster de alta e intermedia incidentalidad. Las pruebas a posteriori de Tukey indicaron que ahí las diferencias eran significativas ($p < 0.05$).

Los datos de tamaño del efecto de variabilidad explicada más evidentes se ubicaron entre 0,010 y 0,015 (que correspondería a proporciones individuales por variable de 1% a 1,5%) lo que permitiría afirmar que, si bien no todas las dimensiones del potencial resiliente son indicadoras de efectos de clúster, sí hay dimensiones que se ven afectadas significativamente como son la capacidad de monitoreo y el potencial de desempeño resiliente total. Es llamativo que las capacidades de anticipación y de aprendizaje no se mostraron significativas y dieron un tamaño de efecto casi nulo (tabla 23, figura 27).

7.5.2 Nivel de seguridad operacional según clúster de incidentalidad. En lo que se refiere al comportamiento de la seguridad operacional según clúster de incidentalidad, en la tabla 24 se presentan los promedios e intervalos de confianza de las subescalas y la escala SegOp según clúster de incidentalidad, hallazgos que además se ilustran en la figura 28 y la figura 29 y se someten a prueba estadística en la tabla 25 con los resultados de la prueba de Anova de una vía y sus respectivos tamaños del efecto.

Se puede apreciar que contrario a lo esperado, en general los promedios más altos de percepción de la seguridad operacional los presentó consistentemente el clúster de mayor incidentalidad, particularmente en las subescalas de aprendizaje, compromiso, legitimidad y adaptabilidad, mientras que el perfil del clúster de incidentalidad intermedia puntuó con los menores niveles de seguridad operacional.

Tabla 24

Promedios de la escala SegOp diferenciados según clúster de incidentalidad

Subescala	Clúster	N	Media	Desviación estándar	95% intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Compromiso	Menor	113	71,8	18,3	68,4	75,2	6,3	100,0
	intermedio	249	70,6	18,9	68,2	72,9	,0	100,0
	Mayor	181	73,8	20,0	70,9	76,8	6,3	100,0
Gestión Información	Menor	113	61,5	13,4	59,1	64,0	20,0	100,0
	intermedio	249	60,0	13,9	58,3	61,8	,0	90,0
	Mayor	181	62,4	14,2	60,3	64,5	8,3	95,0
Componentes Seguridad	Menor	113	66,1	14,3	63,4	68,8	18,8	91,7
	intermedio	249	64,8	15,1	62,9	66,6	,0	91,7
	Mayor	181	67,6	15,7	65,3	69,9	19,4	91,7
Comp. Gestión seg. y oper.	Menor	113	72,4	16,7	69,3	75,5	21,9	100,0
	intermedio	249	69,4	18,2	67,2	71,7	,0	100,0
	Mayor	181	73,4	16,5	71,0	75,9	25,0	100,0
Accesibilidad	Menor	113	63,9	19,3	60,3	67,5	25,0	100,0
	intermedio	249	59,5	22,2	56,8	62,3	,0	100,0
	Mayor	181	66,2	22,3	62,9	69,4	12,5	100,0
Legitimidad	Menor	113	70,5	21,9	66,4	74,5	,0	100,0
	intermedio	248	68,4	21,1	65,7	71,0	,0	100,0
	Mayor	181	73,0	20,3	70,0	75,9	8,3	100,0
Adaptabilidad	Menor	113	72,8	19,4	69,1	76,4	,0	100,0
	intermedio	248	67,7	20,3	65,2	70,3	,0	100,0
	Mayor	181	72,7	18,8	69,9	75,4	6,3	100,0
Aprendizaje	Menor	113	74,8	20,7	70,9	78,6	,0	100,0
	intermedio	248	71,0	21,7	68,3	73,7	,0	100,0
	Mayor	180	75,3	21,8	72,1	78,5	,0	100,0
Cultura de la Seguridad	Menor	113	69,2	17,7	65,9	72,5	20,5	100,0
	intermedio	249	65,1	18,8	62,8	67,5	,0	100,0
	Mayor	181	70,7	18,6	67,9	73,4	17,3	100,0
Seguridad Operacional	Menor	113	69,2	15,5	66,3	72,0	21,3	96,7
	intermedio	249	66,2	16,5	64,1	68,2	2,6	96,7
	Mayor	181	70,5	16,4	68,1	72,9	22,5	96,7



Figura 28. Subescalas de la escala SegOp según clúster de incidentalidad

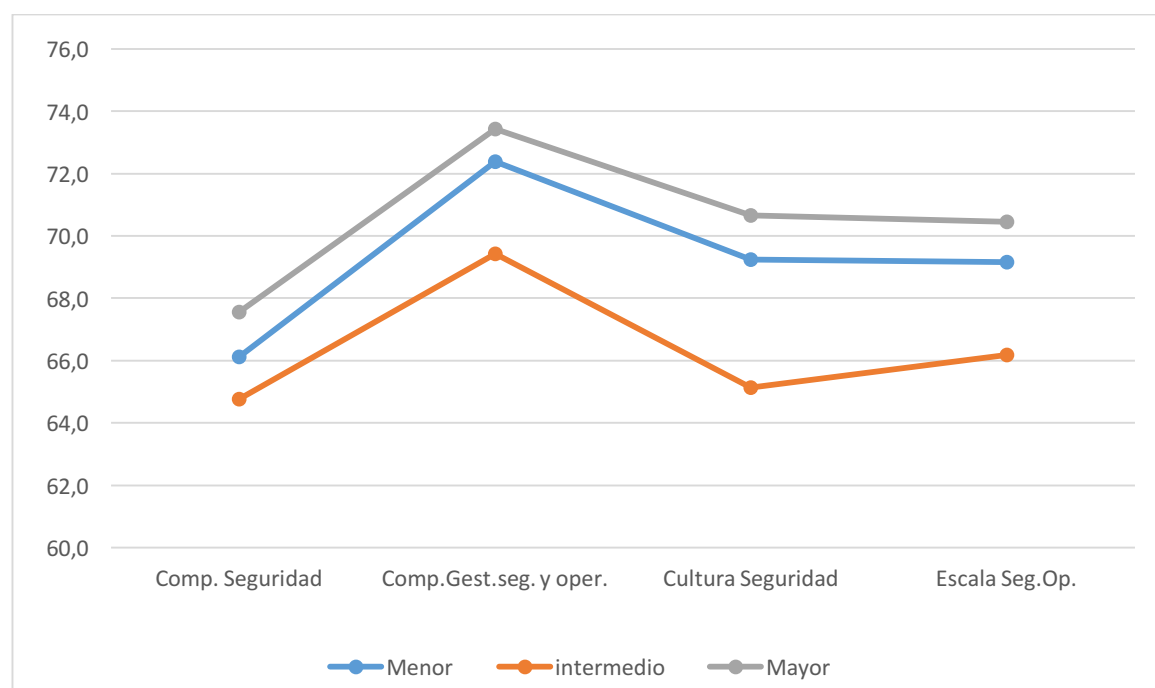


Figura 29. Promedios de las subescalas de la escala SegOp según clúster de incidentalidad

Por su parte, los puntajes correspondientes al clúster de incidentalidad menor se ubicaron en un grado medio entre el perfil del clúster de alta y el de intermedia incidentalidad, mostrando así que no se configura una relación explícitamente directa o inversamente proporcional entre el clúster de incidentalidad y el nivel de seguridad operacional (figura 28), de hecho los mayores niveles de seguridad operacional los presenta el clúster de mayor incidentalidad, seguidos por los de menor y en nivel más bajo están los valores de seguridad operacional del clúster de incidentalidad intermedia, a la manera general de un comportamiento en forma aproximada de una distribución jota.

Tabla 25

Anova para los promedios de la escala SegOp según clúster de incidentalidad

Variables de respuesta	<i>F</i>	<i>Sig.</i>	Tamaño del efecto [§] (<i>Eta parcial</i> ²)
Compromiso	1,550	,213	,006
Gestión Información	1,622	,198	,006
Componente Seguridad	1,785	,169	,007
Comp. Gestión seg. y oper.	3,037	,049*	,011 [⊗]
Accesibilidad	5,149	,006**	,019 ^{⊗⊗}
Legitimidad	2,501	,083	,009 [⊗]
Adaptabilidad	4,282	,014*	,016 [⊗]
Aprendizaje	2,478	,085	,009 [⊗]
Cultura de la Seguridad	5,069	,007**	,018 [⊗]
Seguridad Operacional	3,861	,022*	,014 [⊗]

* $p < 0,05$; ** $p < 0,01$.

[§]Nota: *Eta parcial* ²: [⊗]pequeño=0.01; ^{⊗⊗}mediano=0.06; ^{⊗⊗⊗}grande=0.13 (Domínguez-Lara, 2017).

En cuanto a los tamaños de efecto según el estadístico *eta parcial* ^{2 0} (tabla 25), las variabilidades explicadas más altas de la seguridad operacional se ubicaron entre 0,009 y 0,019 (que correspondería a proporciones individuales explicadas por variable de 0,9% a 1,9%) lo que lleva a afirmar que las dimensiones de las seguridad operacional que muestran efectos significativos y relevantes de los clúster son la accesibilidad, la cultura de la seguridad y la seguridad operacional total, donde el efecto del clúster logra las mayores nivel de variabilidad

explicada (figura 29).

En el siguiente apartado, se abordan los resultados por grupos de nivel de participación operacional, hipótesis 3 del estudio.

7.6 Análisis Diferencial en Función del Nivel de Participación Operacional

En la muestra del personal de participantes se recabó información sobre los rangos institucionales en la jerarquía de responsabilidad, mando y gerencia, diferenciando de manera ascendente los niveles táctico, operacional y estratégico, lo que por demás también está relacionado con los niveles de conocimiento y tiempo en la institución.

La intención de la hipótesis 3 de investigación (se espera que existan diferencias estadísticamente significativas en el potencial de desempeño resiliente entre el nivel gerencial estratégico de la seguridad operacional y los nivel táctico y operacional de la organización de aviación) es diferenciar el grupo que diseña operaciones del grupo que las ejecuta, la cual se formuló previendo diferencias significativas en el desempeño resiliente y en la seguridad operacional según el nivel de participación operacional que, para el efecto, están diferenciados en rangos ascendentes de 1°, 2° y 3° nivel, siendo estos últimos los de mayor rango.

7.6.1 Potencial de desempeño resiliente según el nivel de participación operacional. La tabla 26 muestra los promedios e intervalos de confianza de las subescalas y la escala PoDeRe diferenciados según el nivel de participación operacional, que a su vez se ilustran en las figuras 31 y 32, y fueron sometidas a prueba estadística en la tabla 27 con la prueba Anova de un factor de clasificación junto con la estimación del tamaño del efecto con el estadístico *eta parcial*².

Tabla 26

Promedios de la escala PoDeRe diferenciados según el nivel de participación operacional

				95% intervalo de confianza para la media		Mínimo	Máximo
Rango Jerárquico	N	Media	Desviación estándar	Límite inferior	Límite superior		
Capacidad 1° Nivel	283	71,0	18,4	68,9	73,2	0,0	100,0

		95% intervalo de confianza para la media						
Rango Jerárquico		N	Media	Desviación estándar	Límite inferior	Límite superior	Mínimo	Máximo
Rpta Esc1	2ºNivel	213	71,7	16,8	69,4	74,0	16,7	100,0
	3ºNivel	45	70,8	15,3	66,2	75,4	41,7	100,0
Capacidad	1ºNivel	283	71,2	18,5	69,1	73,4	0,0	100,0
Rpta Esc2	2ºNivel	213	71,6	17,4	69,2	73,9	8,3	100,0
	3ºNivel	45	69,0	16,7	64,0	74,0	29,2	100,0
Capacidad	1ºNivel	283	70,6	19,0	68,4	72,8	0,0	100,0
Rpta Esc3	2ºNivel	213	70,4	18,3	68,0	72,9	20,8	100,0
	3ºNivel	45	69,2	15,1	64,6	73,7	37,5	100,0
Capacidad	1ºNivel	283	71,0	18,1	68,8	73,1	0,0	100,0
Respuesta	2ºNivel	213	71,2	17,0	68,9	73,5	15,3	100,0
	3ºNivel	45	69,6	15,2	65,1	74,2	40,3	100,0
Capacidad	1ºNivel	284	73,0	19,5	70,8	75,3	3,6	100,0
Monitoreo Esc1	2ºNivel	212	72,7	18,5	70,2	75,2	0,0	100,0
	3ºNivel	45	72,6	15,5	68,0	77,3	33,3	100,0
Capacidad	1ºNivel	285	70,7	19,7	68,4	73,0	0,0	100,0
Monitoreo Esc2	2ºNivel	210	70,8	17,7	68,4	73,2	21,4	100,0
	3ºNivel	45	69,2	16,8	64,1	74,2	28,6	100,0
Capacidad	1ºNivel	285	72,6	20,1	70,3	75,0	0,0	100,0
Monitoreo Esc3	2ºNivel	210	72,1	18,3	69,7	74,6	25,0	100,0
	3ºNivel	45	71,1	16,6	66,1	76,1	28,6	100,0
Capacidad	1ºNivel	285	72,0	19,5	69,8	74,3	0,0	100,0
Monitorear	2ºNivel	212	71,4	18,7	68,9	74,0	0,0	100,0
	3ºNivel	45	70,9	16,0	66,1	75,7	33,3	100,0
Capacidad	1ºNivel	285	69,3	18,3	67,1	71,4	4,2	100,0
Aprender	2ºNivel	213	68,8	17,3	66,5	71,2	12,5	100,0
	3ºNivel	45	67,7	17,6	62,4	73,0	33,3	100,0
Capacidad	1ºNivel	284	65,8	20,7	63,4	68,2	0,0	100,0
Anticipar	2ºNivel	213	64,9	21,5	62,0	67,8	4,2	100,0
	3ºNivel	45	64,1	20,9	57,8	70,4	0,0	100,0
Potencial	1ºNivel	285	70,6	17,4	68,6	72,6	7,4	100,0
Desempeño Resiliente	2ºNivel	213	70,4	16,2	68,2	72,6	18,6	100,0
	3ºNivel	45	69,3	15,0	64,8	73,8	35,6	98,5

En general, se puede apreciar que hay similitud entre los promedios de las capacidades del potencial de desempeño resiliente según los grados de los 1º, 2º y 3º nivel, que se ubican entre puntajes de 65 – 73, lo cual se podría catalogar como niveles medio bajos. De hecho, en las figuras 30 y 31 se observa que las subescalas del potencial de desempeño resiliente los oficiales del 3º nivel presentan menor potencial resiliente mientras que los oficiales del 1º nivel

quienes estiman el desempeño resiliente en valores un poco más elevados, aunque en si bien los comportamientos parecen muy equivalentes.

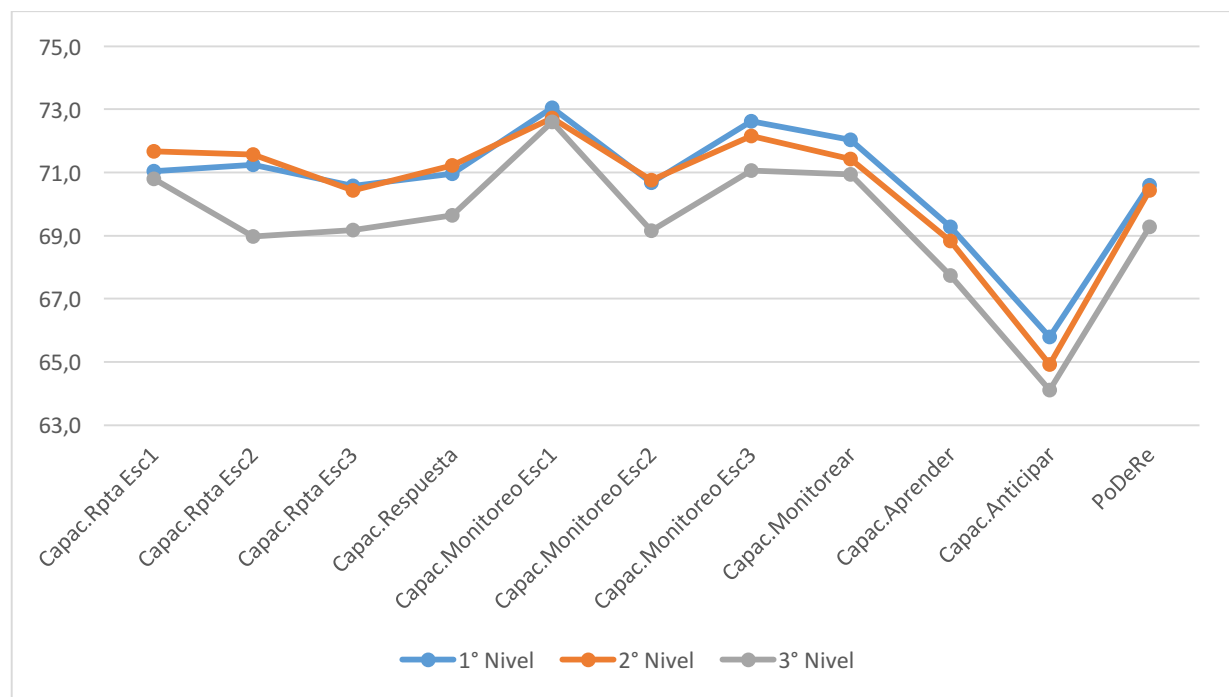


Figura 30. Subescalas de la escala PoDeRe según el nivel de participación operacional

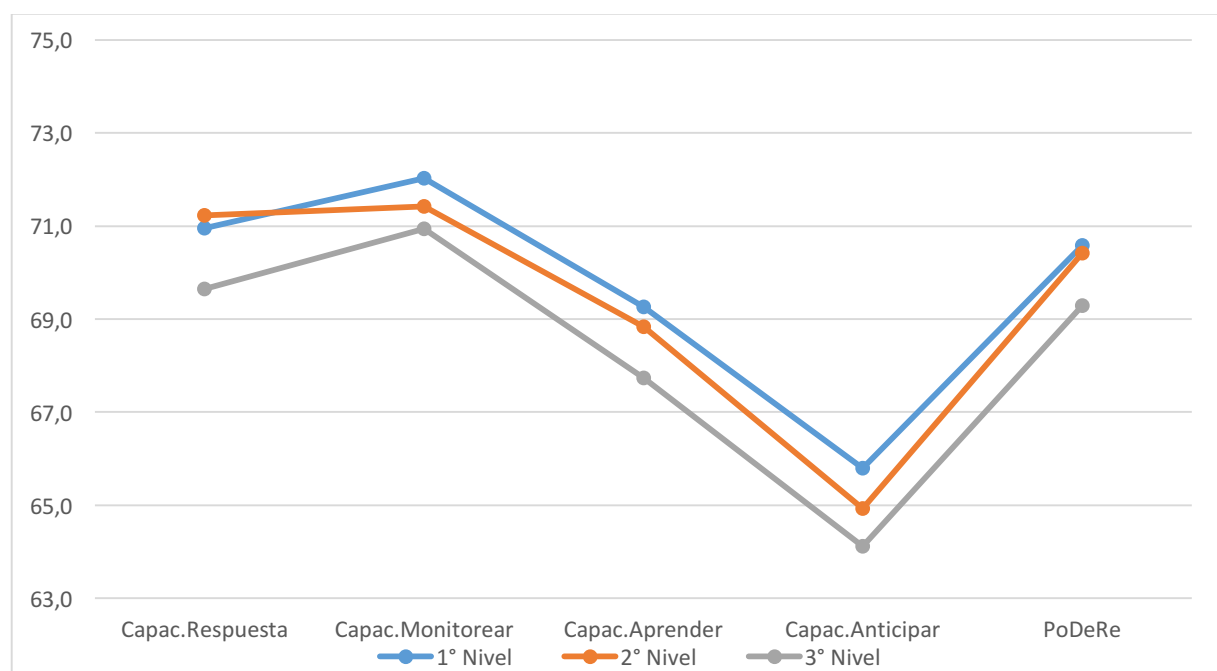


Figura 31. Promedios de subescalas de PoDeRe según el nivel de participación operacional

Las pruebas de Anova de un factor de clasificación (tabla 27) indican que las diferencias observadas no configuran diferencias estadísticamente significativas ($p > 0,05$) y los tamaños

del efecto (η^2 parcial) obtenidos están en valores muy bajos (numéricamente están entre 0,0004 y 0,0014) que corresponderían a 0,04% y 0,14% de variabilidad explicada.

Tabla 27

Pruebas de Anova para los promedios de la escala PoDeRe según nivel de participación operacional y los respectivos tamaños del efecto

Variables de repuesta	F	Sig.	Tamaño del efecto [§] (η^2 parcial)
Capacidad Rpta Esc1	,099	,906	0,0004
Capacidad Rpta Esc2	,390	,677	0,0014
Capacidad Rpta Esc3	,113	,893	0,0004
Capacidad Respuesta	,152	,859	0,0006
Capacidad Monitoreo Esc1	,024	,976	0,0001
Capacidad Monitoreo Esc2	,144	,866	0,0005
Capacidad Monitoreo Esc3	,142	,867	0,0005
Capacidad Monitorear	,102	,903	0,0004
Capacidad Aprender	,153	,858	0,0006
Capacidad Anticipar	,185	,831	0,0007
Potencial Desempeño Resiliente	,117	,890	0,0004

* $p < 0,05$; ** $p < 0,01$.

[§]Nota: η^2 parcial: ☉pequeño=0.01; ☉☉mediano=0.06; ☉☉☉grande=0.13 (Domínguez-Lara, 2017).

Lo anterior lleva a afirmar que definitivamente tanto por los valores de p como por los tamaños del efecto, el nivel de participación operacional no determina consideraciones diferenciales sobre el potencial de desempeño resiliente de esta entidad de aviación militar.

Seguidamente se presenta el análisis estadístico de diferencia de grupos para la variable seguridad operacional.

7.6.2 Nivel de seguridad operacional según el nivel de participación operacional.

Pasando ahora a la consideración de la seguridad operacional según el nivel de participación operacional, en la tabla 28 se presentan los promedios e intervalos de confianza de las subescalas y la escala SegOp.

Tabla 28

Promedios de la escala SegOp diferenciados según nivel de participación operacional

	Grado militar	N	Media	Desviación estándar	95% del intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Compromiso	1º Nivel	285	72,6	19,4	70,4	74,9	,0	100,0
	2º Nivel	213	71,1	18,5	68,6	73,6	6,3	100,0
	3º Nivel	45	71,4	20,9	65,1	77,7	,0	100,0
Gestión	1º Nivel	285	61,3	14,0	59,7	62,9	,0	100,0
Información	2º Nivel	213	61,4	13,7	59,5	63,2	15,0	90,0
	3º Nivel	45	59,0	14,6	54,6	63,4	8,3	85,0
Componentes	1º Nivel	285	66,4	15,3	64,6	68,1	,0	91,7
Seguridad	2º Nivel	213	65,7	14,8	63,7	67,7	19,4	91,7
	3º Nivel	45	64,9	16,1	60,1	69,7	4,2	91,7
Comp.	1º Nivel	285	71,7	17,8	69,6	73,7	,0	100,0
Gestión seg. y oper.	2º Nivel	213	71,0	17,2	68,7	73,4	21,9	100,0
	3º Nivel	45	71,2	16,5	66,2	76,1	31,3	100,0
Accesibilidad	1º Nivel	285	63,9	21,8	61,4	66,5	,0	100,0
	2º Nivel	213	61,6	22,0	58,7	64,6	5,0	100,0
	3º Nivel	45	59,3	21,0	53,0	65,6	12,5	100,0
Legitimidad	1º Nivel	284	70,7	21,4	68,2	73,2	,0	100,0
	2º Nivel	213	69,8	20,7	67,0	72,6	8,3	100,0
	3º Nivel	45	70,7	21,4	64,3	77,2	,0	100,0
Adaptabilidad	1º Nivel	284	70,9	20,3	68,6	73,3	,0	100,0
	2º Nivel	213	69,5	19,4	66,9	72,1	,0	100,0
	3º Nivel	45	71,6	17,6	66,3	76,9	18,8	100,0
Aprendizaje	1º Nivel	283	73,3	22,0	70,8	75,9	,0	100,0
	2º Nivel	213	72,9	21,1	70,0	75,7	,0	100,0
	3º Nivel	45	73,9	21,9	67,3	80,5	,0	100,0
Cultura de la Seguridad	1º Nivel	285	68,6	18,9	66,4	70,8	,0	100,0
	2º Nivel	213	67,0	18,4	64,5	69,5	17,3	100,0
	3º Nivel	45	66,9	18,0	61,5	72,3	10,4	100,0
Seguridad Operacional	1º Nivel	285	68,7	16,6	66,8	70,6	2,6	96,7
	2º Nivel	213	67,7	16,1	65,6	69,9	22,5	96,7
	3º Nivel	45	67,5	16,1	62,7	72,3	16,0	96,7

Por su parte, en las figuras 32 y 33 se presentan los perfiles de seguridad operacional con las subescalas y la escala del instrumento SegOp según el nivel de participación operacional.

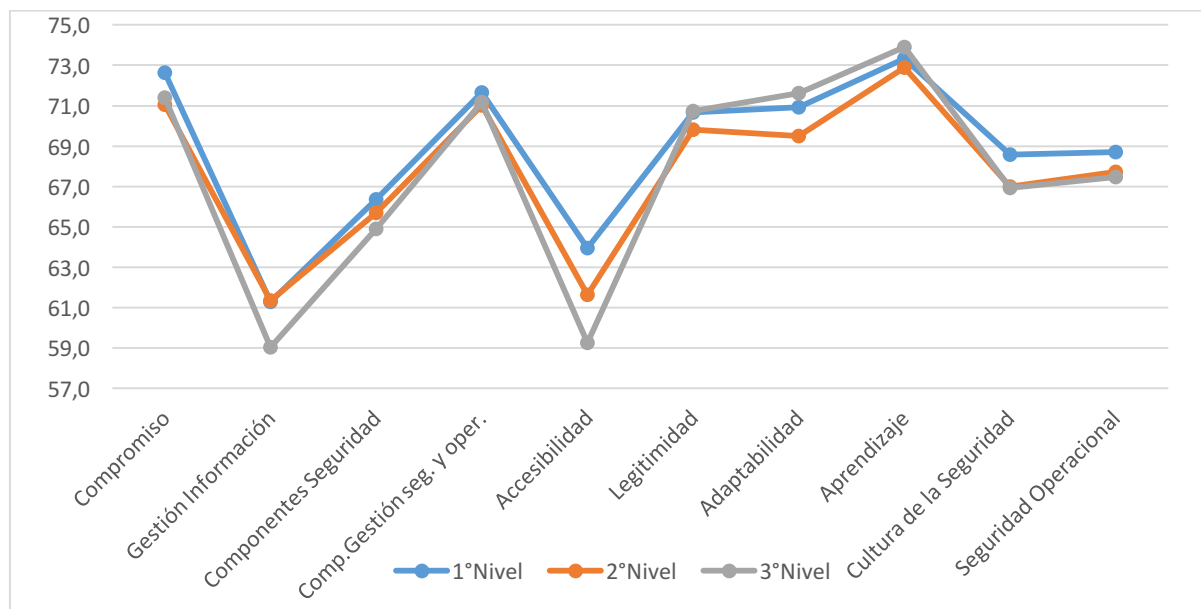


Figura 32. Subescalas de la escala SegOp según el nivel de participación operacional

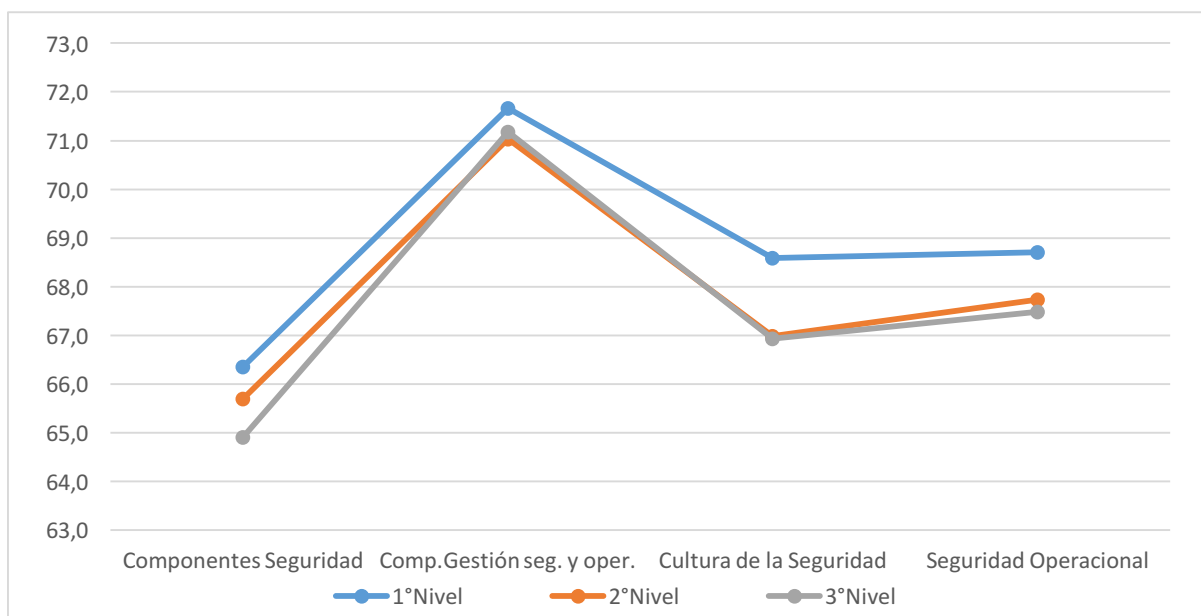


Figura 33. Promedios de las subescalas de la escala SegOp según el nivel de participación operacional

Así, se puede apreciar que en general los promedios más altos de seguridad operacional los presentaron consistentemente en todas las subescalas los oficiales de 1° nivel, mientras que los oficiales de los 2° y 3° nivel tuvieron valores un poco menores, aunque más similares entre ellos.

En la tabla 29 se presentan los resultados inferenciales de las pruebas Anova de una vía y

los tamaños del efecto *eta parcial*² correspondientes.

Tabla 29

Anova para los promedios de la escala SegOp según rango jerárquico

Variables de respuesta	F	Sig.	Tamaño del efecto [§] (<i>Eta parcial</i> ²)
Compromiso	0,423	0,655	0,0016
Gestión Información	0,555	0,574	0,0021
Componentes Seguridad	0,236	0,790	0,0009
Comp. Gestión de seguridad y operación	0,083	0,920	0,0003
Accesibilidad	1,275	0,280	0,0047
Legitimidad	0,106	0,899	0,0004
Adaptabilidad	0,407	0,666	0,0015
Aprendizaje	0,050	0,952	0,0002
Cultura de la Seguridad	0,505	0,604	0,0019
Seguridad Operacional	0,270	0,763	0,0010

*p<0,05; **p<0,01.

§Nota: *Eta parcial*²: ☉ pequeño=0.01; ☉☉ mediano=0.06; ☉☉☉ grande=0.13 (Domínguez-Lara, 2017).

Dados los valores de *p* las diferencias observadas en las variables de la seguridad operacional según el nivel de participación operacional no presentan diferencias estadísticamente significativas ($p>0,05$) y, por su parte, los tamaños del efecto (*Eta parcial*²) obtenidos presentan valores muy bajos (numéricamente están entre 0,0002 y 0,0047) que corresponderían a 0,02% y 0,47% de variabilidad explicada de la seguridad operacional a partir del rango de los oficiales.

Así entonces, se puede confirmar que los valores *p* y los tamaños del efecto indican que el nivel de participación operacional no influye de manera diferencial sobre el nivel de seguridad operacional de la organización militar.

Ahora bien, con el fin de realizar un análisis estadístico ajustado al planteamiento de la hipótesis 3, que sugiere la posible diferencia de percepción entre el grupo que diseña las operaciones y el grupo que las ejecuta, se realizó el análisis estadístico dividiendo la muestra en dos grupos, cuyos resultados se presentan a continuación.

7.6.3 Desempeño resiliente y seguridad operacional según rangos jerárquicos re-categorizados. Nivel de participación Operacional. Como análisis complementario de la evidencia, dados los anteriores resultados, se recategorizó el nivel de participación operacional de manera que se pudiera desagregar el efecto diferencial del nivel de dirección de operaciones (nivel 3 de participación operacional) vs los niveles operador (1 y 2 nivel de participación operacional), como complemento ampliado de la valoración estadística de la hipótesis 3 propuesta en el anterior capítulo de Método.

En la tabla 30 se reportan los niveles de significancia de las pruebas U de Mann-Whitney³ realizadas a las escalas PoDeRe y SegOp y sus respectivas subescalas en la comparación entre niveles de participación operacional 1° y 2° (operadores de primera línea) vs el nivel 3° (dirección de operaciones).

Como se puede apreciar allí, no se dieron diferencias significativas en ninguna de las escalas y subescalas PoDeRe y SegOp entre los dos grupos comparados, por lo cual se puede concluir que con esta recategorización del nivel de participación operacional se confirma la independencia entre las variables en comparación.

Tabla 30

Pruebas inferenciales de las escalas PoDeRe y SegOp según el nivel de participación operacional, niveles 1° y 2° vs el nivel 3°

	U de Mann-Whitney ^a	Z	Sig. (bilateral)
<i>Escala PoDeRe</i>			
Capacidad Rpta Esc1	10588,5	-,571	,568
Capacidad Rpta Esc2	10069,0	-1,090	,276

³ Dado que la conformación de los grupos así diferenciados dio una relación de 11,1 pilotos de los nivel 1°-2° por cada piloto del nivel 3°, lo que porcentualmente llega a ser del 91,7%, vs 8,3%, se da un marcado desbalance en los tamaños de las submuestras comparadas; no obstante, el alto tamaño muestral (teorema del límite central [Daniel, 2002]) y aun cuando se evidenció homogeneidad de varianza con la Prueba de Levene ($p > 0,05$), se optó por aplicar análisis no-paramétrico con la prueba U de Mann-Whitney centrada en el análisis de rangos ordinales (Siegel y Castellan, 1995). (N. de la A.)

	U de Mann-Whitney ^a	Z	Sig. (bilateral)
Capacidad Rpta Esc3	10195,5	-,964	,335
Capacidad Respuesta	10234,5	-,922	,356
Capacidad Monitoreo Esc1	10407,5	-,752	,452
Capacidad Monitoreo Esc2	10026,0	-1,112	,266
Capacidad Monitoreo Esc3	10208,5	-,930	,353
Capacidad Monitorear	10247,5	-,930	,352
Capacidad Aprender	10480,5	-,721	,471
Capacidad Anticipar	10484,5	-,696	,486
Potencial Desempeño Resiliente	10256,5	-,941	,347
<i>Escala SegOp</i>			
Compromiso	11183,0	-,022	,982
Gestión Información	10237,5	-,969	,333
Componentes Seguridad	10638,5	-,563	,573
Componente Gestión seg. y oper.	10916,5	-,287	,774
Accesibilidad	10129,5	-1,071	,284
Legitimidad	10886,5	-,299	,765
Adaptabilidad	11062,5	-,120	,904
Aprendizaje	10926,5	-,252	,801
Cultura de la Seguridad	10806,5	-,396	,692
Seguridad Operacional	10776,0	-,426	,670

a. Variable de agrupación: Rango jerárquico

Para profundizar en los resultados obtenidos en este apartado, se decidió realizar una nueva comparación de grupos con base en la variable “tiempo en la especialidad de pilotaje”, por considerarse que está directamente asociada al grado de conocimiento de la organización y a la manera en que está vinculada la persona a las operaciones (dirección vs ejecución).

7.7 Análisis Diferencial en Función del Tiempo en la Especialidad de Pilotaje

Para complementar el análisis, se quiso considerar el tiempo en la especialidad de pilotaje como otro de los factores organizacionales asociados que se están valorando en la institución, hipotetizando (hipótesis 3) diferencias con $p < 0.05$ en desempeño resiliente y en seguridad operacional.

7.7.1 Potencial de desempeño resiliente según el tiempo en la especialidad de pilotaje.

En la tabla 31 se presentan los promedios e intervalos de confianza de la escala PoDeRe y sus subescalas diferenciados entre los intervalos del tiempo laboral como oficiales de aviación.

Tabla 31

Promedios de escala PoDeRe diferenciados según tiempo en la especialidad de pilotaje

Subescala	Tiempo especialidad	N	Media	Desviación estándar	95% del intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Capacidad Rpta Esc1	<5 años	159	73,163	16,5633	70,569	75,757	10,0	100,0
	5-10a.	201	69,753	18,8900	67,126	72,381	,0	100,0
	10-20a.	145	71,276	16,9120	68,500	74,052	16,7	100,0
	>20a.	36	71,366	15,7386	66,041	76,691	41,7	100,0
Capacidad Rpta Esc2	<5 años	159	72,987	16,9461	70,333	75,642	4,2	100,0
	5-10a.	201	70,313	18,8619	67,690	72,936	,0	100,0
	10-20a.	145	70,914	17,9659	67,965	73,863	8,3	100,0
	>20a.	36	69,086	16,9423	63,353	74,818	29,2	100,0
Capacidad Rpta Esc3	<5 años	159	73,137	16,8421	70,499	75,775	4,2	100,0
	5-10a.	201	69,036	19,6397	66,304	71,768	,0	100,0
	10-20a.	145	69,753	18,7039	66,683	72,823	20,8	100,0
	>20a.	36	68,646	15,6107	63,364	73,928	37,5	100,0
Capacidad Respuesta	<5 años	159	73,096	16,2749	70,547	75,645	6,1	100,0
	5-10a.	201	69,701	18,5844	67,116	72,286	,0	100,0
	10-20a.	145	70,648	17,3821	67,794	73,501	15,3	100,0
	>20a.	36	69,699	15,4502	64,471	74,927	40,3	100,0
Capacidad Monitoreo Esc1	<5 años	160	75,370	17,6222	72,618	78,121	14,3	100,0
	5-10a.	201	70,879	19,3706	68,185	73,573	3,6	100,0
	10-20a.	144	73,040	19,7998	69,779	76,302	,0	100,0
	>20a.	36	72,333	15,0854	67,229	77,437	43,8	100,0
Capacidad Monitoreo Esc2	<5 años	160	73,065	17,8115	70,284	75,846	14,3	100,0
	5-10a.	202	68,035	19,7744	65,292	70,779	,0	100,0
	10-20a.	142	71,888	18,1489	68,878	74,899	21,4	100,0
	>20a.	36	68,715	16,8787	63,004	74,426	28,6	100,0
Capacidad Monitoreo Esc3	<5 años	160	75,539	17,1510	72,861	78,217	14,3	100,0
	5-10a.	202	69,602	20,7167	66,728	72,477	,0	100,0
	10-20a.	142	73,114	18,9062	69,978	76,251	25,0	100,0
	>20a.	36	69,916	16,5330	64,322	75,510	28,6	100,0
Capacidad Monitorear	<5 años	160	74,658	17,2220	71,969	77,347	14,3	100,0
	5-10a.	202	69,389	19,6916	66,657	72,121	,0	100,0
	10-20a.	144	72,010	19,9297	68,727	75,293	,0	100,0
	>20a.	36	70,321	15,7227	65,002	75,641	40,5	100,0
Capacidad Aprender	<5 años	160	71,268	17,0103	68,612	73,924	20,8	100,0
	5-10a.	202	67,578	18,2789	65,042	70,114	4,2	100,0
	10-20a.	145	68,629	17,9523	65,683	71,576	12,5	100,0
	>20a.	36	67,940	17,6288	61,975	73,905	33,3	100,0
Capacidad Anticipar	<5 años	160	68,544	19,0689	65,567	71,522	16,7	100,0
	5-10a.	201	62,488	21,8066	59,455	65,521	,0	100,0
	10-20a.	145	65,828	21,6153	62,280	69,376	4,2	100,0
	>20a.	36	64,676	20,7788	57,645	71,706	,0	100,0
Potencial Desempeño Resiliente	<5 años	160	72,963	15,7225	70,508	75,418	14,0	100,0
	5-10a.	202	68,489	17,4881	66,062	70,915	7,4	100,0
	10-20a.	145	70,602	16,8181	67,841	73,362	18,6	100,0
	>20a.	36	69,133	15,1936	63,992	74,274	35,6	98,5

También se muestran en la figura 34 y la figura 35 y fueron sometidas a prueba estadística en la tabla 32 con la prueba Anova de una vía junto con la estimación del tamaño del efecto con el estadístico *eta parcial*².

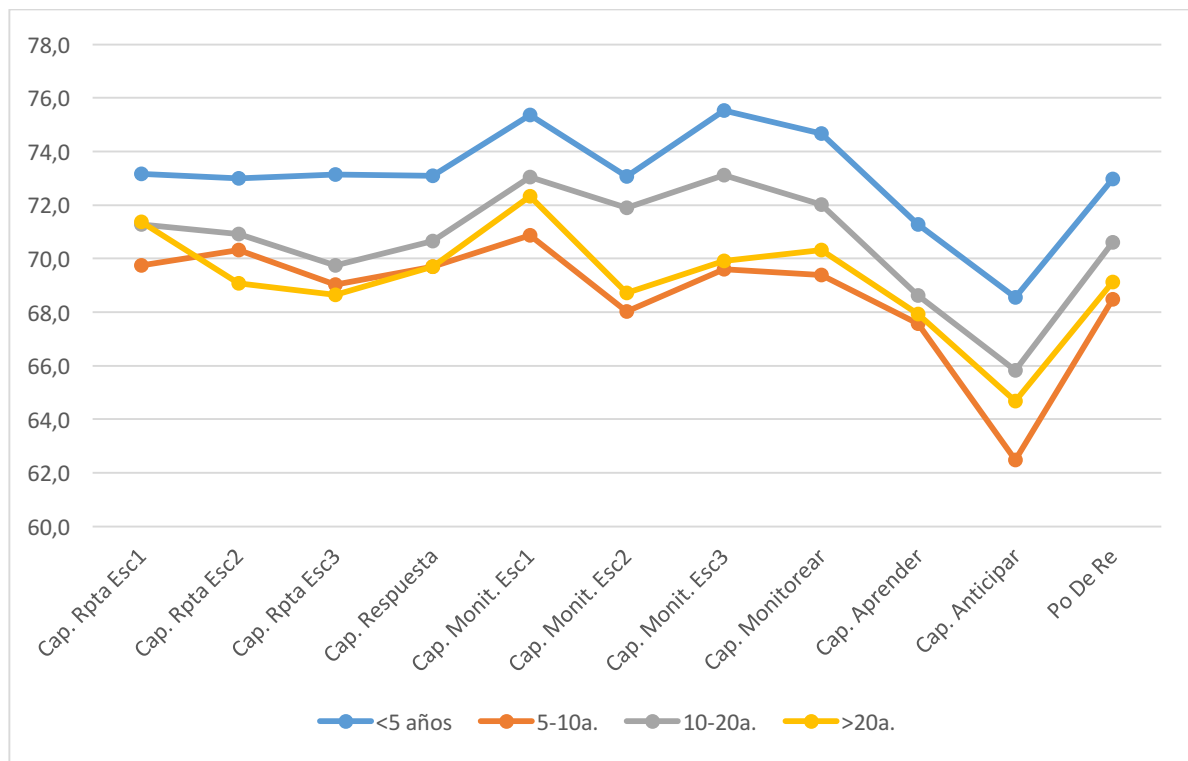


Figura 34. Subescalas de la escala PoDeRe según el tiempo en la especialidad de pilotaje

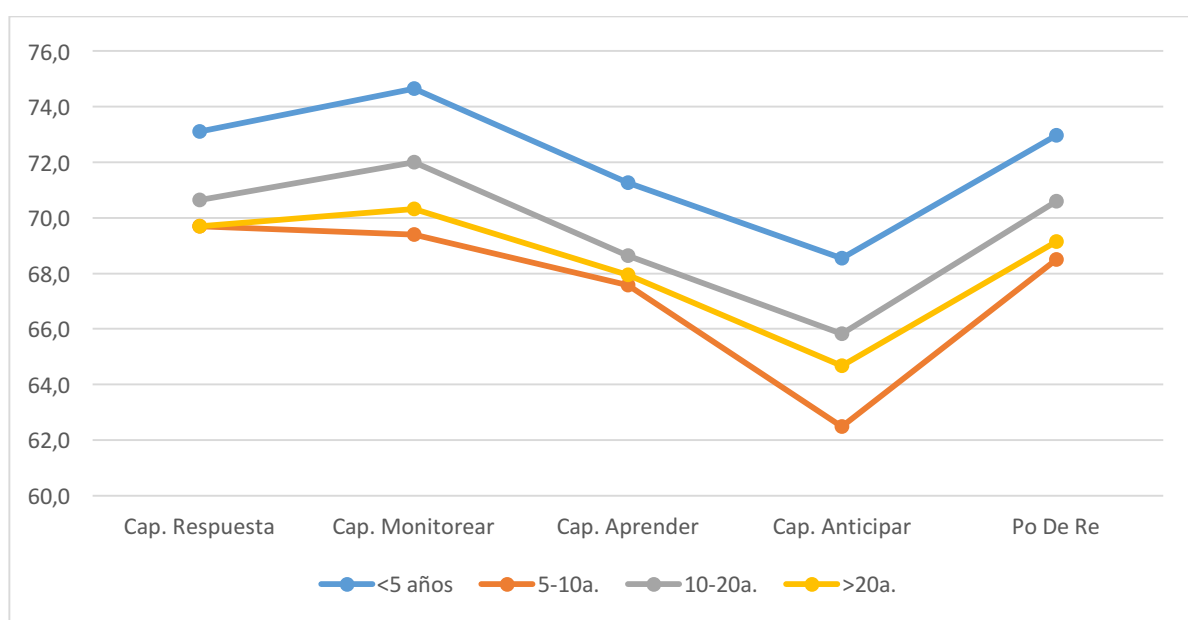


Figura 35. Promedios de subescalas de PoDeRe según el tiempo en la especialidad de pilotaje

Tabla 32

Pruebas de Anova para promedios de la escala PoDeRe según el tiempo en la especialidad de pilotaje y los respectivos tamaños del efecto

Variables	F	Sig.	Tamaño del efecto (Eta parcial ²)
Capacidad Rpta Esc1	1,123	0,339	0,006
Capacidad Rpta Esc2	0,868	0,458	0,005
Capacidad Rpta Esc3	1,718	0,162	0,010 [⊗]
Capacidad Respuesta	1,226	0,299	0,007
Capacidad Monitoreo Esc1	1,720	0,162	0,010 [⊗]
Capacidad Monitoreo Esc2	2,567	0,054	0,014 [⊗]
Capacidad Monitoreo Esc3	3,191	0,023*	0,018 [⊗]
Capacidad Monitorear	2,411	0,066	0,013 [⊗]
Capacidad Aprender	1,361	0,254	0,008 [⊗]
Capacidad Anticipar	2,536	0,056	0,014 [⊗]
Potencial Desempeño Resiliente	2,225	0,084	0,012 [⊗]

* $p < 0,05$; ** $p < 0,01$.

§ Eta parcial²: [⊗]pequeño=0.01; ^{⊗⊗}mediano=0.06; ^{⊗⊗⊗}grande=0.13 (Domínguez-Lara, 2017).

Se encontró que los promedios de potencial de desempeño resiliente según el tiempo de experiencia de los pilotos en su especialidad, como se apreció en las figuras 34 y 35, son más altos en aviadores con tiempo de experiencia $< 5,0$ años alcanzando 73 puntos; de otra parte, los oficiales con experiencia de 5-10 años estiman el desempeño resiliente en los valores más bajos, alrededor de 68 puntos y los de mayor experiencia se ubican en el intertanto.

Las pruebas de Anova de un factor de clasificación (tabla 32) indican que las diferencias solo se hicieron significativas en la capacidad de monitoreo del escenario 3 (supervisión de procesos operativos en el mantenimiento, las operaciones y el entrenamiento) ($p=0,023$) en la que los pilotos con menor tiempo en la especialidad indicaron mayor resiliencia vs. los de mayor experiencia que indicaron menor resiliencia, aunque el *eta parcial*² solo fue de 0,018 indicando un bajo tamaño del efecto (el tiempo de experiencia de vuelo de los oficiales explica solo el 1,8% de la variabilidad de la capacidad de monitoreo en los proceso de supervisión).

Los demás valores del *eta parcial*² con alguna significancia práctica también obtuvieron

bajos tamaño del efecto (numéricamente están entre 0,008 y 0,014, que corresponderían a un 0,8% y 1,4% de variabilidad explicada).

Lo anterior lleva a afirmar que tanto por la significancia p como por los tamaños del efecto, el tiempo de experiencia de vuelo tiene una baja influencia en sobre el nivel del potencial de desempeño resiliente de la institución.

7.7.2 Nivel de seguridad operacional según el tiempo en la especialidad de pilotaje.

Pasando ahora a la consideración de la seguridad operacional según tiempo de experiencia en la especialidad de vuelo, en la tabla 33 se presentan los promedios e intervalos de confianza.

Tabla 33

Promedios de la escala SegOp según el tiempo en la especialidad de pilotaje

Subescala	Tiempo especialidad	N	Media	Desviación estándar	95% del intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Compromiso	<5 años	160	74,909	18,3048	72,051	77,767	18,8	100,0
	5-10a.	202	69,709	19,4271	67,014	72,404	,0	100,0
	10-20a.	145	71,451	19,1179	68,313	74,589	6,3	100,0
	>20a.	36	72,743	20,8177	65,699	79,787	,0	100,0
Gestión Información	<5 años	160	62,648	13,1822	60,590	64,707	25,0	100,0
	5-10a.	202	59,899	13,8981	57,971	61,827	,0	87,5
	10-20a.	145	61,578	14,2826	59,233	63,922	15,0	90,0
	>20a.	36	59,537	15,7541	54,207	64,867	8,3	85,0
Componentes Seguridad	<5 años	160	68,174	14,2406	65,950	70,397	22,2	88,9
	5-10a.	202	64,238	15,4220	62,098	66,377	,0	91,7
	10-20a.	145	66,046	15,3196	63,531	68,560	19,4	91,7
	>20a.	36	65,664	16,6521	60,029	71,298	4,2	91,7
Comp. Gestión seg. y oper.	<5 años	160	73,892	16,5894	71,302	76,483	3,1	100,0
	5-10a.	202	69,879	18,0872	67,370	72,389	,0	100,0
	10-20a.	145	70,512	17,2734	67,676	73,347	21,9	100,0
	>20a.	36	72,053	17,0410	66,287	77,819	31,3	100,0
Accesibilidad	<5 años	160	66,130	20,1679	62,981	69,279	,0	100,0
	5-10a.	202	61,405	23,1090	58,199	64,611	,0	100,0
	10-20a.	145	61,253	21,4488	57,732	64,774	12,5	100,0
	>20a.	36	59,780	21,9527	52,352	67,208	12,5	100,0
Legitimidad	<5 años	160	71,953	19,1581	68,962	74,944	,0	100,0
	5-10a.	201	69,279	21,9592	66,224	72,333	,0	100,0
	10-20a.	145	70,057	21,6839	66,498	73,617	16,7	100,0
	>20a.	36	70,139	21,7649	62,775	77,503	,0	100,0
Adaptabilidad	<5 años	160	73,203	18,0800	70,380	76,026	,0	100,0
	5-10a.	201	69,413	20,2543	66,596	72,230	,0	100,0
	10-20a.	145	68,506	20,6247	65,120	71,891	,0	100,0
	>20a.	36	71,470	19,5169	64,866	78,073	18,8	100,0

Subescala	Tiempo especialidad	N	Media	Desviación estándar	95% del intervalo de confianza para la media		Mínimo	Máximo
					Límite inferior	Límite superior		
Aprendizaje	<5 años	159	73,742	21,1980	70,422	77,062	,0	100,0
	5-10a.	201	73,881	22,2624	70,784	76,977	,0	100,0
	10-20a.	145	71,207	21,1088	67,742	74,672	,0	100,0
	>20a.	36	75,000	21,5473	67,709	82,291	,0	100,0
Cultura de la Seguridad	<5 años	160	70,570	16,9365	67,925	73,214	,0	100,0
	5-10a.	202	66,738	19,5836	64,021	69,455	,0	100,0
	10-20a.	145	66,457	18,9998	63,338	69,576	17,3	100,0
	>20a.	36	67,248	18,5358	60,976	73,520	10,4	100,0
Seguridad Operacional	<5 años	160	70,755	15,0710	68,402	73,108	7,5	96,7
	5-10a.	202	66,762	17,0076	64,402	69,121	2,6	96,7
	10-20a.	145	67,493	16,5057	64,784	70,203	22,5	96,7
	>20a.	36	68,104	16,4020	62,554	73,653	16,0	96,7

Seguidamente en la figura 36 y la figura 37 se presentan los perfiles de seguridad operacional con las subescalas y la escala del instrumento SegOp según el tiempo de experiencia de los oficiales de aviación.

Los promedios más altos de seguridad operacional los presentaron consistentemente en todas las subescalas los pilotos con menor tiempo de experiencia en su especialidad, mientras que los pilotos con mayor tiempo de experiencia presentaron un nivel de seguridad operacional menor y con valores similares entre sí.

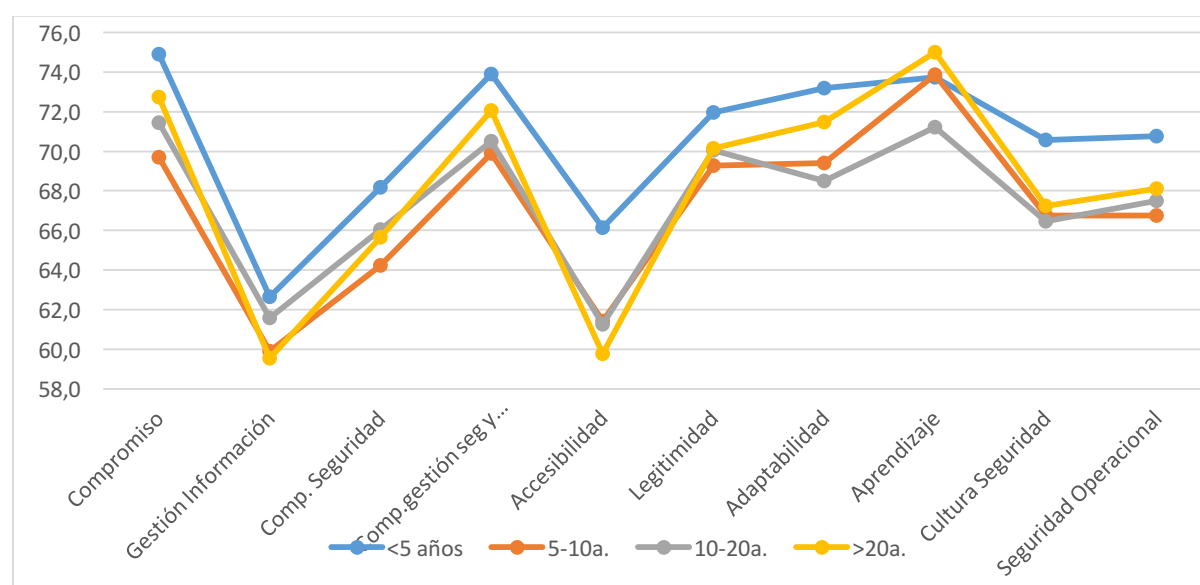


Figura 36. Subescalas de la escala SegOp según el tiempo en la especialidad de pilotaje

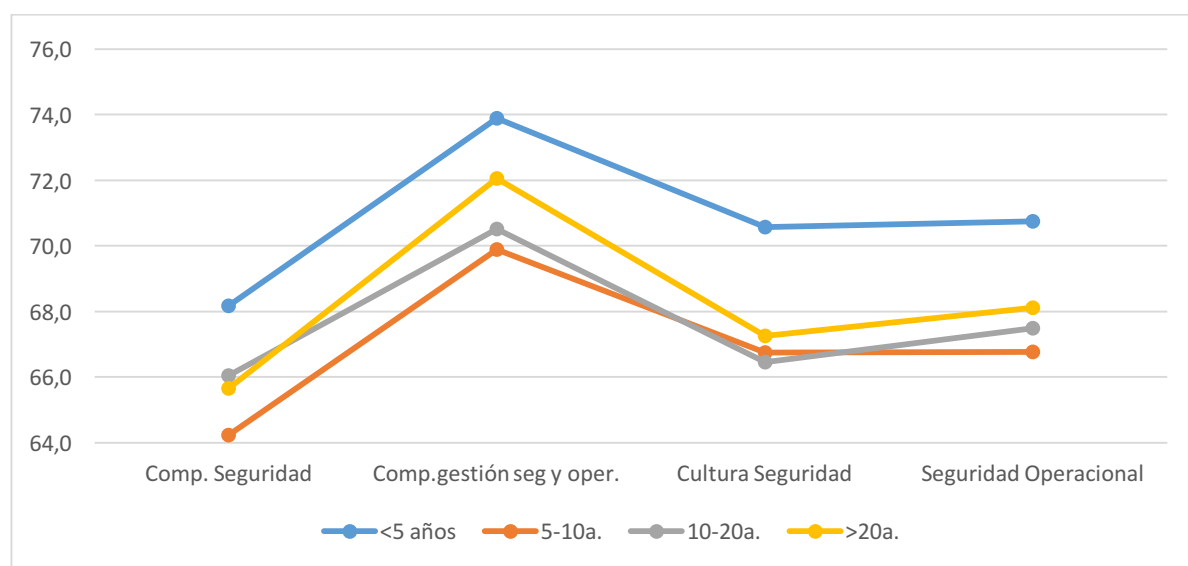


Figura 37. Promedios de las subescalas de la escala SegOp según el tiempo en la especialidad de pilotaje

En la tabla 34 se presentan los resultados inferenciales de las pruebas Anova de una vía y los tamaños del efecto *eta parcial*² correspondientes.

Tabla 34

Anova para los promedios de la escala SegOp según tiempo en la especialidad de pilotaje

Variable	F	Sig.	Tamaño del efecto (<i>Eta parcial</i> ²)
Compromiso	2,256	,081	,012 [⊗]
Gestión Información	1,367	,252	,008 [⊗]
Componentes Seguridad	2,017	,110	,011 [⊗]
Componente Gestión seg. y oper.	1,757	,154	,010 [⊗]
Accesibilidad	1,993	,114	,011 [⊗]
Legitimidad	,492	,688	,003
Adaptabilidad	1,731	,159	,010 [⊗]
Aprendizaje	,595	,619	,003
Cultura de la Seguridad	1,662	,174	,009
Seguridad Operacional	1,930	,124	,011 [⊗]

*p< 0,05; **p<0.01.

§Nota: *Eta parcial*²: [⊗]pequeño=0.01; ^{⊗⊗}mediano=0.06; ^{⊗⊗⊗}grande=0.13 (Domínguez-Lara, 2017).

Según los valores de *p*, las diferencias observadas en las variables de la seguridad operacional según la experiencia en la especialidad de pilotaje no presentan diferencias estadísticamente significativas (*p*>0,05) y los tamaños del efecto (*Eta parcial*²) de alguna

consideración, se encuentran en valores bajos (numéricamente están entre 0,008 y 0,012) que corresponderían a 0,08% y 1,2% de variabilidad explicada de la seguridad operacional a partir de tiempo de experiencia de los oficiales.

Así entonces, se puede confirmar que los valores p (significancias) y tamaños del efecto, indican que el tiempo de experiencia de los pilotos en su especialidad no muestra relación diferencial sobre el nivel de seguridad operacional de la entidad.

A continuación, se presenta el análisis correlacional que corresponde a la hipótesis 1. La razón por la que se presenta acá es por su importancia y vinculación con la hipótesis 4.

7.8 Análisis Correlacional: Relación Potencial de Desempeño Resiliente y Seguridad Operacional

Pasando al análisis correlacional que somete a prueba la presunción que hipotetizaba una relación directa significativa entre el potencial de desempeño resiliente y la seguridad operacional (hipótesis 1) en la institución de aviación militar, se elaboró la matriz de correlaciones que se despliega en la tabla 35.

Tabla 35

Matriz correlacional entre potencial de desempeño resiliente y seguridad operacional y sus respectivas subescalas

		Potencial					Comp.								
		Capac. Respuesta	Capacidad Monitorear	Capacidad Aprender	Capacidad Anticipar	Desempeño Resiliente	Comprom iso	Gestión Información	Comp. Seguridad	Gestión seg. y oper.	Accesibili dad	Legitimid ad	Adapta bilidad	Aprendi zaje	Cultura Seguridad
Capacidad Respuesta	r	1	,829**	,716**	,673**	,934**	,652**	,634**	,690**	,710**	,643**	,596**	,631**	,586**	,695**
	p		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	541	540	541	540	541	541	541	541	541	541	541	541	539	541
Capacidad Monitorear	r	,829**	1	,757**	,682**	,946**	,639**	,648**	,690**	,711**	,635**	,658**	,665**	,635**	,725**
	p	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	540	542	542	541	542	542	542	542	542	542	541	541	540	542
Capacidad Aprender	r	,716**	,757**	1	,766**	,848**	,729**	,684**	,760**	,741**	,698**	,646**	,679**	,640**	,752**
	p	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Capacidad Anticipar	r	,673**	,682**	,766**	1	,804**	,745**	,729**	,791**	,753**	,714**	,682**	,684**	,621**	,772**
	p	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	540	541	542	542	542	542	542	542	542	542	541	541	540	542
Potencial Desempeño Resiliente	r	,934**	,946**	,848**	,804**	1	,737**	,725**	,784**	,795**	,725**	,704**	,727**	,678**	,800**
	p	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Compro- miso	r	,652**	,639**	,729**	,745**	,737**	1	,739**	,944**	,808**	,694**	,710**	,690**	,661**	,778**
	p	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Gestión Informac.	r	,634**	,648**	,684**	,729**	,725**	,739**	1	,915**	,724**	,659**	,636**	,634**	,616**	,719**
	p	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Componen- te Seguridad	r	,690**	,690**	,760**	,791**	,784**	,944**	,915**	1	,825**	,729**	,730**	,714**	,688**	,808**
	p	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
C. Gestión seg. y oper.	r	,710**	,711**	,741**	,753**	,795**	,808**	,724**	,825**	1	,760**	,758**	,785**	,701**	,853**
	p	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543

		Capac. Respuesta	Capacidad Monitorear	Capacidad Aprender	Capacidad Anticipar	Potencial Desempeño Resiliente	Compromiso	Gestión Información	Comp. Seguridad	Comp. Gestión seg. y oper.	Accesibili- dad	Legitimidad	Adapta- bilidad	Aprende- zaje	Cultura Seguridad
Accesibi- lidad	r	,643**	,635**	,698**	,714**	,725**	,694**	,659**	,729**	,760**	1	,709**	,730**	,610**	,912**
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Legitimi- dad	r	,596**	,658**	,646**	,682**	,704**	,710**	,636**	,730**	,758**	,709**	1	,762**	,652**	,879**
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000
	N	541	541	542	541	542	542	542	542	542	542	542	542	540	542
Adaptabili- dad	r	,631**	,665**	,679**	,684**	,727**	,690**	,634**	,714**	,785**	,730**	,762**	1	,711**	,913**
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000
	N	541	541	542	541	542	542	542	542	542	542	542	542	540	542
Aprende- zaje	r	,586**	,635**	,640**	,621**	,678**	,661**	,616**	,688**	,701**	,610**	,652**	,711**	1	,765**
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000
	N	539	540	541	540	541	541	541	541	541	541	540	540	541	541
Cultura Seguridad	r	,695**	,725**	,752**	,772**	,800**	,778**	,719**	,808**	,853**	,912**	,879**	,913**	,765**	1
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543
Seguridad operacional	r	,741**	,757**	,797**	,820**	,844**	,879**	,821**	,916**	,939**	,869**	,855**	,873**	,767**	,962**
	p	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	N	541	542	543	542	543	543	543	543	543	543	542	542	541	543

Se puede apreciar que tanto las correlaciones entre el potencial de desempeño resiliente y la seguridad operacional, como las correlaciones entre las capacidades de responder, monitorear, anticipar y aprender con dicho nivel de seguridad operacional son estadísticamente significativas ($p < 0,05$) y también muestran una polaridad de relación directa (positiva).

Esta evidencia permite indicar que efectivamente la afirmación hipotetizada es sostenible estadísticamente al confirmar que el alto nivel de potencial de desempeño resiliente se asocia con una mayor seguridad operacional y, por el contrario, un bajo nivel de desempeño resiliente se relaciona con un menor nivel de seguridad operacional.

Esto se puede apreciar en la figura 38 en el *scatterplot* entre los puntajes totales de estas dos variables, que a la vez refleja la relación directa y la alta concentración de los valores observados, así como la diferenciación entre los clúster de incidentalidad.

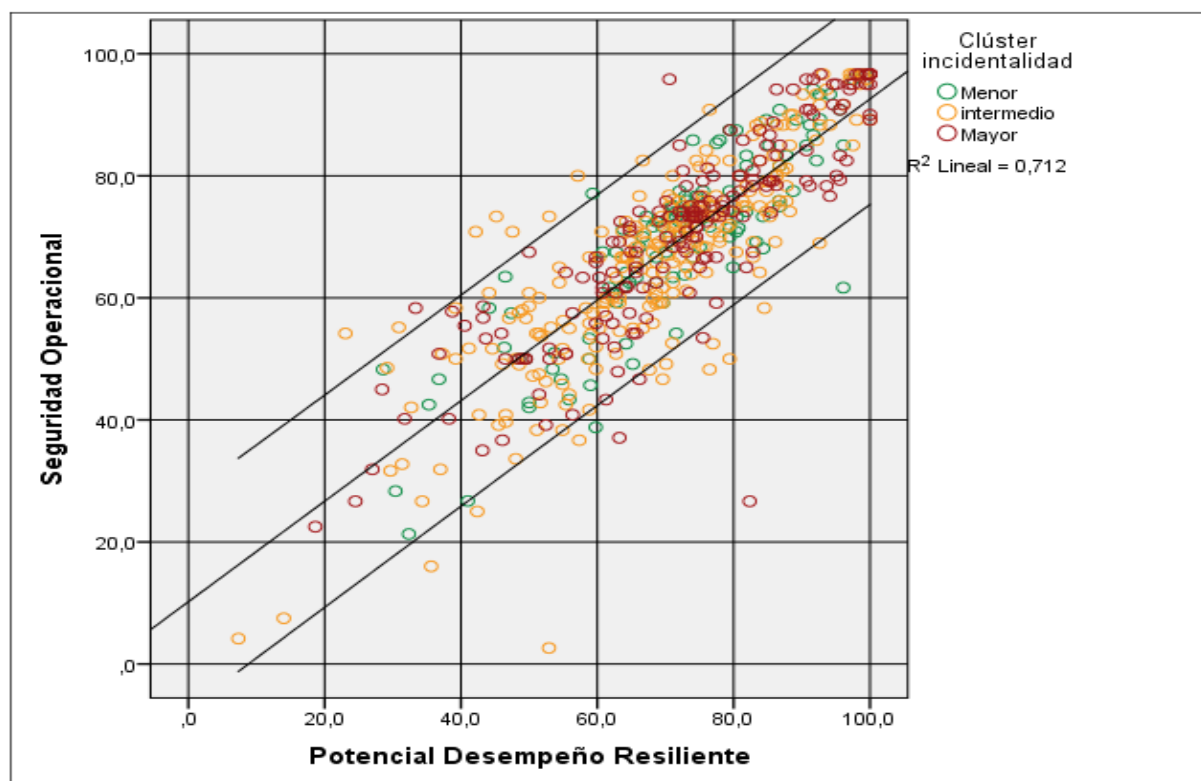


Figura 38. Scatterplot de potencial de desempeño resiliente y la seguridad operacional en los clúster de incidentalidad

Así mismo, en la tabla 36 se mostró también que las correlaciones entre las subescalas del potencial de desempeño resiliente y la seguridad operacional también fueron significativas y con polaridad directa en las relaciones, luego también se puede afirmar que las capacidades resilientes de la institución de responder, monitorear, anticipar y aprender correlacionan positivamente con la seguridad operacional. En la figura 39 se muestran los respectivos scatterplot.

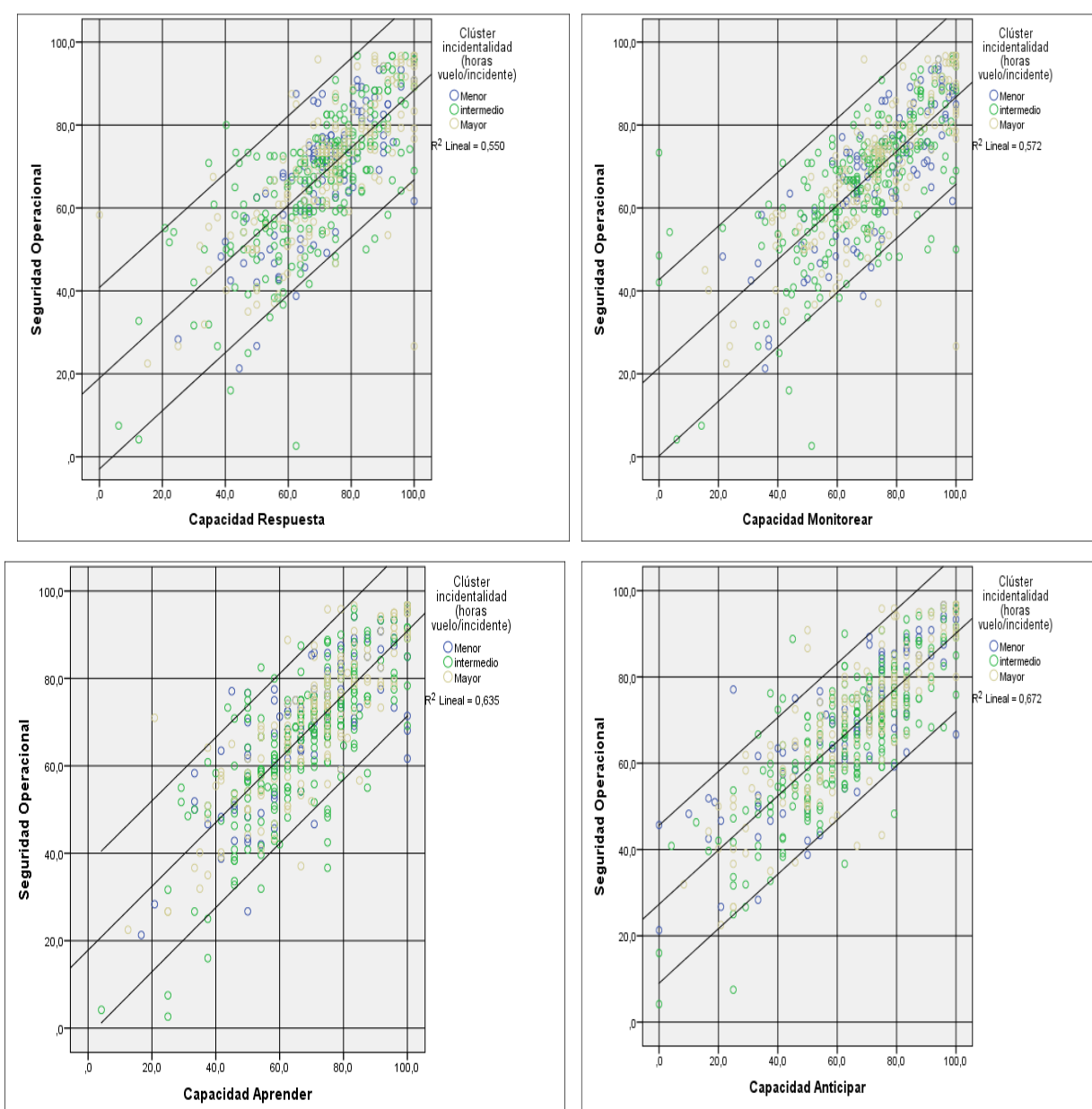


Figura 39. Scatterplot entre las dimensiones del potencial de desempeño resiliente y la seguridad operacional de la entidad militar

Se resalta que las magnitudes de las correlaciones encontradas son relativamente altas y efectivamente superan el nivel de significancia hipotetizado como referente de aceptación / rechazo de las hipótesis relacionales subyacentes, lo cual indica que hay una media / alta fuerza de la relación real entre las variables de potencial resiliente y la seguridad operacional institucional, cuyas implicaciones luego serán analizadas.

Así, con base en lo anterior se puede concluir que esta investigación arroja evidencia empírica significativa que da respaldo a la hipótesis 1 de relación directa entre el potencial de desempeño resiliente y la seguridad operacional, máxime que las magnitudes correlacionales son media altas y altas y por ello posiblemente tal tendencia relacional se da en la mayor parte de la entidad estudiada y es la tendencia mayoritaria.

Teniendo en cuenta este resultado, se procedió a desarrollar un análisis estadístico de función predictiva que permitiera establecer posibles relaciones causales entre las variables de modo que sea posible estimar el comportamiento de la seguridad operacional a partir del potencial de desempeño resiliente de la organización.

7.9 Análisis Regresional: Modelamientos Predictivos de la Seguridad Operacional en Función del Potencial de Desempeño Resiliente

7.9.1 Modelo de predicción múltiple: Teniendo en consideración la hipótesis 4 que plantea la búsqueda de una función predictiva (regresión múltiple) que permita estimar el nivel de seguridad operacional en función del potencial de desempeño resiliente a partir de los resultados correlacionales, se analiza la capacidad predictiva tomando como variable predictora el potencial desempeño resiliente y como variable criterio la seguridad operacional. Para ello, la tabla 36 presenta el modelo de estimación ajustado donde además se conforma la ecuación de regresión respectiva, que se propone como opción utilizable para la predicción del nivel de seguridad operacional de la institución militar de aviación en función del potencial de desempeño resiliente conocido.

Tabla 36

Modelo predictivo de seguridad operacional en función del potencial de desempeño resiliente

Modelo	Coeficientes no estandarizados		t	Sig.	Intervalo de confianza para B	
	B				L. inferior	L. superior
1 (Constante)	10,203		6,256	,000	6,999	13,407
Potencial Desempeño Resiliente	,824		36,558	,000	,780	,869

Variable dependiente: Seguridad Operacional

Con base en lo anterior, se podría configurar la ecuación de predicción lineal que se presenta en la ecuación 2.

$$SegOp = 10,2 + 0,82 PoDeRe$$

Ec. 2.

∴ SegOp: Grado de seguridad operacional (VD)

PoDeRe: Nivel de Potencial de Desempeño Resiliente (VI)

Con este modelo de estimación se puede afirmar que con $p < 0,01$ se puede predecir significativamente que si se logra mejorar específicamente el potencial de desempeño resiliente en un punto porcentual (según la escala PoDeRe), el nivel de seguridad operacional se aumentaría en 0,82 (según la escala SegOp) y viceversa, es decir, si se considera un decremento, se dará un decremento.

Así mismo, aunque solo sea de interés teórico, también se podría prever que ante una situación dramática de inhibición completa del potencial de desempeño resiliente se tendría una seguridad operacional positiva de solo 10,2 puntajes porcentuales.

De otra parte, al considerar las subescalas del potencial de desempeño resiliente en la valoración del ajuste de una ecuación predictiva múltiple tipo step wise forward, se obtiene el modelo de regresión lineal que se despliega en la tabla 37.

Tabla 37

Modelo predictivo step waise forward de la seguridad operacional en función de las capacidades del desempeño resiliente

Variable	Coeficiente B	t	Sig.	Intervalo 95,0% confianza para B		Correlaciones			Estadísticas colinealidad	
				L. Inf.	L. Sup.	O. cero	Parcial	Parte	Tolerancia	FIV
(Constante)	11,441	7,853	,000	8,579	14,304					
Capacidad anticipar	,315	12,452	,000	,265	,365	,818	,475	,253	,379	2,639
C. Monitoreo esc3	,180	5,942	,000	,120	,239	,761	,249	,121	,327	3,062
C. Aprender	,213	6,458	,000	,148	,278	,797	,270	,131	,313	3,199
C. de Rpta esc2	,121	4,032	,000	,062	,180	,722	,172	,082	,372	2,690

Variables excluidas

Variable ^a	Beta	t	Sig.	Correlación parcial	Colinealidad		
					Tolerancia	FIV ^b	Tolerancia mínima
C. Rpta Esc1	,064 ^c	1,198	,231	,052	,146	6,866	,146
C. Rpta Esc3	,051 ^c	,902	,368	,039	,131	7,627	,131
C. Monitoreo Esc1	,068 ^c	1,112	,267	,048	,112	8,950	,112
C. Monitoreo Esc2	,021 ^c	,311	,756	,013	,095	10,531	,095

a. Variable dependiente: Seguridad Operacional ^b Factor de inflación de la varianza.

e. Predictores modelo: (Constante), Capacidad anticipar, Capacidad monitoreo Esc3, Capacidad aprender, Capacidad rpta Esc2

Con base en los resultados anteriores, se puede indicar un nuevo modelo de predicción lineal múltiple ajustado con $p < 0.05$ que se presenta en la ecuación 3.

$$\begin{aligned}
 \text{SegOp} = & 11,4 + 0,32\text{CaAn} + 0,18\text{CaM3} + 0,21\text{CaAp} \\
 & + 0,12\text{CaRp2}
 \end{aligned}$$

∴ SegOp: Nivel de seguridad operacional (VD)
 CaAn: Capacidad Anticipar
 CaM3: Capacidad Monitoreo Escenario 3
 CaAp: Capacidad Aprender
 CaRp2: Capacidad Rpta Escenario 2

Ec. 3.

Esta ecuación evidencia la función predictiva de las subescalas de potencial de desempeño resiliente sobre el nivel de seguridad operacional, precisando que esa predictibilidad radica en la capacidad para anticipar, la capacidad de monitoreo en el escenario 3 (supervisión de las operaciones), la capacidad para aprender y la capacidad para responder en el escenario 2

(entrenamiento).

De esta manera, con una significancia probabilística (< 0.01) se podría llegar a estimar potencialmente que al lograr un incremento en la resiliencia de un punto porcentual en los niveles de anticipación, monitoreo (en escenario de supervisión de operacional), aprendizaje y respuesta (en escenario de entrenamiento), se obtendría un mejoramiento del nivel de seguridad operacional en un nivel que oscilaría entre 0,12 y 0,31 puntos porcentuales (aunque ciertamente, no son en sí mismo elementos sumativos).

Igualmente, también se podría prever que ante una inhibición completa del potencial de desempeño resiliente se tendría una seguridad operacional positiva que solo llegaría a 11,4 puntos porcentuales.

Descrito lo anterior y buscando una mayor precisión de la función predictiva, a continuación, se presentan los resultados de una regresión logística, modelo estadístico que se aplicó con objeto de ampliar la perspectiva de estimación de la seguridad operacional.

7.9.2 Modelo de predicción logística: Con el propósito de extraer más evidencia predictiva, se desarrolló un análisis tipo step wise forward bajo la consideración de un modelamiento con base en regresión logística binaria que permitiese la predicción de la seguridad operacional (0=baja [0-70]; 1=alta [71-100]) y el cálculo multivariado de OR (odds ratio, estimador del riesgo relativo) como coeficientes de regresión parcial. La tabla 38 muestra el modelo logístico ajustado.

Tabla 38

Modelo logístico de estimación de la seguridad operacional en función de predictores del potencial de resiliencia

Variables en la ecuación							
Variables		B	Error estándar	Sig.	$Exp(B)^b$	95% C.I. para $Exp(B)$	
						Inferior	Superior
Paso 4 ^a	Cap.Rpta.Esc3	,884	,296	,003	2,420	1,356	4,319
	Cap.Monit.Esc2	1,712	,294	,000	5,542	3,113	9,869

Variables en la ecuación						
Variables	B	Error estándar	Sig.	$Exp(B)^b$	95% C.I. para $Exp(B)$	
					Inferior	Superior
Cap.Aprender	1,305	,286	,000	3,688	2,105	6,462
Cap.Anticipar	1,677	,274	,000	5,351	3,128	9,153
Constante	-8,707	,689	,000	,000		

a. Variables especificadas en el paso 4: Cap.Rpta.Esc3.
b. Corresponde al *OR*, estimador del riesgo relativo.

Con base en ello se deja propuesta la ecuación 4 de predicción logística para estimar una condición de alta seguridad operacional, con base en las capacidades del potencial de resiliencia de la organización.

$$P_{(Y=1)} = \frac{1}{1 + e^{-(8,707 + 0,884CaRpta3 + 1,712CaMo2 + 1,305CaAp + 1,677CaAnt)}}$$

Ec. 4

∴ P_(Y=1): Probabilidad de Alta Seguridad Operacional
e: Constante neperiana de los logaritmos naturales
CaRpta3: Capacidad de responder en el escenario 3
CaMo2: Capacidad de monitorear en el escenario 2
CaAp: Capacidad de aprendizaje
CaAnt: Capacidad de anticipación

Luego así, con una significancia de $p = 0.02$, el modelo ajustado podrá estimar la condición de seguridad operacional con los predictores del potencial de desempeño resiliente como variables categóricas ($0 = \leq 70$; $1 = > 70-100$).

El modelo indica que la mayor seguridad operacional ($1 = > 70-100$) se da con altos nivel de capacidad de respuesta en el escenario 3, en la capacidad de monitoreo en el escenario 2, en la capacidad de aprendizaje y en la capacidad de anticipación como capacidades resilientes que estiman significativamente la seguridad operacional. Por ende, son estas las dimensiones que se deben potenciar en la institución para fortalecer la seguridad operacional, mientras que las demás capacidades no aportan significativamente a la predicción.

Este modelo ajustado según la prueba de Hosmer y Lemeshow (Hair et al., 2000) arrojó en

conjunto un nivel de clasificación correcta pronosticada del 95%, donde todos elementos de alta seguridad se clasifican como tal y los de baja seguridad en la estimación se clasifican en la categoría correspondiente.

Descrito lo anterior con este estudio se puede concluir que hay evidencia significativa suficiente que confirma que en la institución de aviación militar el nivel de seguridad operacional y el potencial de desempeño resiliente, no solo están relacionadas en función directa, sino que el potencial de desempeño resiliente es además, un estimador significativo del nivel de seguridad, de manera que un alto nivel de resiliencia permite predecir un mayor grado de seguridad operacional y viceversa, una menor resiliencia correlaciona y predice una menor seguridad operacional, además que dadas las medianamente altas y altas correlacionales, posiblemente tal tendencia relacional se da en distintas situaciones operacionales de la entidad de aviación militar.

7.10 Análisis Cualitativo

La hipótesis 5 de esta investigación es un supuesto que corresponde a la fase cualitativa del diseño secuencial explicativo (mixto) y su resultado corresponde a la realización de dos grupos focales y entrevistas personales a cinco integrantes de la organización (tabla 39), ubicados en diferentes niveles de la estructura institucional quienes voluntariamente aceptaron participar en el análisis de los resultados cuantitativos. Esta muestra constituye el 1,6% de la población general y el 2,6% de la muestra del estudio cuantitativo, ubicándose dentro de la muestra de máxima variabilidad planteada en el procedimiento.

Tabla 39

Participantes en los grupos focales y las entrevistas

#	Piloto		Tiempo en la organización	Nivel de participación operacional
	Si	No		
Grupo focal # 1				

#	Piloto		Tiempo en la organización	Nivel de participación operacional
	Si	No		
1	X		Más de 15 años	Estratégico
2	X		Más de 15 años	Estratégico
3	X		Más de 15 años	Estratégico
4		X	Más de 15 años	Estratégico
5	X		Más de 15 años	Estratégico
6		X	Más de 15 años	Estratégico
Grupo focal # 2				
1	X		Más de 15 años	Operacional/Táctico
2	X		Entre 10 y 15	Táctico
3		X	Entre 10 y 15	Táctico
4		X	Entre 10 y 15	No participa directamente
Entrevistas				
1	X		Más de 15 años	Operacional
2	X		Más de 15 años	Táctico
3	X		Más de 15 años	Estratégico
4	X		Entre 10 y 15	Táctico
5	X		Entre 10 y 15	Táctico

Se hace notar que esta fase del estudio tomó como punto de partida los principales hallazgos de la fase cuantitativa y su objetivo es establecer posibles configuraciones organizacionales o patrones de interacción que brinden un abordaje comprensivo de los hallazgos.

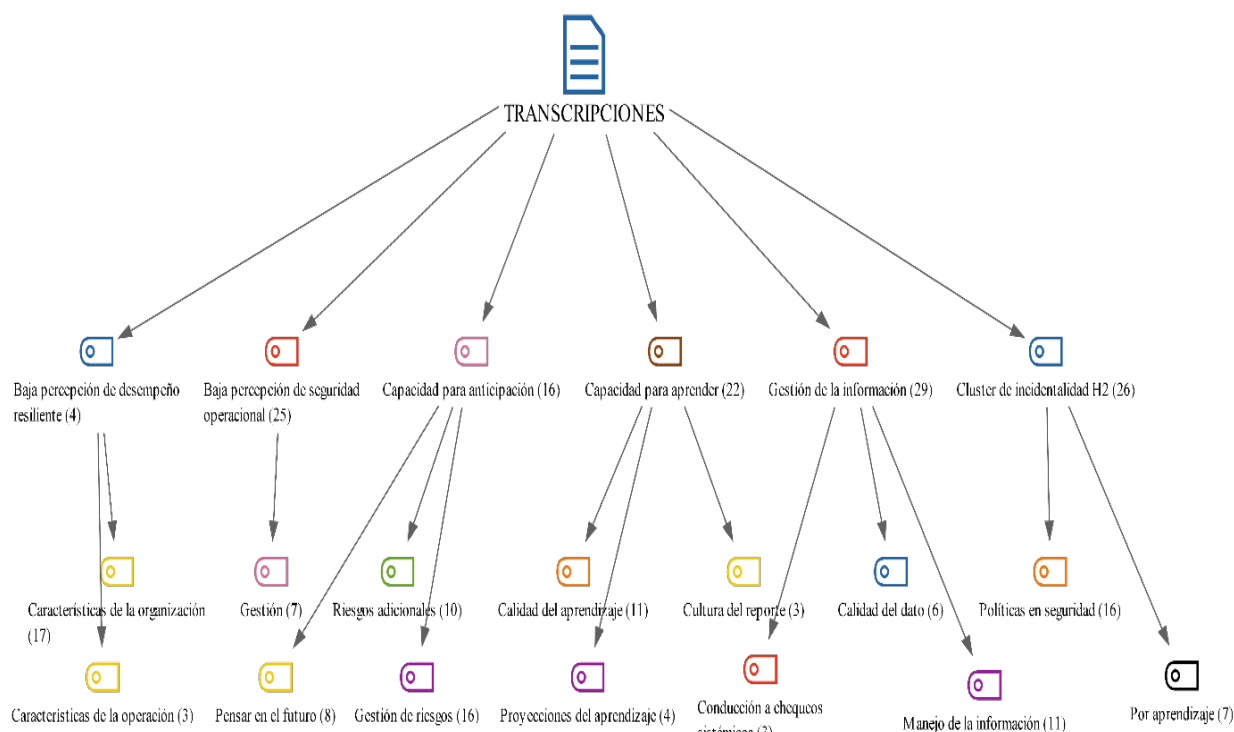
La intervención con los grupos y personas se realizó aplicando la guía elaborada (Anexo G) y se indagó puntualmente sobre los hallazgos de la fase cuantitativa. La información verbal obtenida fue transcrita y, posteriormente, codificada utilizando el software MAXQDA 2020 (Verbi Software, 2019).

7.10.1 Análisis categorial

Para el procesamiento de los datos textuales obtenidos en los grupos focales y las entrevistas se realizó el análisis categorial previsto, lo que permitió examinar críticamente las argumentaciones dadas y buscar su cercanía o correspondencia temática con el cuerpo de conocimientos de la investigación. Así, en la figura 40 se presenta el mapa de codificaciones de las categorías y subcategorías jerárquicas detectadas (sistema de códigos) a partir de las argumentaciones de los participantes alrededor de los resultados cuantitativos asociados a la

seguridad operacional y la perspectiva del potencial de desempeño resiliente de la organización. Las argumentaciones asociadas a los segmentos codificados están desplegadas en el Anexo K.

Mapa de Códigos MAXQDA 2020



Fuente: Elaborado con MAXQDA 2020 (Verbi Software. (2019).

Figura 40. Análisis Cualitativo: Mapeo de la estructura categorial y segmentación codificada

Se aprecia que, en el primer nivel, las categorías con mayor número de segmentos asociados son la baja percepción de seguridad operacional, la gestión de la información, la capacidad para aprender y el clúster de incidentalidad (H2).

En la figura 41 se presenta una nube como representación visual de las codificaciones categoriales realizadas a partir de los textos digitalizados de los grupos focales y las entrevistas personalizadas. El tamaño de la palabra está relacionado con el número de segmentos asociados.

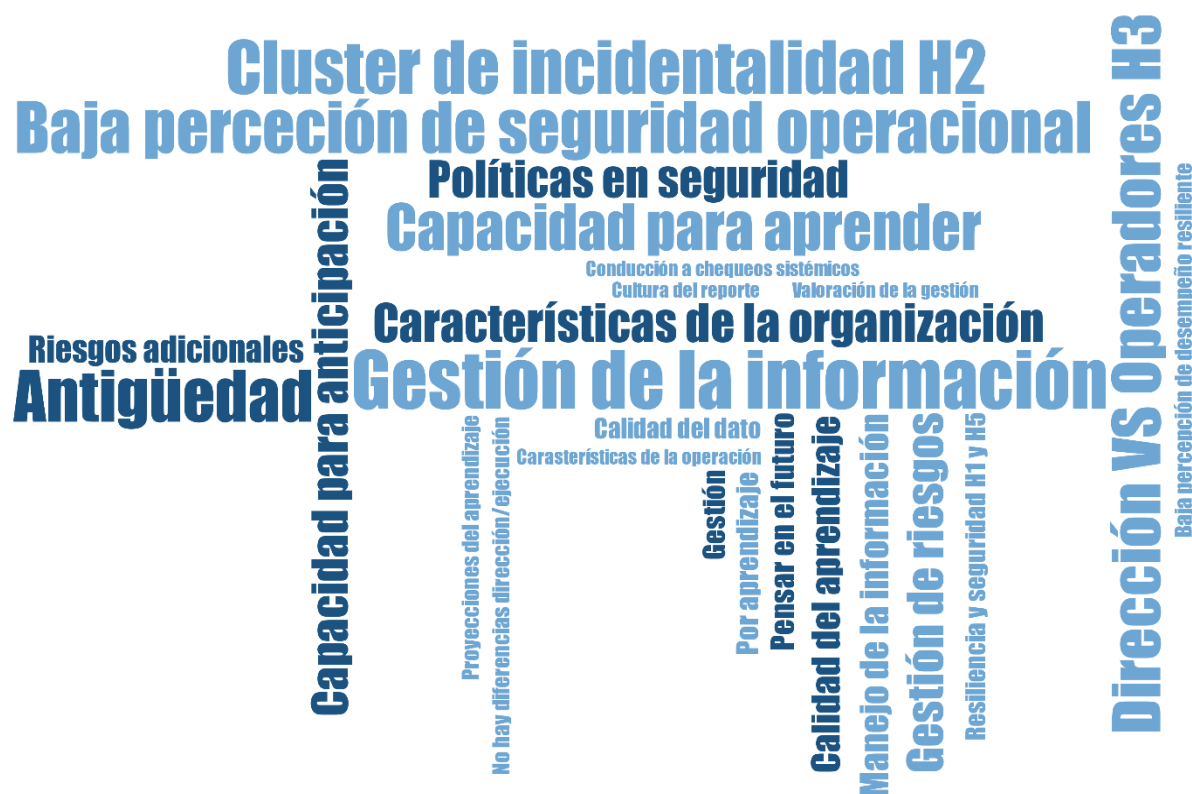


Figura 41. Nube de códigos: Análisis categorial de la visión interpretativa de la seguridad operacional en torno al potencial resiliente

Con el fin de mostrar sistemáticamente los hallazgos cualitativos, seguidamente se presentan las tablas que relacionan categorías (códigos) con posibles configuraciones organizacionales que resultan de un ejercicio inductivo a partir del análisis de los segmentos de las transcripciones asociados a cada código (Anexo K). Adicionalmente, desde un enfoque comprensivo se citan algunos fragmentos de las argumentaciones transcritas.

7.10.2 Configuraciones organizacionales

En la tabla 40 se presenta una aproximación a las configuraciones organizacionales derivadas de las apreciaciones interpretativas explicitadas por los participantes en torno a la percepción del desempeño resiliente y la seguridad operacional.

Tabla 40

Configuraciones organizacionales para el potencial de desempeño resiliente y la seguridad operacional

Código	Resumen – Aproximación a configuraciones organizacionales
Baja percepción del desempeño resiliente	- La organización no ha pensado la seguridad desde el paradigma de la ingeniería de la resiliencia. - No ha desarrollado consciente y sistemáticamente sus capacidades.
Baja percepción de la seguridad operacional	- En cumplimiento a lo establecido por la Unidad Administrativa Especial de Aeronáutica Civil, la organización cuenta con un SMS (Manual de Gestión de Seguridad Operacional), pero este documento está en permanente proceso de actualización y legalización. La difusión de políticas, procedimientos, indicadores y demás contenidos del sistema de seguridad allí establecidos son de conocimiento del personal que dirige las actividades de seguridad, no tanto así para el grupo humano que conforma la organización. - Esto afecta la percepción positiva de la gestión en seguridad, sumado al desconocimiento general sobre las acciones de mejora que tocan la dinámica de la organización. - Este documento (SMS) pretende evidenciar el sistema de gestión de la seguridad, sus elementos e interacciones. Sin embargo, no ha gozado de momentos de estabilidad (puesta en funcionamiento) que le permita evaluar su efectividad y definir hacia dónde dirigir sus mejoras. - Es fundamental abordar la seguridad desde un pensamiento crítico, de permanente logro y mejora, con foco en las concurrencias funcionales y no en los procedimientos e individuos. Esto lleva a la necesidad de reforzar la formación en seguridad de quienes estructuran e implementan medidas. - La organización hace una gestión permanente de la seguridad desde su mirada y con los recursos disponibles, pero se interpone la ausencia de confianza organización-operador y la dificultad para permear toda la organización por su tamaño y complejidad.

Frente a la baja percepción de desempeño resiliente, el nivel gestor de la seguridad operacional plantea que es un reto hacer el trabajo en una organización con amplia variedad de aeronaves, multiplicidad de misiones y, por tanto, riesgos que se asumen dentro de la

operación. Debido a ello, es probable que las personas no valoren de manera positiva la gestión en seguridad operacional o no se perciban claramente las capacidades reales de la organización en términos de seguridad operacional.

Para este grupo, la institución se encuentra en continuo aprendizaje y, por tanto, en posibilidad constante de mejora. Sin embargo, piensan que hay mucho que aprender con el fin de seguir mejorando y que cambiar la manera de la institución de valorar la seguridad - particularmente el nivel estratégico- no es fácil porque un accidente causa que se pierda de vista la gestión y los resultados logrados.

Los participantes de nivel operacional y táctico consideran que es necesario contar con personas idóneas que puedan pensar estratégicamente la seguridad, con dedicación exclusiva a esa tarea. Perciben la existencia de dos prácticas organizacionales derivadas de la cultura propia de una organización militar, en primer lugar, se tiende a designar a personas en cargos críticos sin cuidar el balance con su idoneidad y, en segundo, es probable que la toma de decisiones no contemple un entendimiento sistémico de la organización.

Otro desafío que enfrenta la organización para posicionar la gestión de seguridad operacional tiene que ver con la oportunidad con que realiza y difunde las conclusiones de las investigaciones de eventos, así como la profundidad en sus resultados de modo que sea clara la orientación hacia mejoras sistémicas o funcionales que garanticen el impacto en los resultados.

Es probable que la capacidad de hacer lecturas complejas de la realidad en la que se circunscriben los eventos esté estrechamente relacionada con la formación en seguridad operacional que tengan las personas o equipos humanos que desempeñan la labor de diseño y puesta en funcionamiento de las medidas de seguridad, lo cual se constituye en una importante oportunidad de mejora para la organización.

El reto para quienes se desempeñan en seguridad es generar credibilidad en la gestión en

un ambiente cambiante tanto operacional como administrativamente y generar confianza, a sabiendas que las acciones de seguridad sobre el individuo, en general, no son bien recibidas. Sin embargo, el sistema justifica tomar medidas drásticas porque las acciones causan la pérdida de confianza de la organización en el operador y su toma de decisiones.

Por otra parte, en la tabla 41 se muestra la aproximación comprensiva a configuraciones organizacionales relacionadas con la capacidad de la institución para anticiparse, definida por Hollnagel (2006) como “saber qué esperar” ante la demanda operacional y con la consideración de la experiencia previa.

Tabla 41

Configuraciones organizacionales para capacidad de anticipación

Código	Resumen – Aproximación a configuraciones organizacionales
Capacidad de anticipación	- El sistema de gestión de seguridad operacional contiene tareas clave dirigidas a identificar riesgos en sus ambientes de operación, sin embargo, es un verdadero desafío lograrlo de manera eficaz, así como identificar las amenazas y oportunidades futuras con base en un modelo claro de futuro. Como resultado de esta debilidad, el despliegue de los límites entre las prácticas aceptables y no aceptables, tiene limitaciones. - Hay otras variables exógenas al ambiente operacional, más cercanas al macrosistema en el que opera la organización que afectan significativamente la operación, riesgos de los que el nivel operador desconoce su gestión. - Por último, se identifica que la organización es eminentemente reactiva. A pesar de que la seguridad es considerada un valor organizacional, es decir, hacer parte de la actuación rutinaria de todas las personas, la dinámica organizacional envuelve a las personas en responsabilidades administrativas de diversa complejidad que alejan su atención de la seguridad y las operaciones.

Los participantes de nivel directivo reconocen que el sistema tiene fortalezas en gestionar riesgos, pero igualmente tiene una debilidad importante en su capacidad para identificarlos

oportunamente.

Por su parte, los participantes de nivel operacional identifican limitaciones en la organización para determinar con claridad qué es aceptable y qué no, en términos de riesgo. Su capacidad para identificar y anticiparse a posibles amenazas futuras es otro factor susceptible de mejoramiento.

La antigüedad de la flota, los criterios para la ampliación de su vida útil y los mecanismos organizacionales utilizados para enfrentar esta realidad, los recortes presupuestales, el avance de la aviación en otras organizaciones militares que desarrollan capacidades que antes eran exclusivas de esta, el balance entre administración y operaciones, las políticas de contratación estatal, entre otras situaciones citadas por los participantes, son realidades que identifican claramente como amenazas, pero cuya gestión desde el alto nivel, aún desconocen. Esto les hace pensar que quizá no existe un modelo que propicie la evaluación juiciosa y sistemática de las amenazas y oportunidades futuras y que brinde información pronóstica que les prepare para lo que puede venir.

Sin embargo, el nivel directivo sabe que la organización sí intenta pensar su futuro utilizando estrategias de prospectiva, con una preocupación genuina por ampliar su tecnología y sus capacidades. La limitación surge en un aspecto propio de la cultura castrense y es que la dirección de estos avances y la velocidad de su implementación están sometidos a los criterios de mando del momento, que varían de acuerdo con la realidad del país.

También presentan para consideración un factor de presión que puede constituirse en un riesgo cuya gestión no tienen clara y es el alto compromiso de cada operador por cumplir la misión, incluso por encima de los estándares de seguridad, por cuanto cada operación aérea está directamente vinculada con objetivos de seguridad nacional y apunta a valores subjetivos de alto valor.

Otro aspecto que preocupa a nivel táctico es que la organización ha dirigido sus acciones en

seguridad más a restringir que a evaluar y gestionar riesgos; es decir, las acciones operativas que tienen resultados adversos se restringen, mientras otras organizaciones militares se amplían cada vez más.

Parece que, a futuro, muchas realidades, más que riesgos, se convertirán en limitaciones para la operación segura. Por ejemplo, los recortes presupuestales crean una ambivalencia entre resultados operacionales y cantidad de horas de vuelo disponibles para operar. De otra parte, es necesario mantener el entrenamiento continuado de las tripulaciones lo que reduce el impacto de la operación. Por supuesto, estos recortes afectan también el mantenimiento de las aeronaves y fomenta prácticas que podrían generar riesgos en la operación.

Tabla 42

Configuraciones organizacionales para la capacidad para aprender

Código	Resumen – Aproximación a configuraciones organizacionales
Capacidad para aprender	La Fuerza proyecta convertirse en una comunidad de aprendizaje capaz de transformar datos en información que le permita transformarse. Para ello, su oportunidad de mejora gira alrededor de los siguientes aspectos: - Crear aprendizaje de las cosas que salen bien, no solamente de los eventos adversos. - Filtrar qué tipo de eventos producen aprendizaje valioso para la organización. - Difundir oportunamente el impacto práctico en la seguridad de los reportes que recibe el sistema. - Mantener el nivel de alerta sobre el aprendizaje nuevo.

La institución debe convertirse en una comunidad de aprendizaje, esto significa ser capaz de analizar lo que le pasa, modificarse; pasar de acumular datos a conocer qué le ocurre como sistema para modificar su propio comportamiento.

Básicamente, el aprendizaje solo se recoge de los eventos que salen mal y, por tanto, de eventos que ya han ocurrido. Aunque no es la única fuente de aprendizaje en un sistema

resiliente, desde allí se construyen alertas necesarias para evitar situaciones similares en el futuro. También observan que se ha incrementado la cultura de reporte, incluso de situaciones en las que no ha pasado ningún evento de seguridad, pero que construyen la posibilidad de uno.

Sin embargo, se hace evidente que la cantidad de reportes puede desbordar la capacidad de respuesta del sistema y eso hace que se pierda el aprendizaje. Este incremento puede estar influido por un aspecto cultural en el que la organización valora mejor las unidades que reportan más eventos, por lo que el desafío del sistema está en identificar qué información comporta un verdadero aprendizaje.

Un aspecto que se resalta es que las responsabilidades administrativas disminuyen la capacidad de aprender. Aunque la organización ha emitido políticas al respecto, las personas deben estar en las operaciones y en el funcionamiento administrativo de la organización, pero culturalmente se favorece más lo segundo que lo primero.

Ese desbalance en el que se pueden sacrificar prácticas clave para la seguridad de las operaciones, se torna más crítico en la medida en que las personas avanzan en su desarrollo dentro de la organización, de manera que el tiempo de permanencia en la organización es inversamente proporcional al tiempo en que se está en las operaciones y en la seguridad.

Ahora bien, la capacidad organizacional para aprender está estrechamente vinculado con la gestión de la información. La tabla 43 permite acceder a las interacciones de la organización alrededor de la gestión de información.

Tabla 43

Configuraciones organizacionales para gestión de la información

Código	Resumen – Aproximación a configuraciones organizacionales
Gestión de la información	- La gestión de la información en seguridad operacional necesita ganar velocidad y precisión. Debe plantearse como autónoma, suficiente y crítica

para responder eficientemente a los objetivos de seguridad en la organización.

- Un sistema resiliente debe tener la capacidad de comunicar las conclusiones de los eventos adversos con un índice de oportunidad trazado previamente por el sistema, aspecto que se constituye en un desafío para la organización hoy.
 - La organización, a alto nivel, es consciente de que poseer muchos datos no está directamente relacionado con tener información pertinente y relevante para la seguridad. Debe hacerse evidente tanto el proceso de análisis como el impacto que las acciones han tenido en el mejoramiento de procesos y en la seguridad operacional. Para dar este alcance a la gestión de información, las investigaciones no deben orientarse hacia las personas sino a las funciones e interacciones del sistema.
 - La puesta en marcha de un procedimiento de auditoría al sistema podría permitir su mejoramiento continuo.
 - Es pertinente también que el sistema comprenda que, si en la organización existe temor para reportar, es altamente probable que los reportes no necesariamente constituyan una lectura de la realidad de la organización en términos de seguridad y gestión de riesgo. Esto lleva a la necesidad de revisar críticamente la cultura de seguridad que se ha instalado en todo el sistema.
-

Como conclusión de esta categoría de análisis, se hace evidente que la organización de seguridad debe buscar mayor oportunidad y precisión en la gestión de información, además porque son conscientes de que eso es básico para gestionar la capacidad de aprendizaje del sistema.

Se posee una plataforma de reportes en la que se sube la información de eventos y contiene la data de muchos años y, en ese sentido, se aprecia una mejora sustancial en la recolección de datos; sin embargo, no es tan evidente que haya proceso de análisis de alcance sistémico.

La calidad de los datos es un tema directamente vinculado con la gestión de información y, en este sentido, se hallan importantes oportunidades de mejora. Se trata de establecer los parámetros que permitan determinar si se están recogiendo datos que aportan

significativamente a la seguridad porque, de otra manera, el resultado tampoco va a ser de valor para la gestión.

Se podría pensar en establecer auditorías al sistema de información, construir estándares, unificar criterios, entre otras actividades que aseguren que las clasificaciones y conclusiones plasmadas en los reportes responden a un parámetro organizacional.

Lo relevante es lograr que la gestión de la información permita un chequeo del sistema de seguridad operacional en su conjunto y proporcione comprobaciones regulares sobre procesos organizativos de alto nivel que evidencien un entendimiento sistémico de la organización, trascendiendo el lenguaje de los factores humanos y factores técnicos.

Aunque es claro que el subsistema de reportes no es la única fuente de información para el sistema de seguridad, también lo es que el funcionamiento óptimo de este mecanismo depende de que en la organización haya una cultura de accesibilidad estable (sostenida en el tiempo) que garantice el acceso a la información de seguridad. Las personas deben sentir confianza en el sistema en el contexto de una cultura de seguridad percibida como equilibrada y objetiva en la que las medidas preventivas sean imparciales y predecibles.

Con respecto a las apreciaciones de los participantes sobre los hallazgos presentados en la hipótesis 2, se indagó por los posibles argumentos comprensivos que permitieran entender las razones por las cuales las unidades con menor incidentalidad presentaron mayor percepción de potencial de desempeño resiliente y seguridad operacional e inversamente.

Tabla 44

Configuraciones organizacionales para las diferencias por clúster de incidentalidad

Código	Resumen – Aproximación a configuraciones organizacionales
PoDeRe y SegOp	A juicio de los participantes, varias lógicas institucionales dan cuenta del hallazgo de la hipótesis 2.
por clúster de	- Por un lado, encuentran una relación entre mayor percepción de PoDeRe y

incidentalidad (H2)	SegOp en unidades con mayor incidentalidad basados en el factor aprendizaje: los eventos adversos generan aprendizaje, aunque existe el riesgo sea de corto plazo. - Parten de la premisa de que existen personas que no requieren que pase algo para que cuiden sus parámetros de seguridad. Sin embargo, la ocurrencia de un evento adverso evidencia el funcionamiento del sistema y esto puede contribuir a percibir mayor seguridad operacional. - La política institucional de “cultura justa”, que se aplica cuando ocurre un evento, también puede contribuir a incrementar la percepción de seguridad por cuanto se toman acciones y medidas preventivas que contribuyen a encauzar el desempeño en el personal operativo, cuando menos de manera transitoria.
--------------------------------	---

Los eventos, adversos o no, conllevan en sí mismos aprendizaje para las personas y para el sistema. Sin embargo, todas las personas no alcanzan el mismo nivel y profundidad en esa capacidad de aprender por lo que es función del sistema encontrar los mecanismos que permitan unificar y asegurar las lecciones aprendidas con el fin de que no se conviertan tan solo en un incremento temporal de la alerta (aprendizaje de corto plazo) sino en una respuesta consistente y coherente frente a la percepción del riesgo.

Clásicamente en la historia de la aviación, se conoce que los accidentes son repetitivos. Es poco probable que se presente una situación totalmente nueva. Por eso es vital preguntarse acerca de las razones por las cuales el evento vuelve a suceder ya que, implícitamente, esto evidencia que el aprendizaje no se ha dado o no se ha transmitido en todos los niveles de la organización como debería hacerse para pensar en características de resiliencia del sistema.

La organización opera en un entorno y macroentorno con múltiples variables intervinientes. Las personas rotan con alguna frecuencia por las diversas unidades organizacionales y esto plantea el reto de plasmar las mejoras del sistema de seguridad operacional en mecanismos que garanticen su permanencia en el tiempo y su correcta difusión y actualización.

De otra parte, es importante plantear que la gestión de la seguridad operacional en la

organización se da desde la creencia de que hay individuos que son intrínsecamente seguros que no requieren un evento negativo para tener presentes los parámetros de seguridad durante las operaciones, pero hay otros que no lo son quizá respaldados en un sentimiento de invulnerabilidad. Para el nivel directivo, son estos últimos los que pueden presentar una más baja percepción de seguridad operacional.

Se evidencia con consistencia en los participantes de todos los niveles de la organización, la idea de que vivir eventos adversos incrementa el nivel de preocupación por la seguridad en las operaciones.

Otra lógica organizacional que puede explicar estos resultados es que cuando ocurre un evento, es más probable que las personas perciban cómo toda la dinámica organizacional entra a actuar en función del manejo del evento. Si no ocurre un evento adverso, las personas pueden saber que el sistema está ahí pero no ven cómo se manifiesta, por tanto, es posible que frente a la mayor incidentalidad haya más conciencia porque se puede apreciar la interacción de todos los elementos del sistema de seguridad.

La información cualitativa también arrojó, que, al tratarse (la seguridad) de una política del alto mando y un valor de la organización, responde en mucho a las políticas que cada mando imprime al manejo de la gestión de la seguridad operacional. Si la política es responsabilizar a las personas de sus acciones o inacciones, el desafío del equipo que gestiona directamente la seguridad, a su juicio, está en evitar que esta manera de intervenir no sea vivida como punitiva por las personas en la organización.

Para lograr esto y tener un criterio claro de decisión, la organización creó un procedimiento que llama “cultura justa”, orientado a que esa imputación de responsabilidad se dirija a aquellas personas que cometan violaciones o faltas muy extremas. Sin embargo, son conscientes de que hay una afectación negativa real a la percepción de seguridad a la que se suma que la capacidad para divulgar las acciones preventivas de orientación sistémica adoptadas por la organización,

es muy limitada.

Por este desconocimiento y debido a que las personas están en contacto con las decisiones en materia de seguridad que pueden percibir a su nivel, el procedimiento de cultura justa es vivido como eminentemente sancionatorio, no como una acción correctiva sobre procedimientos, riesgos o variables susceptibles de mejorarse.

La organización también tiene una oportunidad de mejora en la equidad con la que se aplican los procedimientos de seguridad previamente establecidos, por cuanto es posible que las decisiones (medidas preventivas y correctivas) tomadas ante un evento adverso por un cuerpo colegiado (junta de seguridad) que ha estudiado de manera juiciosa la situación, queden sometidas a criterio de una persona que puede o no, validar la decisión.

Cuando no se sigue la recomendación del grupo de expertos, se da un mensaje de ambigüedad que no fortalece la percepción de seguridad.

Las acciones tomadas como resultado de la puesta en funcionamiento del sistema de seguridad deben redundar en un claro mejoramiento de la organización, sus procesos, procedimientos, funciones, interacciones, acuerdos operacionales y demás elementos que interactúan dentro del ambiente operacional.

Pasando a otro tema, la hipótesis 3, que planteaba la existencia de diferencias significativas en la percepción de percepción de desempeño resiliente y seguridad operacional entre el grupo responsable de dirigir las operaciones y quienes las conducen, no fue confirmada.

Sin embargo, los participantes encontraron sentido en este hallazgo dentro de la dinámica la organización. También identificaron una narrativa institucional frente al hallazgo que relaciona la percepción de desempeño resiliente y seguridad operacional desde la antigüedad militar. La tabla 45 presenta las posibles configuraciones organizacionales para este hallazgo.

Tabla 45

Configuraciones organizacionales para las capacidades de Dirección vs. Operadores: Comparación por antigüedad militar.

Código	Resumen – Aproximación a configuraciones organizacionales
Dirección vs. Operadores: Comparación por antigüedad militar. Análisis Complementario	Varias lógicas institucionales dan cuenta de la hipótesis 3 y complementarias: - Quienes diseñan y dirigen las operaciones, también son operadores y esto podría explicar que no se presenten diferencias significativas entre los dos grupos. Frente a la hipótesis 3 complementaria que arroja una mayor percepción de seguridad en los grupos de menor tiempo en la organización, baja en los de antigüedad intermedia y media en los de mayor antigüedad, aparecen la siguiente argumentación: - Las personas de menor antigüedad militar no han experimentado la complejidad de la operación y sus riesgos inherentes por lo que pueden percibir mayor seguridad operacional. Los de antigüedad intermedia, pueden percibir mayor probabilidad de que algo pueda ocurrir, lo cual disminuye su percepción de seguridad. Los oficiales de mayor antigüedad se encuentran más al frente de tareas administrativas que operativas por lo cual su percepción de seguridad operacional puede ser de nivel medio.

Hay un consenso entre los participantes sobre la no existencia de diferencias significativas entre los niveles operador y diseñador de operaciones por cuanto, en la realidad de la organización, todas las personas que diseñan y dirigen las operaciones han participado en ellas o participan en ellas, en tiempo real.

Para asegurar este hallazgo, la investigadora realizó una comparación en tres grupos por tiempo de experiencia en la aviación que está directamente relacionado con el tiempo de permanencia en la organización y el grado. Allí se encontró que el grupo de menor antigüedad tiene mayor percepción de resiliencia y seguridad. El de antigüedad intermedia tiene una percepción baja de estas variables y los de mayor tiempo, están en valores intermedios.

Es probable que esto obedezca al nivel de criticidad que pueden interpretar las personas de

acuerdo a su antigüedad en la organización, de modo que quienes llevan menor tiempo en la organización tiene un menor sustrato experiencial que aquellos que llevan más tiempo.

El grupo de antigüedad intermedia (entre 10 y 15 años) puede percibir menor resiliencia y seguridad debido a que han transitado en la organización viviendo directamente situaciones riesgosas y eventos adversos, razón por la cual pueden llegar a pensar que es posible que pase algo no deseado en medio de un ambiente no controlado y con variables externas que no pueden cambiar. Su ubicación dentro de la organización les permite tener una lectura de lo que pasa abajo y encima de ellos y esto puede incrementar su percepción de falencias organizacionales.

Las personas más antiguas, pueden ubicarse en una valoración media debido a que por su grado militar ya no están involucradas tan directamente en las operaciones, pero conocen que existen vacíos en el sistema. Sin embargo, han visto las trasformaciones de la organización y la seguridad y saben que se ha ganado terreno para generar condiciones de operación más seguras.

De otra parte, el hallazgo puede tener también relación con la conciencia que van adquiriendo las personas sobre la complejidad de la operación a medida que avanzan en su permanencia. Esto va de la mano con el conocimiento de la institución y su funcionamiento.

Desde el entendimiento de los participantes, la antigüedad en la organización otorga también otra lectura desde la formación y contacto directo con la seguridad. Las personas recién incorporadas entran a formar parte de un sistema que tiene incorporada la seguridad y pueden percibir su presencia permanente en el ambiente operacional. Los de antigüedad intermedia, han hecho parte de las transformaciones y pueden reconocer cuando algo es nuevo dentro del sistema. Los más antiguos, tienen su foco concentrado en el tema administrativo y su proyección de carrera, pero son conscientes de los desafíos que están vigentes en la organización.

En este momento, la seguridad es una cultura consciente en las personas que puede ser más

o menos visible de acuerdo con el momento de vida de la persona dentro de la organización y su propio grado de exposición al riesgo. Es probable que los menos antiguos no sean tan conscientes de las implicaciones de las cosas, mientras los más antiguos pueden centrarse en conceptualizar de acuerdo a como ven las cosas a su nivel. Los intermedios ven cómo funciona la institución y las dificultades provenientes de los niveles organizacionales ubicados arriba y debajo de ellos.

Aquí vuelve a cobrar importancia el hecho de que los menos antiguos están más conectados con el ambiente operacional y es probable que eso les permita ver lo que está bien o lo que es susceptible de mejorar. Los más antiguos tienen más experiencia, pero otra visión de las cosas porque están inmersos en otras tareas propias de la organización.

Para terminar, se presentan las apreciaciones de los participantes sobre las hipótesis 1 y 4, que establecen la estrecha relación entre las variables potencial de desempeño resiliente y seguridad, además de las ecuaciones predictivas que especifican el nivel de predicción de la primera sobre la segunda.

Tabla 46

Configuraciones organizacionales para resiliencia y seguridad

Código	Resumen – Aproximación a configuraciones organizacionales
Resiliencia y seguridad (H1 y H4)	- La alta correlación entre la variable potencial de desempeño resiliente y seguridad operacional no suscitó mayores comentarios por el desconocimiento del concepto. - Los escenarios presentados como función predictiva corresponden, según los participantes, a observaciones ya conocidas por ellos, pero la investigación les permite precisar acciones de seguridad sobre funciones específicas de la organización.

Por último, referente a la hipótesis 1 y 4 que muestra la alta correlación y relación predictiva de las variables seguridad operacional y potencial de desempeño resiliente, el grupo

responsable de la gestión de la seguridad considera fundamental fortalecer la capacidad de identificar riesgos de manera que le permita al sistema anticiparse y dar respuesta eficaz a los cambios del entorno.

Entre más capacidad de anticipación se adquiera como institución, mejores van a ser los resultados en seguridad. Al presentar los hallazgos predictivos en ecuaciones específicas del potencial de desempeño resiliente, se concluye que los resultados arrojan datos empíricos de cosas que conocían más por intuición, lo cual les permite enfocar sus esfuerzos para mejorar la seguridad.

Los otros participantes no opinaron respecto de las hipótesis centrales de investigación, por tratarse de información nueva para ellos. En general, consideraron un interesante aporte el poder precisar las acciones de seguridad sobre funciones específicas de la organización.

Hasta aquí, las dinámicas organizacionales que se convierten en desafíos para la organización en la búsqueda de fortalecer su potencial de desempeño resiliente como camino expedito para mejorar la seguridad operacional.

7.11 Re-análisis de la Potencia (*power*)

Finalmente, como estaba previsto en el diseño muestral (pág. 82; figura 13), se calculó el nivel de potencia (*power*) resultante del estudio luego de realizar la aplicación a la muestra final.

Se había presupuestado una potencia de 0,80, bajo una significancia alfa de 0,05, con hipótesis unilateral, y un estimador poblacional de $\gamma > 0,5$ (hipótesis alternativa) de la correlación entre potencial de desempeño resiliente y seguridad operacional, que para el efecto los datos arrojaron que la correlación real obtenida fue de $r=0.962$ ($p<0,001$) y con ello recalculando con el software “Tamaño de la Muestra” versión 1.1 (Pérez, et al. 2001) el nivel de potencia final queda estimado en 1,0 (figura 43).

Prueba de hipótesis para el coeficiente de correlación

Toma de datos

-Error tipo I: .05

Tamaño muestra: 545

-Coef. correlación poblacional: .962

-Valor de prueba en la hipótesis nula: .5

Calcular... Cerrar

Resultados

Poder: 1

Tipo de cálculo

☒ 1 Cola ☐ 2 Colas

☐ Tamaño muestra ☒ Poder

Fuente: Elaborada con aplicativo de software Tamaño de la Muestra. v.1.1 (Pérez et al. 2001).

Figura 42. Re-cálculo de la potencia (*power*) de la investigación

Con esto estadísticamente se garantiza que la significancia de las pruebas de hipótesis de las correlaciones supera significativamente lo esperado y por demás indican un alto nivel de tamaño de efecto, con buen nivel de validez externa y validez estadística (Kerlinger y Lee, 2002; Suárez, 2015; Vera, 2018), indicando que en el estudio se estima una baja probabilidad de presentar el Error I (falso positivo) o en el Error II (falso negativo) (Pérez et al., 2001), siendo un soporte válido para las hipótesis sometidas a prueba.

Discusión

Capítulo

8. Discusión

En este capítulo se presentan los hallazgos arrojados por la investigación en diálogo crítico y constructivo con los principales presupuestos teóricos y las realidades develadas en la fase cualitativa de la investigación.

8.1 De la Relación entre Potencial de Desempeño Resiliente y Seguridad Operacional. (Hipótesis 1 y 4).

El concepto de resiliencia y la ingeniería de organizaciones para desarrollar el potencial de desempeño resiliente surge ante la necesidad de generar una ruptura epistemológica en el ámbito de la seguridad operacional y sus estrategias de gestión. Sin embargo, esta asociación entre resiliencia y seguridad no aparece tan clara cuando se mira la seguridad desde las estadísticas de eventos adversos que enfrenta una organización de alto riesgo.

Algo similar encontraron Hale y Heijer (2006), quienes midieron aspectos de seguridad asociados a falta de resiliencia en un sistema de transporte masivo distinto a la aviación y encontraron que el sistema tenía baja resiliencia, pero sus niveles de seguridad eran altos en ciertas áreas, lo que pareciera mostrar cierta independencia entre resiliencia y seguridad cuando se mira esta última como ausencia de eventos no deseados.

Por esto, el objetivo de esta investigación fue establecer una relación entre estas dos variables, abordando la resiliencia desde la propuesta de Holnagel (2009) quien propone la existencia de cuatro capacidades fundamentales de una organización resiliente: capacidad para responder, monitorear, aprender y anticipar. La seguridad operacional, por su parte, fue abordada desde la perspectiva de Reason (2010) que aleja el foco de las estadísticas de eventos y accede a la seguridad como un fenómeno sistémico resultado de la interacción entre procesos y funciones.

La resiliencia es una condición intrínseca de un sistema que emerge cuando es retado a

operar en condiciones no contempladas en el diseño original de sus operaciones o cuando la condición que enfrenta, supera sus capacidades (Herrera, 2016). En ese orden, el alcance de la investigación fue diagnosticar el sistema en términos de sus capacidades resilientes, utilizando la propuesta de Hollnagel (2014).

Al realizar el análisis correlacional se encontró que había una alta correlación entre el potencial de desempeño resiliente y la seguridad operacional, por lo que se procedió a desarrollar análisis multivariantes que permitieran ajustar ecuaciones predictivas, como modelamientos aplicables a la estimación de la seguridad operacional.

En la medición de potencial de desempeño resiliente, la organización obtuvo un puntaje medio bajo. Sus oportunidades de mejora se ubicaron en la capacidad para anticipar y su fortaleza está en la capacidad de monitorear específicamente en el escenario de ejecución de operaciones de mantenimiento, vuelo y entrenamiento.

Esto significa que si bien se cuenta con indicadores claros que le permite conocer cómo está funcionando, su reto está en afianzar una cultura que anime a pensar en el futuro, identificar y evaluar amenazas y oportunidades futuras, comunicar eficazmente las expectativas de la organización, diseñar y popularizar el modelo de futuro articulado a la estrategia, divulgar el nivel de riesgo considerado aceptable, así como los límites que establecen esta aceptabilidad.

El orden de la valoración de las cuatro capacidades del potencial de desempeño resiliente de acuerdo con su favorabilidad, está en el siguiente orden: capacidad de monitorear $71,7 \pm 17,4$; capacidad de responder $70,9 \pm 17,5$; capacidad de aprender $68,9 \pm 17,8$ y capacidad de anticipar $65,3 \pm 21,0$. Sin embargo, las cuatro capacidades tuvieron puntajes medio bajos, lo que significa que la organización debe trabajar en los procesos y funciones que fortalecen su potencial de desempeño resiliente.

En este sentido, se podría afirmar que la organización tiene un potencial moderado (no alto, no bajo) para reaccionar y adaptarse ante perturbaciones imprevistas que desafían la estructura

del sistema y generan inestabilidad en su funcionamiento. Particularmente, un sistema que no se proyecta al futuro y no evalúa sus riesgos, tampoco puede prepararse para responder efectivamente a cambios en el entorno de operación y esta lentitud en la respuesta, afecta su capacidad adaptativa (Dekker, 2006).

Zipkin et al (2006), plantean claramente que un sistema es resiliente cuando sus mecanismos de control le permiten responder adecuadamente a riesgos previamente identificados, antes de que se conviertan en amenazas para su funcionamiento, de manera que este hallazgo es una importante oportunidad para la organización.

La evaluación de riesgo para un sistema resiliente debe superar la primera línea de operación, debe darle al sistema la posibilidad de ubicarse no sólo en lo inmediato, sino también en el medio y largo plazo (Dallat, et al. 2017). Los participantes de la fase cualitativa planteaban temas como la reducción presupuestal, la competencia de mercado (otras organizaciones militares haciendo lo mismo), la reducción de personal, entre otras, como amenazas a la estabilidad del sistema cuyo modelo de afrontamiento, si existe, desconocen.

Al revisar la concentración de respuestas de los participantes en las categorías alta, media o baja valoración, se observa que en categoría de baja percepción de resiliencia se agrupó el 44,4% de personas; en media, el 37,0% y en alta, el 18,6%. La subescala con mayor concentración en calificación baja fue la capacidad institucional para aprender con 46,0% de participantes, lo que evidencia que las personas ven la necesidad de identificar los eventos de seguridad operacional de los que se produce aprendizaje organizacional, generar aprendizaje permanente basado en los éxitos y no sólo en las fallas, disponer recursos para el aprendizaje y evidenciar las lecciones aprendidas en mejoras a procesos y funciones de la organización.

En la fase cualitativa, los participantes reconocen la necesidad de fortalecer este aspecto, pues hasta hoy la efectividad del sistema de seguridad se evalúa con base en indicadores de accidentes, de manera que un evento adverso significa que no se está haciendo la tarea de

manera adecuada. No identifican la presencia de alguna práctica organizacional que permita valorar lo que se hace bien y, menos, recoger aprendizaje desde esa óptica (Woods y Hollnagel, 2006).

En cuanto a concentración de respuestas por categoría, resalta como una fortaleza de la organización la capacidad de monitorear, es decir, que hay mayor percepción de la existencia de indicadores de rendimiento que permiten saber cómo se están haciendo las cosas en seguridad y esos indicadores son verificados y revisados con regularidad.

En cuanto a la percepción de seguridad operacional, se obtuvo una valoración general medio baja de $68,2 \pm 16,3$. El componente con mayor valoración fue el de gestión de la seguridad y operaciones con el $71,5 \pm 17,2$, lo que indica que, aunque hay oportunidad de mejora, la institución posee moderados recursos instrumentales que le permiten ser flexible frente a los cambios institucionales y del entorno, tener en cuenta las políticas de seguridad en su toma de decisiones, brindar soporte logístico oportuno y eficaz a las operaciones, priorizar el entrenamiento del personal operativo, hacer un adecuado equilibrio entre protección (seguridad) y producción (operaciones), contar con procedimientos estandarizados, poseer un nivel de supervisión entrenado y estandarizado e indicadores que mejoran los procesos de la institución.

El componente con menor valoración general es el de seguridad, $66,1 \pm 14,9$, que está compuesto por dos subescalas, a saber: compromiso y gestión de la información. En este caso, solo la subescala de gestión de la información evidencia oportunidades de mejora y compromiso es una de las escalas con mayor puntuación, $72,2 \pm 18,7$.

Así las cosas, se puede afirmar que la organización trabaja con moderada firmeza en ser un modelo en el sector en buenas prácticas de seguridad, toma decisiones que demuestren un genuino interés por la seguridad, aporta los recursos técnicos, humanos y presupuestales idóneos para la gestión de la seguridad y genera acciones que refuerzan las defensas del

sistema.

La gestión de información, por su parte, obtuvo la más baja calificación $61,2 \pm 13,7$, y plantea la necesidad de evaluar la pertinencia de la información y conclusiones que emite el sistema, su capacidad para proporcionar chequeos regulares sobre procesos organizativos, la oportunidad en la difusión tanto de los resultados de las investigaciones de eventos como de los peligros que amenazan las operaciones y si este manejo de información señalaba solo a los operadores de primera línea como responsables de los eventos adversos.

Convertir datos en información no es tarea fácil. Hollnagel (1993, como se cita en Dijkstra, 2006) plantea que en el análisis de información es usual confundir hechos con causas porque el fenotipo -que correspondería a los hechos, lo que ocurrió- se confunde con el genotipo o conjunto de factores que lo producen. Las repercusiones de esta debilidad de un sistema se dan sobre la generación de información útil en la identificación de amenazas o para el mejoramiento de procesos y prácticas organizacionales.

Las personas en la organización reconocen que se ha fomentado una cultura de reporte, pero también que existe miedo para informar. Es importante darle una lectura más profunda a este aspecto que resulta vital para la salud del sistema de seguridad operacional e indagar si existe realmente una cultura que informa en la institución, en términos de Reason (2010), una organización que moviliza a las personas a reportar lo pertinente, que cuida la confidencialidad y cuya generación de resultados es accesible, oportuna, útil y confiable.

Llama la atención que, en la escala total de seguridad operacional, el 49,2% de los participantes tiene una baja percepción, lo que podría indicar que el sistema presenta un bajo nivel de seguridad operacional. En cuanto a los componentes, el que agrupó la mayor parte de puntuaciones bajas fue el de seguridad (65,2%), seguido de cultura de seguridad (49,9%) y gestión de la seguridad y operaciones (40%).

En las subescalas, las que presentan mayor concentración de puntuaciones bajas son gestión

de la información (79,4%) y la subescala del componente de cultura de seguridad, accesibilidad (63,2%). Esta subescala medía la sencillez y amigabilidad de la estructura de informe de riesgos; la confianza de las personas en la institución para informar riesgos; la independencia de las entidades encargadas de investigar de aquellas que imparten acciones correctivas; la rapidez, utilidad, accesibilidad y pertinencia de la retroalimentación y la capacidad de los informes para mostrar factores locales y organizativos que promueven errores.

En cuanto a la relación que se buscaba establecer entre potencial de desempeño resiliente y seguridad operacional, se encontró que no solamente hay una correlación clara, sino que esta relación es de tipo causal, de manera que estadísticamente se crea una función predictiva de la seguridad operacional a partir del potencial de desempeño resiliente.

Esa función predictiva se planteó a partir de dos estadísticos que, en últimas, arrojan evidencia de que, trabajando capacidades específicas de la resiliencia, se afecta positivamente la seguridad operacional al interior de la organización.

8.2 De la Relación del Potencial de Desempeño Resiliente y la Seguridad Operacional con otras Variables de Estudio. (Hipótesis 2, 3 y complementarias).

El estudio buscó establecer la posible relación de potencial de desempeño resiliente y seguridad operacional con dos variables organizacionales: los clúster de incidentalidad y el nivel de participación operacional.

A pesar de que tener o no eventos adversos no define la seguridad del sistema, se realizó una comparación entre unidades organizacionales agrupadas por estadísticas de incidentalidad (hipótesis 2). La hipótesis investigativa dirigía a esperar que las agrupaciones que habían sufrido mayor cantidad de eventos adversos tuviesen menos potencial de desempeño resiliente y percepción de seguridad operacional.

Sin embargo, las pruebas estadísticas llevaron a aceptar la existencia de diferencias, por cuanto el hallazgo fue que se encontraron diferencias significativas entre clúster de alta e

intermedia incidentalidad en las subescalas de capacidad para responder en el escenario 2 (entrenamiento), capacidad para monitoreo en el escenario 2 (entrenamiento) y 3 (supervisión) y en la escala total. Este grupo es el que percibe mayores niveles de resiliencia y de seguridad operacional.

Adicionalmente, las dimensiones de capacidad para monitorear y la escala general de resiliencia están asociadas por variabilidad explicada significativa, lo que significa que sí hay una relación directa.

En la fase cualitativa, se estableció como argumento comprensivo de este hallazgo el hecho de que la ocurrencia de eventos mantiene, de alguna manera, un sano nivel de alerta y las personas pueden ser más conscientes del sistema de seguridad y su interacción con las operaciones.

La otra variable estudiada responde al planteamiento teórico de la brecha que existe entre trabajo diseñado y trabajo real (Leplat y Hoc, 2005). Para establecer esta comparación y evaluar el comportamiento de las variables en medición, se agruparon los sujetos por nivel de participación operacional (hipótesis 3).

Sin embargo, se aceptó la hipótesis de nula por cuanto no se encontraron diferencias significativas entre los dos grupos. Para los participantes de la fase cualitativa, el factor que más puede explicar este hallazgo es el hecho de que no parece haber una división real entre quienes diseñan y quienes ejecutan. Las operaciones son autorizadas por el nivel operacional, pero es el comandante de la aeronave el que planea, diseña y ejecuta la operación.

La organización goza de una particularidad y es que, en todos los rangos jerárquicos (a excepción de generales), las personas son operadores de primera línea. Incluso las personas responsables de la gestión de la seguridad y de las operaciones, son pilotos activos de la organización.

Para profundizar en la posibilidad de probar esta hipótesis se realizó una comparación

alterna entre tres grupos de participantes de acuerdo con su tiempo de permanencia en la institución. Allí se encontró que las personas con menor tiempo de permanencia percibían mayor resiliencia y seguridad; quienes estaban en el rango medio de permanencia, percibían menor resiliencia y seguridad; las personas con mayor tiempo de permanencia se ubicaron en el intermedio.

El argumento que justifica esta comparación es que las personas con menor tiempo de permanencia e intermedio habitualmente están más vinculadas a la operación que las que tienen mayor tiempo de permanencia en donde se privilegian las tareas administrativas. Las diferencias observadas se pueden explicar justamente en función del grado de permanencia en las operaciones porque quienes están más vinculados al ámbito de las operaciones pueden acercarse más al sistema de seguridad y captar las capacidades organizacionales reales.

Los intermedios tienden a ser más críticos porque han madurado su experiencia y se hacen más conscientes de las oportunidades de mejora del sistema, mientras que los más antiguos normalizan el sistema y sus debilidades debido a que cambian el foco de atención hacia las responsabilidades administrativas y su proyección personal de la organización.

8.3 De los Hallazgos Derivados del Diseño

En el estudio participaron 545 individuos, pilotos activos de la organización de los tres rangos jerárquicos establecidos para el estudio y en su distribución se aprecia el carácter piramidal de la organización. También vale la pena destacar que, en términos de operación aérea, ningún piloto -independiente de su jerarquía- pertenece al nivel estratégico, sino que vuela para una unidad operacional o táctica.

En este sentido, el nivel estratégico es eminentemente administrativo y esto puede verse reflejado en la distribución.

El tamaño de la muestra revela que la investigación gozó del respaldo de la alta dirección institucional y permite suponer una buena disposición organizacional para leerse a sí misma

desde otra perspectiva y adoptar conceptos nuevos dentro de su gestión.

El proyecto de investigación planteó la realización de un estudio mixto que mezcló metodologías cuantitativos y cualitativos en su desarrollo. Esto se considera una fortaleza del estudio porque si bien la aplicación de instrumentos agiliza las mediciones y la toma de decisiones también es poco probable que en materia de seguridad operacional sea posible generalizar los resultados, debido a que están circunscritos a la organización, su entorno y el core de su negocio por lo que es legítimo que sean entendidos a partir de las realidades de los participantes.

La seguridad debe ser gestionada en el día a día y, por tratarse de un constructo teórico de carácter intangible que se visibiliza a través de los eventos no deseados, requiere de un trabajo sistemático y sistémico.

De otra parte, un análisis particular lo amerita la frecuencia de respuesta de “no sabe, no conoce” que se obtuvo en las dos escalas aplicadas tanto de potencial de desempeño resiliente como de seguridad operacional. De hecho, en la escala PoDeRe solo el 80,6% de los pilotos dieron respuesta completa a la prueba y el 7,3% dejaron 6 o más preguntas en “no sabe, no conoce”. En la escala de seguridad operacional fueron el 79,1% y el 4,0% respectivamente, quedando un aproximado del 20% con respuestas incompletas.

Si bien no se tiene evidencia sobre las motivaciones personales para dejar respuestas en “no sabe, no conoce”, dado que los ítems no se refieren a aspectos reservados de la organización ni privados de los individuos y que, por demás, los pilotos son agentes de seguridad operacional así como también comportan la actitud resiliente de la organización, en estricto no les sería permisible estar en condición de “no saber”, lo que podría llegar a convertirse en un riesgo potencial al indicar un desconocimiento de condiciones operacionales que deberían ser de su dominio experto y su falencia podría redundar en resultados adversos dentro del funcionamiento de la organización.

Como anteriormente se mencionó, los “no sabe, no conoce” y las no respuestas también podrían ser el enmascaramiento de una conducta de reserva, un no-comprometerse con las opciones de respuesta o la percepción de una cultura punitiva en materia de seguridad.

Así entonces, la institución tendría en ello un foco de atención para un accionar preventivo a través de potenciar la suficiencia del componente humano como gestor del potencial de desempeño resiliente organizacional que finalmente redundará en el nivel de seguridad operacional en las actividades militares.

No obstante, el nivel de respuesta de “no sabe, no conoce” como opción evitativa de una respuesta explícita, podría estar indicando una actitud de reserva de los pilotos al no querer comprometerse con una respuesta direccionada. En esta escala sería más severo si llegare a ser desconocimiento de condiciones de la seguridad operacional de la organización. La organización no puede pasar por alto la previsión de una oportunidad de mejoramiento al potenciar la seguridad operacional vía fortalecimiento de la resiliencia institucional centrada en la conducta del personal de vuelo.

8.4 Discusión Final

Para focalizar la discusión final se tomó como pretexto algunos de los indicadores planteados por Woods (2006) que evidencian aspectos de la seguridad que caracterizan la falta de resiliencia y que son signos para diagnosticar el nivel de seguridad. A estos indicadores se integran los hallazgos de la investigación.

En todos los niveles de la organización se considera que hay un esfuerzo sistemático por equilibrar los objetivos de seguridad y los de producción de operaciones; sin embargo, el nivel operacional y táctico ve que en las decisiones cotidianas priman las operaciones sobre la seguridad, incluso con defensas deterioradas.

La gestión de la seguridad está focalizada en la solución de situaciones riesgosas puntuales de modo que las personas no reconocen un modelo global de control de riesgo o el sistema

como tal, muchas veces solamente saben que deben cumplir tareas. La ocurrencia de eventos adversos les permite ser conscientes de algunas fortalezas de la organización, pero no logran una visión integrada de la seguridad del sistema en todos sus componentes.

En cuanto a las recomendaciones, la investigación identifica oportunidades de mejora en el sistema de seguridad a partir de la intervención en capacidades resilientes, así: capacidad de anticipar, capacidad de monitorear en el escenario de supervisión de operaciones, capacidad de aprender y capacidad de responder en el escenario del entrenamiento. La regresión logística incluye también la capacidad de respuesta en el escenario de supervisión, la capacidad de monitorear en el escenario de entrenamiento.

Para poder lograr esta mejora, la organización requiere el diseño y puesta en funcionamiento de un modelo de gestión de la seguridad operacional basado en la resiliencia, ya con la certeza de que la mejora en cualquiera de sus capacidades va a afectar positivamente la seguridad.

La gestión de información es otro aspecto clave para mejorar. Según sugiere Woods (2006), las evaluaciones de riesgo deberían ser sometidas a una revisión apropiada con base en la nueva información que ingresa al sistema. Si esta información no ingresa, el sistema puede ser rígido y no incluir la comparación de los riesgos en los diferentes componentes, lo que indica que las prioridades no están totalmente abiertas a la reflexión sobre los riesgos.

Se recomienda la revisión del actual sistema de información para lograr agilidad, claridad conceptual y precisión. El modelo HFACS no estaría en línea con un modelo pensado desde el paradigma sistémico, pero, más que eso, la enorme complejidad que representa como herramienta para la investigación de eventos tal y como fue diseñado por la organización, se hizo evidente al hallar un grado importante de ambigüedad conceptual y criterio subjetivo en la descripción de eventos y en la determinación de causas, así como errores en la clasificación.

Este hecho cuestiona la calidad de la información manejada hasta hoy como entrada

fundamental de la gestión de la seguridad, su mejoramiento continuo y el aprendizaje organizacional.

De otra parte, es evidente que las operaciones aéreas sean el núcleo del negocio para este tipo de organizaciones y que, por tanto, este sea el foco de sus decisiones. Sin embargo, la organización hace un esfuerzo importante por equilibrar su operación con la seguridad y esto se constituye en una gran fortaleza para ser explotada a favor de un equilibrio más funcional de manera que no parezca que el compromiso con la seguridad sea casi de carácter nominal y evitar que las decisiones rutinarias generen tensiones y riesgos al interior del sistema.

Una seguridad que se activa frente a la ocurrencia de eventos y busca responsables en la primera línea de operación evidencia un sistema en proceso de maduración. La institución debe velar por evolucionar en materia de gestión de la seguridad operacional, ya que hasta ahora, sus acciones, documentos e indicadores indican que planea una gestión de la seguridad operacional desde el paradigma tradicional.

8.5 Limitaciones y Futuras Líneas de Investigación

Dentro de las limitaciones de la presente investigación se puede mencionar el tamaño de la muestra tomada para la realización de la fase cualitativa. Si bien el estudio respondió a lo planteado originalmente, se hizo evidente que la mejor metodología para profundizar en los resultados cuantitativos era la realización de grupos focales, mismos que deseablemente deben plantearse por niveles de participación operacional y en varias unidades de la organización.

Esta forma de intervención podría aportar mayor riqueza en la comprensión de los datos debido a la complejidad de la institución que tiene cubrimiento nacional, diversidad misional, variedad de equipos, restricciones presupuestales, riesgos meteorológicos propios de la geografía del país, variadas y muchas formas de violencia que afectan el orden nacional, solo por mencionar algunas particularidades.

Esto también hace evidente la enorme complejidad que reviste la gestión de la seguridad

operacional al interior de la organización. El reto está en definir las estrategias apropiadas para permear la organización hasta el último nivel de modo que se genere una cultura de seguridad sólida.

Una segunda limitación estaría relacionada con la posibilidad de ampliar su alcance, probando la validez estadística de los instrumentos en diferentes organizaciones de alto riesgo (aviación comercial, plantas petroquímicas, mineras, etc) para establecer su utilidad en otros sectores dada la solidez demostrada en la investigación.

En tercer lugar, se podría ampliar la lectura de la resiliencia en la organización incluyendo una medición por áreas de la organización en una muestra más heterogénea. Para este caso, se tuvo en cuenta el grupo de pilotos que son las personas que están continuamente en contacto con las operaciones. Sin embargo, están también las áreas de mantenimiento y administrativa que representan subsistemas claves en la organización y en la gestión de la seguridad.

Una cuarta oportunidad de mejora para la investigación estaría en la necesidad de hacer una nueva y más precisa lectura de la distinción entre el grupo que diseña las operaciones (tarea prescrita) y el grupo que las ejecuta (trabajo real) a la luz de la dinámica de la organización para poner nuevamente a prueba la hipótesis teórica que plantea la existencia de diferencias en la percepción del potencial de desempeño resiliente entre estos dos grupos.

Respecto al planteamiento de futuras líneas de investigación, una vez establecida la relación causal y predictiva entre resiliencia y seguridad, sería valioso incrementar el alcance a través del diseño de un modelo de resiliencia dentro de una organización específica, su implementación y probando su impacto en la seguridad a través de indicadores clave.

Esta idea implica la realización de un estudio con diseño transversal cuasiexperimental con mediciones previa y posterior a la implementación del modelo a través del mismo instrumento de manera que se obtengan comparaciones válidas. Teniendo en cuenta el impacto de una forma de intervención de esta magnitud, se requeriría mínimo dos a tres años de medición para tener

resultados consistentes.

De otra parte, Amalberti (2009) plantea que existe resiliencia por niveles de la organización. Incluso Van der Vorm (s.f.) plantea que la resiliencia organizacional es resultado de la resiliencia individual, de grupo y organizacional. Esto invita a profundizar en este concepto que abre la posibilidad de hacer mediciones más completas por niveles seccionados de acuerdo con los intereses de la organización que permitan identificar necesidades objetivas con el fin de intervenirlas.

La riqueza aquí radicaría en intentar una lectura de resiliencia sistémica a partir de la diferenciación por niveles, lo que permitiría establecer si el valor de la resiliencia organizacional reside particularmente en algún nivel y definir estadísticamente de qué manera participa.

Otra posibilidad futura reside en diseñar y probar métodos predictivos de resiliencia para gestionar la seguridad operacional con base en sistemas de alertas que realmente lleve a la organización a anticiparse de manera efectiva, lo que implicaría el reto de desarrollar indicadores que permitan medir lo que no ocurrió.

Capítulo

9. Conclusiones y Recomendaciones

Seguidamente se formulan las conclusiones del estudio y se proponen algunas recomendaciones según la apreciación conceptual del director de la investigación y las consideraciones teórico - prácticas de la investigadora.

9.1 Conclusiones

9.1.1 Del ámbito investigativo

- La principal contribución de esta investigación radica en su diseño metodológico que, al constituirse como un estudio mixto, permitió abordar de manera más completa su objeto de estudio a la luz de la realidad de la organización, así como brindar herramientas válidas para medir el potencial de desempeño resiliente y la seguridad operacional con el fin de ser utilizadas en otro tipo de organizaciones de alto riesgo.
- El nivel de seguridad operacional y el potencial de desempeño resiliente, no solo están relacionadas en función directa, sino que el nivel resiliente es un estimador significativo de la seguridad operacional, de manera que un alto nivel de resiliencia permite predecir un mayor grado de seguridad operacional, así como una menor resiliencia correlaciona y predice una menor seguridad operacional.

Esta relación permitió establecer con claridad para la organización, los escenarios que se constituyen en cursos de acción específicos para gestionar con mayor eficiencia la seguridad operacional.

- Contrario a lo esperado, los mayores niveles de seguridad operacional los presentó consistentemente el clúster de mayor incidentalidad, particularmente en las subescalas de aprendizaje, compromiso, legitimidad y adaptabilidad, mientras que el perfil del clúster de incidentalidad intermedia puntuó con los menores niveles de seguridad operacional.

- Los mayores niveles de la seguridad operacional los presenta el clúster de mayor incidentalidad, seguidos por los de menor y en nivel más bajo están los del clúster de incidentalidad intermedia, evidenciándose un comportamiento de distribución en forma de jota, en el que se da una variación no lineal de la seguridad con marcado descenso en el clúster de incidentalidad intermedia.

9.1.2 Del ámbito de la organización de aviación militar

- Tanto el potencial de desempeño resiliente como el nivel de seguridad operacional están un rango medio bajo en la organización de aviación militar. La subescala con menor puntaje es la capacidad de anticipar mientras que la que puntuó más alto fue la capacidad de monitoreo, específicamente en el escenario de ejecución de operaciones (mantenimiento, vuelo y entrenamiento). En seguridad operacional el menor puntaje fue en la gestión de información y el componente más alto fue el de aprendizaje.
- Las mayores consideraciones de alta seguridad operacional se dan en los subcomponentes de compromiso, aprendizaje y adaptabilidad, donde se apreció mayor respuesta de seguridad. aunque los niveles proporcionales en estas subescalas no lograron llegar a las categorías de media y alta seguridad operacional.
- En la organización existen moderados de recursos instrumentales y actitudinales para enfrentar contingencias fortuitas de la actividad operacional. Sobresalió la capacidad de monitoreo, en los escenarios de supervisión de procesos operativos y de ejecución de operaciones, seguidos de la capacidad de aprendizaje.
- El potencial de desempeño resiliente en las subescalas de capacidad de responder (escenario 2: entrenamiento de personal operativo), capacidad de monitoreo (escenario 2: entrenamiento de personal operativo y escenario 3: supervisión de procesos operativos) y en la escala total, es significativamente diferente entre los clúster de incidentalidad en particular entre los clúster de alta e intermedia incidentalidad.

- El nivel de participación operacional (táctico vs operacional vs estratégico) no determina consideraciones diferenciales significativas sobre el potencial de desempeño resiliente, así como tampoco de la seguridad operacional en la organización, incluso al recategorizar la participación operacional entre las líneas operacionales 1|°-2° vs 3|, confirmándose la independencia entre estas variables.
- El tiempo en la especialidad de pilotaje tiene una discreta influencia sobre el potencial de desempeño resiliente y sobre el nivel de seguridad operacional de la organización militar de aviación.
- Un alto nivel del potencial de desempeño resiliente se asocia con una mayor seguridad operacional y viceversa, dando lugar a una relación directa, aunque no proporcional, pero sí con comportamiento diferencial entre los clúster de alta media y baja incidentalidad.
- Las capacidades resilientes de responder, monitorear, anticipar y aprender correlacionan positivamente con el nivel de seguridad operacional en la organización de aviación militar; además, hay relación directa significativa alta entre el potencial de desempeño resiliente y la seguridad operacional, como tendencia relacional mayoritaria.
- La función predictiva de las subescalas de potencial de desempeño resiliente sobre el nivel de seguridad operacional, radica en la capacidad para anticipar, la capacidad de monitoreo en el escenario 3 (supervisión de las operaciones), la capacidad para aprender y la capacidad para responder en el escenario 2 (entrenamiento).
- Es probable que las personas en la organización no estén percibiendo claramente las capacidades reales de la organización en términos de seguridad operacional. El sistema tiene fortalezas en la gestión de riesgos, pero igualmente tiene debilidad en su capacidad para identificarlos oportunamente y actuar de manera preventiva.

- La institución es reactiva ante los eventos de seguridad operacional y se le dificulta anticiparse a riesgos en el entorno. Si bien hay un claro intento de pensar el futuro a través de la prospectiva, se observa que las decisiones sometidas a una recurrente falta de continuidad no permite producir los efectos que se buscan.
- Una fuente de amenaza es el avance decisivo de otras instituciones militares con un área de aviación que están desarrollando capacidades que antes eran exclusivas de esta organización. Esas instituciones cuentan con más personal y mayor capacidad de adaptación.

9.2 Recomendaciones

Finalizado el desarrollo de la investigación y establecidas las conclusiones, se plantean las siguientes recomendaciones:

9.2.1 De impacto teórico en el ámbito de la psicología aeronáutica

- Desarrollar investigaciones que permitan fortalecer y clarificar la evidencia propia de las organizaciones de aviación sobre los efectos y la eficacia del potencial de desempeño resiliente en los programas de seguridad operacional, así como perfeccionar las herramientas de intervención preventivas, la batería evaluativa y el monitoreo de alertas tempranas.
- Conformar programas de investigación organizacionales que permitan la comparabilidad de los efectos y la eficacia de la acción preventiva con base en el fortalecimiento del potencial de desempeño resiliente en diferentes condiciones de operación.

9.2.2 De impacto teórico-práctico en el ámbito aeronáutico

- Diseñar, establecer e impulsar una línea de investigación institucional para la generación de herramientas de valoración e intervención del potencial de desempeño resiliente adaptadas a la organización para el fortalecimiento de la seguridad

operacional basado en evidencia científica, de manera que se pueda aportar al mejoramiento de las condiciones de seguridad.

- Como ciencia organizacional y social, la psicología aeronáutica en Colombia debe introducir prácticas basadas en modelos de orientación sistémica que impacten positivamente la seguridad operacional en organizaciones de aviación para abonar el terreno que facilite dejar de lado los modelos lineales y la búsqueda de causas basada en acciones individuales que caracteriza la seguridad operacional hasta hoy, abordaje que restringe la seguridad operacional y no origina una verdadera acción preventiva.

9.2.3 De impacto práctico en la organización de aviación militar

- La organización debe actuar en el fortalecimiento del potencial de desempeño resiliente de manera sistemática, holística y armónica, involucrando en sus respectivos ámbitos los rangos de los niveles estratégico, operacional y táctico.
- Es necesario una decisión del alto mando que lleve a definir las estrategias apropiadas para permear toda la organización, hasta el último nivel, de modo que se genere una cultura de seguridad sólida más que un actuar eventual o reactivo.
- En el ámbito específico de la seguridad operacional en la organización, se plantea con sentido de urgencia la formación de investigadores que puedan evaluar los eventos de seguridad operacional con una visión sistémica, la estandarización del proceso de investigación que origine un criterio unificado con información confiable y el diseño e implementación de un modelo de seguridad operacional planteado desde el fortalecimiento de las capacidades resilientes de la organización.

Referencias

- Amalberti, R. (2009). De la gestión de los errores humanos a la gestión de los riesgos. *Manual de Ergonomía*. Madrid: Modus Laborandi. ISBN. 978-84-15109-15-0.
- Arnold, M. y Osorio, F. (1998). Introducción a los Conceptos Básicos de la Teoría General de los Sistemas. *Cinta de Moebio*, 3. Recuperado de: <http://redalyc.org/pdf/101/10100306.pdf>
- Astocaza, D. M. y González, M. D. (2014). Modelo de gestión de un sistema sociotécnico como innovación. Pontificia Universidad Católica del Perú. *IV congreso Internacional de Gestión Tecnología e Innovación - COGESTEC*. Cartagena. Recuperado de [http://cogestec.ingenio.com.co/db/separated/2014%20\(41\).pdf](http://cogestec.ingenio.com.co/db/separated/2014%20(41).pdf)
- Azadeth, A., Salehi, V., Arvan, M. y Dolatkah, M. (2013). Assesment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: a petrochemical plant. *Safety Science*. 68:99-107. doi 10.1016/j.ssci.2014.03.004
- Bellini, E., Cocone, L. y Nesi, P. (2018). A functional resonance analysis method driven resilience quantification for socio-technical systems. *IEEE Systems Journal*. doi 10.1109/JSYST.2019.2905713
- Blaya, F., Abad, L., García, M. y Sampedro, P. (2012). Los factores humanos y la ergonomía en entornos industriales. *Revista de Ciencia, Tecnología y Medio Ambiente*. Madrid, Universidad Alfonso X El Sabio.
- Carvalho, P., dos Santos, I., Gomes, J.O. y Borges, M. (2007). Micro incident analysis framework to assess safety and resilience in the operation of safe critical systems; a case study in a nuclear power plant. *Journal of Loss Prevention in the Process Industries*. 21:277-286. doi 10.1016/j.jlp.2007.04.005
- Cárdenas, M. Arancibia, M. (2014). Potencia estadística y cálculo del tamaño del efecto en g*power: complementos a las pruebas de significación estadística y su aplicación en psicología. *Salud & Sociedad*. v. 5 no. 2, pp. 210 – 224. mayo – agosto, 2014. ISSN 0718-7475.
- Cervantes, V.H. (2005). *Interpretaciones del coeficiente alpha de Cronbach*. Universidad Nacional de Colombia Avances en Medición, 3, 9-28.
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences*. Second Edition. Hillsdale, NJ: LEA. ISBN 0-8058-0283-5.
- Cohen, J. (1992). Cosas que he aprendido (hasta ahora). *Anales de psicología*. 1992, 8 (1-2), 3-17.

- Cook, R.I.; Render, M.L. y Woods, D.D. (2000). Gaps in the continuity of care and progress on patient safety, *British Medical Journal*, 320, 791-794.
- Dallat, C., Salmón, P. y Goode, N. (2017). Identifying risk and emergent risk across sociotechnical systems; the NETworked hazard analysis and risk management system (NET-HARMS). *Theoretical Issues in Ergonomics Sciences*, 19:4, 456-482, Doi 10.1080/1463922X.2017.1281197
- Daniel, W. (2002). *Bioestadística: Bases para el análisis de las ciencias de la salud*. 4ª ed. México: Limusa Wiley.
- De Keyser, V. (1990). El error humano. *Mundo científico*. 99, 211-229.
- Dekker, S. (2006). Resilience engineering: Chronicling the emergence of confused consensus. En E. Hollnagel, D. Woods y N. Leveson. (Eds.). *Resilience engineering. Concepts and precepts*. (pp. 77-92). Madrid: Modus Laborandi.
- Dijkstra, A. (2006). Safety management in airlines. En E. Hollnagel, D. Woods y N. Leveson. (Eds.). *Resilience engineering. Concepts and precepts*. (pp. 37-43). Estados Unidos: Ashgate.
- Domínguez-Lara, S. (2017). Magnitud del efecto, una guía rápida. *J. Edumed*. 2017.07.002. Universidad de San Martín de Porres, Lima (Perú). <https://doi.org/10.1016/j.edumed.2017.07.002>
- Fiorentino, M.T. (2008). La construcción de la resiliencia en el mejoramiento de la calidad de vida y la salud. Universidad Nacional de San Luis Argentina. *Suma Psicológica*, Vol. 15 N° 1 Marzo de 2008, 95-114, ISSN 0121-4381.
- Flórez y Tomas, (1993). La teoría general de sistemas. *Cuaderno de Geografía: Revista Colombiana de Geografía*. 4:1-2,111-137. ISSN 2256-5442.
- Foerster, H. V. (2006). *Las semillas de la cibernética*. 2da. ed. Barcelona: Gedisa.
- Gómez, M. A. (2016). Sobre la psicología organizacional y del trabajo en Colombia. *Revista colombiana de ciencias sociales*. 7(1), 131-153. Recuperado de <file://Dialnet-SobreLaPsicologiaOrganizacionalYDelTrabajoEnColomb-5454161.pdf>
- Hair, J., Anderson, R., Tatham, R. y Black, W. (2000). *Análisis multivariante*. Madrid: Prentice Hall.
- Hale, A. y Heijer, T. (2006). ¿Es realmente necesaria la resiliencia? El caso de los ferrocarriles. En Hollnagel E., Woods D. y Leveson N. (Eds.). *Ingeniería de la Resiliencia. Conceptos y preceptos*. (pp. XX-XX). Madrid: Modus Laborandi.
- Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación*. 6ª. Ed.

México: McGraw-Hill.

- Herrera, I. (2016). *Resilience engineering and indicator of resilience*. Departamento de Economía Industrial y Administración Tecnológica. Universidad Noruega de Ciencia y Tecnología. Recuperado de <https://www.irgc.org/risk-governance/resilience/>
- Hogan, T. (2004). *Pruebas psicológicas. Una introducción práctica*. México: Manual Moderno. ISBN 970-729-087-0.
- Hollnagel, E. Woods, D. Leveson, N. (2006). *Resilience Engineering. Concepts and Precepts*. Madrid: Modus Laborandi.
- Hollnagel, E. (2006). Resilience: The challenge of the unstable. En Hollnagel, E., Woods, D. y Leveson, N. (Eds.). *Resilience Engineering. Concepts and Precepts*. Madrid: Modus Laborandi.
- Hollnagel, E. (2009). *Barreras y prevención de accidentes*. 1ª ed. Madrid, España: Modus Laborandi.
- Hollnagel, E. (2013). *An application of the functional resonance analysis method (FRAM) to risk assessment of organisational change*. Swedish Radiation Safety Authority. ISSN: 2000-0456.
- Hollnagel, E. (2014). *Safety I and safety II. The past and future of safety management*. Farnham, UK: Ashgate.
- Hollnagel, E. (2015). *RAG – Resilience Analysis Grid*. Recuperado de: <http://www.erickhollnagel.com/pnewebmedia/RAG%20outline%20V2.pdf>
- Hollnagel, E. (2018). *Safety-II in the practice. Developing the resilience potentials*. New York: Routledge Taylor & Francis Group.
- Huber, G.J., Gomes, J.O. y Carvalho, P.V. (2012). A program to support the construction and evaluation of resilience indicators. 41:2810-2816. Doi 10.3233/wor-2012-0528-2810
- Jakobsson, U. & Westergren, A. (2005). Statistical methods for assessing agreement for ordinal data. *Scandinavian Journal of caring Science*, 19 (4), 427-431.
- Kerlinger, F. y Lee, H. (2002). *Investigación del comportamiento. Métodos de investigación en ciencias sociales*. México: McGraw-Hill.
- Leal, N. (2002). Diseño de un sistema sociotécnico en la empresa Workspaces que ayude a organizarse para trabajar con conceptos de manufactura de clase mundial (Tesis de maestría). Recuperado de <http://eprints.uanl.mx/5226/1/1020148376.PDF>
- Ledesma, R., Macbeth, G. y Cortada De Kohan, N. (2008). Tamaño del efecto: Revisión teórica y aplicaciones con el sistema estadístico Vista. *Revista Latinoamericana de*

- Psicología*, 40 (3), 425-439. ISSN: 0120-0534. Recuperado de: <https://www.redalyc.org/articulo.oa?id=805/80511493002>
- Leplat, J. y Hoc J.M. (2009). Tarea y actividad en el análisis psicológico de situaciones. *Manual de Ergonomía*. 163-177. Madrid: Modus Laborandi.
- Ljungberg, D. y Lundh, V. (2013). *Resilience Engineering within ATM – Development, adaption and application of the Resilience Analysis Grid (RAG)*. (Tesis de grado Universidad Técnica de Linköping. Suecia).
- Manrique, K. y González, A. (2013). *Desarrollo de sistemas sociotécnicos en el área de seguridad y salud ocupacional de una empresa de servicio*. Pontificia Universidad Católica del Perú. Recuperado de http://www.altec2013.org/programme_pdf/429.pdf
- Martínez, M., Gracia, F.J. y Peiró, J.M. (2018). El estudio del comportamiento humano de seguridad en organizaciones de alta fiabilidad: El caso de la industria nuclear. *Papeles del Psicólogo*, vol. 39, núm. 3. Consejo General de Colegios Oficiales de Psicólogos. Recuperado de <https://www.redalyc.org/jatsRepo/778/77857281004/html/index.html>
- Mc Donald, N. (2006). Organizational resilience and industrial risk. En E. Hollnagel, D. Woods y N. Leveson. (Eds.). *Resilience Engineering. Concepts and Precepts*. (pp. 155-180). Estados Unidos: Ashgate.
- Mendizábal, N. (2006) Los componentes del diseño flexible en la investigación cualitativa en Vasilachis de Gialdino, I. (comp.) *Estrategias de la investigación cualitativa*. Barcelona: Editorial Gedisa.
- Ministerio de Salud de la República de Colombia (1993). Resolución 8430 de 1993. Normas científicas, técnicas y administrativas para la investigación en salud. [En red]. Recuperado de: <http://www.minsalud.gov.co/normatividad/resolucion%208430%20de%201993.pdf>
- Moreno, A.J. (2006). Resiliencia, tenacidad y fractura. Recuperado de https://ajmoreno.webs.ull.es/resistencia%20de%20materiales/Resistencia_files/Resiliencia.pdf
- Morin, E. (1994). *Introducción al Pensamiento Complejo*. 1ª ed. en castellano Madrid (España): Gedisa Editorial.
- Murphy L.A., Huang Y.H., Robertson M.M., Jeffries S. 2., Dainoff, M.J. (2018). A sociotechnical systems approach to enhance safety climate in the trucking industry: Results of an in-depth investigation. *Applied Ergonomics*. 66:70-81. Doi: 10.1016/j.apergo.2017.08.002.
- Naevestad, T. (2009). Mapping research on culture and safety in high-risk organizations:

- arguments for a sociotechnical understanding of safety culture. *Journal of Contingencies and Crisis Management*. 7,2:126-135. Doi 10.1111/j.1468-5973.2009.00573.x
- Oien, K., Massaiu, S., Tinmannsvik R.K. y Storseth, F. (2010). *Development of early warning indicators base don resilience engineering*. Manuscrito presentado al PSAM. Probabilistic Safety Assesment and Management.
- Organización de Aviación Civil Internacional -OACI- (2013). *Documento 9859 AN/474. Manual de Gestión de la Seguridad Operacional*. 3ra . ed. Montreal: OAC.
- Pariés, J. (2006). Complejidad, emergencia, resiliencia. En Hollnagel, E., Woods, D. y Leveson, N. (Eds.). *Ingeniería de la Resiliencia. Conceptos y preceptos*. (p. 1-5). Madrid: Modus Laborandi.
- Pérez, A., Rodríguez, M., Gil, F. y Ramírez, G. (2001). *Tamaño de la Muestra. Versión 1.1* [software]. Bogotá: Pontificia Universidad Javeriana / INCLEN.
- Pew, R. (2010). *Alphonse Chapanis: Pionner in the application of psychology to enginnering design*. Association of psychological science. Recuperado de: <http://www.psychologicalscience.org/observer/Alphonse-chapani-pionner-in-the-application-of-psychology-to-enginnering-design>
- Poy, M. (2006). *Aspectos funcionales de los riesgos y desvíos de las normas de seguridad en el trabajo. Un aporte a la comprensión de las relaciones entre actividad humana y seguridad*. (Tesis doctoral, Universidad de Palermo, Buenos Aires, Argentina). Recuperado de https://dspace.palermo.edu:8443/xmlui/bitstream/handle/10226/1671/Poy%20Mario%20Tesis_CC.pdf?sequence=1
- Poy, M., Turjanski D. y Aslanides. M. (2005). *La gestión del riesgo en la actividad de pilotos de línea aérea: análisis de un caso real*. Manuscrito presentado para su publicación.
- Rädiker, S. y Kuckartz, U. (2020). *Análisis de datos cualitativos con MAXQDA: Texto, audio, video*. Berlin: MAXQDA Press. Recuperado de https://doi.org/10.36192/978-3-948768003_01
- Rae, A. y Provan, D. (2019). Safe work versus the safety of work. *Safety Science*. 111:119-127. Doi: 10.1016/j.ssci.2018.07.001
- Reason, J. (2010). La gestión de los grandes riesgos. *Principios humanos y organizativos de la seguridad*. 1ª ed. Madrid, España: Modus Laborandi
- Reason, J. (2011). *La contribución humana. Actos peligrosos y acciones ejemplares*. 1ª ed.

Madrid, España: Modus Laborandi.

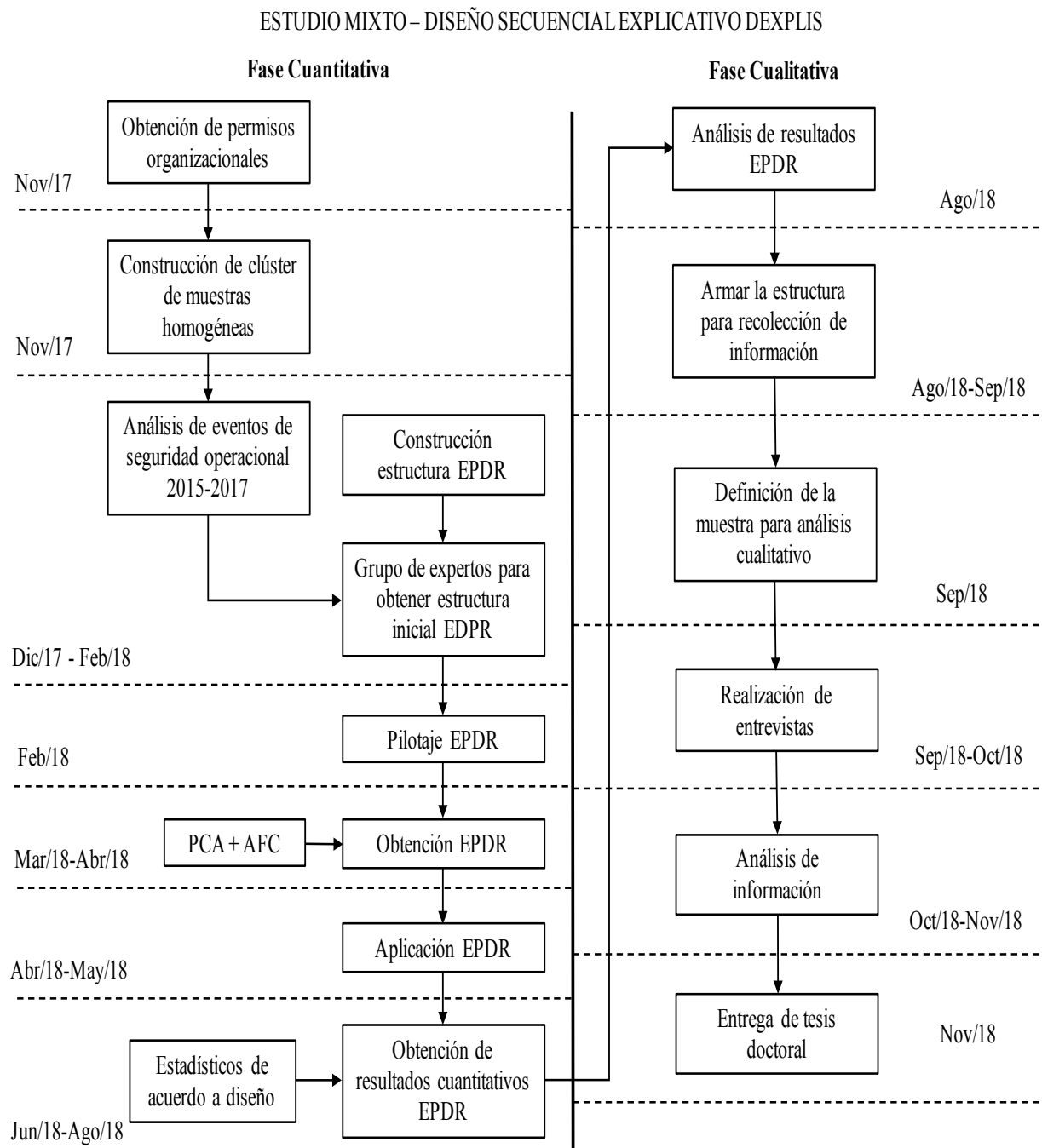
- Reyes, I. (2019). *Análisis descriptivo de información estadística sobre eventos de seguridad operacional 2015-2017*. Bogotá (Documento no publicado).
- Roscoe, S. (1980). *Aviation Psychology*. 1ª ed. Iowa, Estados Unidos: The Iowa State University Press
- Sabogal, L. Barraza, E. Hernández, A. y Zapata, L. (2011). Validación del cuestionario de motivación y estrategias de aprendizaje en estudiantes universitarios de una institución pública. *Psicogente*, 14 (25): pp. 36-50. Junio, 2011. ISSN 0124-0137.
- Saíz, M. y Saíz, D. (2012). El inicio de la psicología aplicada a la aviación: desde el principio del siglo XX a la década de los años treinta. *Revista de Historia de la Psicología*, 2012, vol. 33, núm. 4 (diciembre).
- Said, S., Bouloiz, H. y Gallab, M. (2019). A new structure of sociotechnical system processes using resilience engineering. *International Journal of Engineering Business Management*. 11: 1-10. Doi 10.1177/1847979019827151.
- Sebastián, M. L. (2009). Fallo humano: la quiebra de un paradigma. Colegio Oficial de Psicología de Andalucía Occidental y Universidad de Sevilla *Apuntes de Psicología*. 2009, Vol. 27, número 1, págs. 21-51. ISSN 0213-3334
- Sheridan, T. (2008). Risk, human, error, and system resilience: fundamental ideas. *Human Factors: The Journal of the Human Factors and Ergonomics Society*. 50:418, Doi: 10.1518/001872008X250773
- Shirali, G.A., Mohammadfam, I. y Ebrahimipour, V. (2013). A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering and System Safety*, 119, 88–94, Doi 10.1016/j.ress.2013.05.003.
- Shirali, G.A., Motamedzade, M., Mohammadfam, I., Ebrahimipour, V. y Moghimbeigi, A. (2015). Assesment of resilience engineering factors based on system properties in a process industry. 18: 19. Doi: 10.1007/s10111-015-0343-13.
- Siegel, S. y Castellan, J. (1995). *Estadística no paramétrica aplicadas a las ciencias de la conducta*. 4ª ed. México: Trillas.
- Stringfellow, M. (2010). *Accident analysis and hazard analysis for human and organizational factors*. Massachusetts Institute of Tecnology. (Tesis doctoral). Massachusetts, Estados Unidos).
- Suárez, A. (2015). La estadística en la validación de escalas, una visión práctica para su

- construcción o su adaptación. *Revista I3+*, 2(2), 46 – 61 p.
- Thomassen, O. J., Heggen, K. y Strand, R. (2017). Applying principles of sociotechnical systems onto working environment research. *Nordic Journal of Working Life Studies*. 52-65.
- Torres, L. C. (s.f.). *La complejidad humana*. Departamento de Ingeniería de Sistemas e Industrial Universidad Nacional de Colombia. Recuperado de <https://disi.unal.edu.co/~lctorress/tgs/Tgs003.pdf>
- Van der Vorm, J., Van der Beek, D., Bos, E., Steijger, N., Gallis, R. y Zwetsloot, G. (s.f.). Images of resilience: the resilience analysis grid applicable at several organizational levels?. Netherlands: Toegepast Natuurwetenschappelijk Onderzoek
- Vasilachis de Gialdino, I.(2006) La investigación cualitativa. En Vasilachis de Gialdino, I. (Comp.). *Estrategias de la Investigación Cualitativa*. Barcelona (España): Gedisa Editorial.
- Venkatasubramanian, V., Luo, Y. y Zhang, Z. (2019). Control of complex sociotechnical systems; Importance of causal models and game theory. *Computers and Chemical Engineering*, (123), 1-11, Doi: 10.1016/j.compchemeng.2018.12.010
- Vera, F. (2018). La validez experimental en psicología: una revisión crítica de la literatura. *CIENCIA ergo-sum*, Revista Científica Multidisciplinaria de Prospectiva, vol. 25, núm. 2.
- Verbi Software. (2019). *MAXQDA 2020* [computer software]. Berlin, Germany: Verbi Software. Available from maxqda.com.
- Von Bertalanffy, L. (1989). *Teoría general de los sistemas*. 7ª. Reimpresión. México, D.F.: Fondo de Cultura Económica
- Walker, G. (2015). Come back sociotechnical systems theory, all is forgiven. *Civil Engineering and Environmental Systems*. 32:1-2, 170-179. Doi: 10.1080/10286608.2015.1024112
- Weigmann, D. y Shapell, S. (2003). *A human error approach to aviation accident analysis. The human factors and classification system*. London: Ashgate
- Westrum, R. (2006). Una tipología de las situaciones de resiliencia. En Hollnagel, E., Woods, D. y Leveson, N. (Eds.). *Ingeniería de la Resiliencia. Conceptos y preceptos*. (p. 1-5). Madrid: Modus Laborandi.
- Woods, D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, (141), 5–9. Doi:

10.1016/j.ress. 2015.03.018.

- Woods, D. y Hollnagel, E. (2006). Prologue: Resilience engineering concepts. En Hollnagel, E., Woods, D. y Leveson, N. (Eds.). *Resilience Engineering. Concepts and Precepts*. (p. 1-5). Madrid: Modus Laborandi.
- Wreathall, J. (2006). Propiedades de las organizaciones con resiliencia: una perspectiva inicial. En Hollnagel, E., Woods, D. y Leveson, N. (Eds.). *Ingeniería de la Resiliencia. Conceptos y preceptos*. Madrid: Modus Laborandi.
- Zipkin, D., Gershenfeld, J., Carrol, J. y Barret, B. (2006). Resiliencia y seguridad. En Hollnagel, E. Woods, D. y Leveson, N. (Eds.). *Ingeniería de la Resiliencia. Conceptos y preceptos*. Madrid: Modus Laborandi.

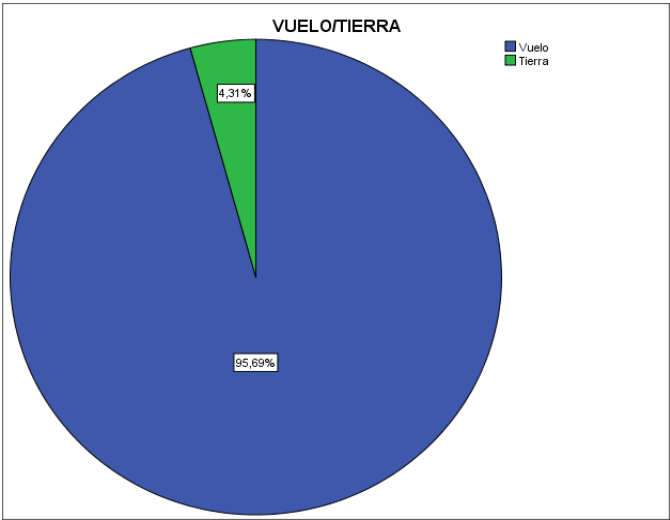
Anexos

Anexo A. Cronograma Inicial de Ejecución

Anexo B. Descripción de Eventos de Incidentalidad / Accidentalidad de la Entidad de Aviación
(Años 2015-2017)

(análisis de la base de datos interna de la entidad- Documento no publicado)

El total de eventos de seguridad operacional reportados en la organización de aviación militar entre los años de 2015 – 2017 fue de 1068 (figura B1), de los cuales el 95,7% (1022) fueron eventos en vuelo y 4,3% (46) en tierra, de manera que se da una relación de 22,2 eventos en vuelo por cada un evento en tierra.



Fuente: elaboración propia de la autora.

Figura B1. Situación de ocurrencia de los eventos de seguridad operacional en la institución de aviación militar

Para efectos del análisis de la calificación y comportamiento de tales evesos se tomó en consideración la tipología que se desplegó en la tabla B1 y para efectos de los análisis subsiguientes se replica acá.

Tabla B1

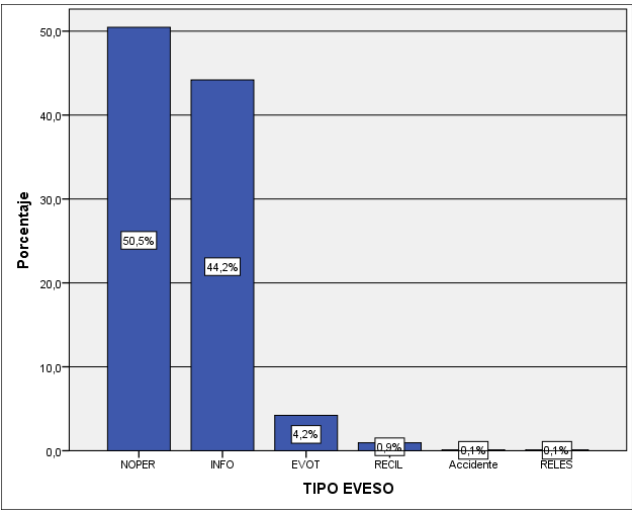
Tipología de los eventos de seguridad operacional en la entidad

Tipología	
EVESO	Evento de seguridad operacional.
INFO	Evento en el que exista una de las siguientes condiciones: teniendo intención de vuelo no existan daños a la aeronave o lesiones a personas, afectación a la seguridad

Tipología	
	de interés para la prevención de accidentes o cuando se apliquen procedimientos anormales por un suceso en la aeronave.
EVOT	Evento operacional en tierra.
NOPER	Novedad operacional.
RECIL	Suceso con intención de vuelo. Recuperable, ilesos.
RELES	Suceso con intención de vuelo. Recuperable, lesionados.
Accidente	Suceso operacional con o sin intención de vuelo en el que exista al menos una de las siguientes condiciones: la aeronave no es recuperable, existen lesiones fatales o algún tipo de incapacidad permanente, evento con fatalidades dentro de los noventa días calendario a su ocurrencia o aeronaves desaparecidas por más de noventa días.

Fuente: Manual de seguridad operacional institucional.

Con base en la categorización se obtuvo la figura B2, donde se aprecia que sobresalen las novedades operacionales y los informes de alerta de seguridad, que en conjunto llegan a ser el 94,7% de los evesos registrados.



Fuente: elaboración propia de la autora.

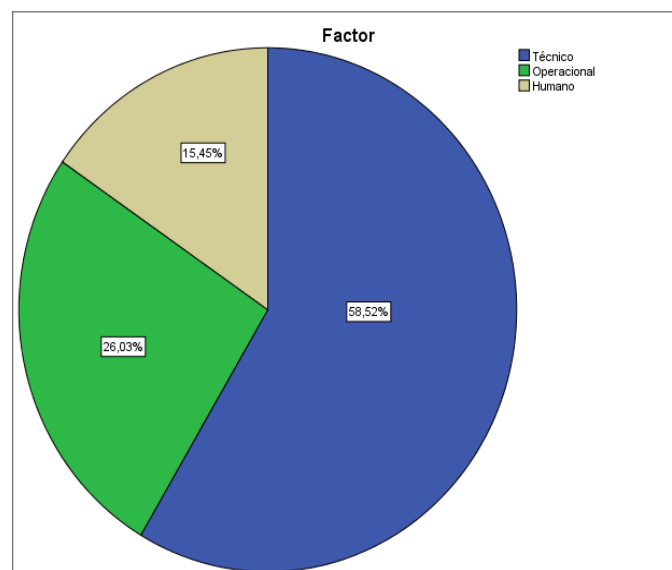
Figura B2. Tipología de los evesos reportados.

En cuanto a incidentes, se presentaron 10 eventos tipo RECIL con afectación del equipo aunque en condiciones recuperables y con el personal ileso y un (1) incidente tipo RELES con

equipo también en condiciones recuperables aunque hubo personal operativo que quedó lesionado.

Se resalta que en los tres años de seguimiento que fueron considerados hubo solo un (0,1%) evento que fue calificado como accidente con importante afectación al equipo y/o a la integridad física de personas involucradas.

Al considerar el factor etiológico al cual circunstancialmente se le asoció la ocurrencia del eveso, la figura B3 muestra que sobresale la proporción de causalidades técnicas con el 58,5%, mientras que el factor humano llegó a estar involucrado en el 15,4% de los evesos.



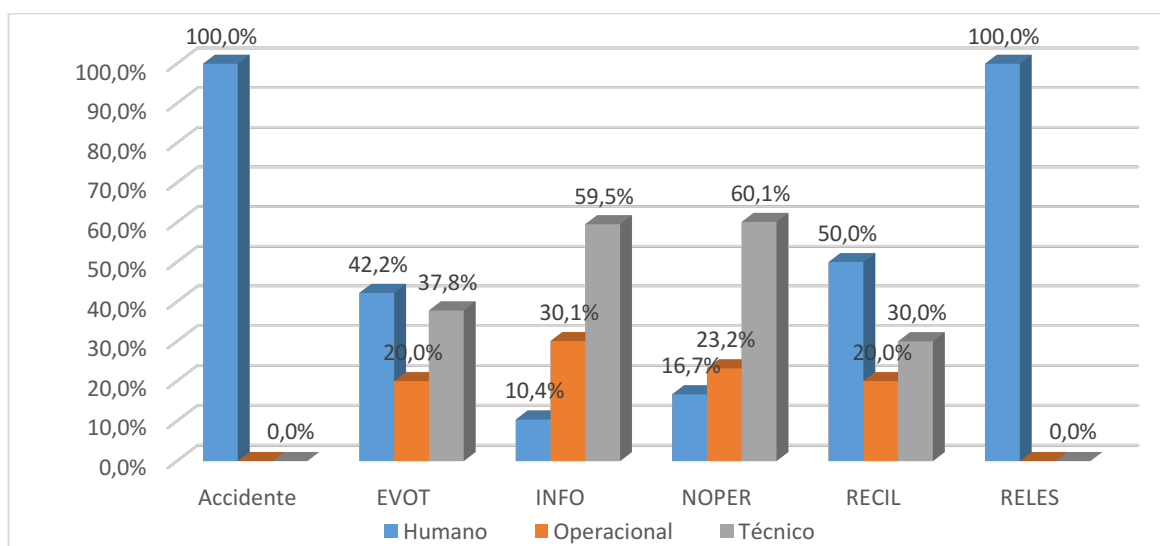
Fuente: elaboración propia de la autora.

Figura B3. Tipo de factor etiológico en la entidad de aviación militar

Según se precisó el 21,74% de los datos contenidos en la clasificación que fueron definidos como factor técnico, corresponde a acciones del nivel operativo, supervisión u organización (Reyes, 2019), lo que probablemente sugiera que el esfuerzo resiliente se deba centrar en el fortalecimiento de situaciones típicas durante la fase de mantenimiento de las aeronaves y que dependen particularmente de las personas que tiene a cargo esta tarea (Reyes, 2019).

Seguidamente, se analizó la asociación entre los factores asociados y la tipología de evesos

reportados, encontrando la distribución que se ilustra en la figura B4, donde se resalta que el factor humano sobresale como posible elemento causal en los incidentes con equipo recuperable y personal ileso (RECIL) y en los evento operacionales en tierra (EVOT), fuera de la consideración del accidente y del RELES (incidente con equipo recuperable y personal lesionado) que fueron de evento unitario en su tipología . En conjunto la relación estadística fue significativa ($\chi^2=58,374$; $gl.=10$; $p=0,000$), de manera que se puede confirmar que los tipo de eventos de seguridad operacional están relacionados con el tipo de factor involucrado sea humano, operacional o técnico.



Fuente: elaboración propia de la autora.

Figura B4. Porcentaje de factores causales asociados según los tipos de EVESO. Porcentajes basados en el n de cada tipología de eveso.

Anexo C. Escala PoDeRe
UNIVERSIDAD DE PALERMO
Doctorado en Psicología

**Escala de Potencial de Desempeño Resiliente de una
Institución de Aviación**

Autores: Reyes-Ávila I. y Poy, R.M. (2019)

Estimado Oficial de aviación:

Con el aval de la Institución estamos interesados en conocer el Potencial de Desempeño Resiliente de la entidad. Así que amablemente nos permitimos solicitarle su **colaboración voluntaria**, dando respuesta libre al siguiente cuestionario. Esto tiene fines estrictamente investigativos y no conlleva contingencia alguna en su vida profesional o carrera militar.

Si libremente acepta colaborar, luego de las preguntas generales encontrará las instrucciones para continuar participando. Si no lo desea, por favor no prosiga con el diligenciamiento e indíquesele a la persona que le entregó o envió el formato.

Si continua, por favor lea primero la pregunta y las opciones de respuesta y luego **marque** la opción que corresponda, solo se desea conocer su opinión experta en temas de cotidianidad aeronáutica. Es un ejercicio libre.

Gracias por su colaboración...

Pregunta	Respuesta	
¿Ha leído el propósito de esta actividad y acepta participar voluntariamente?	Sí (Continúe)	No (Por favor no continúe con el formato)

INFORMACIÓN DEMOGRÁFICA Fecha: ____/____/____ **Itto #:** _____

Unidad operativa actual: _____ Especialidad: _____

Tiempo de desempeño en la especialidad: _____ años

Nivel del cargo actual: Estratégico _____ Operacional _____ Táctico _____

Es oficial de seguridad?: sí ____ no ____ Tiempo desempeño en cargos de seguridad: _____ años

Tiempo desempeño en cargos relacionados con el Sistema de Seguridad Operacional (Operaciones, mantenimiento, entrenamiento). _____ años

A continuación, encontrará una serie de afirmaciones que buscan conocer su opinión sobre el funcionamiento de algunas áreas de la Institución en términos de la capacidad que esta tiene para **Responder, Monitorear, Aprender y Anticipar** situaciones operacionales.

Frente a cada afirmación referidas a las capacidades para **Responder y Monitorear**, estarán las columnas correspondientes a los tres **escenarios** de la Institución que se quiere analizar.

Las capacidades de **anticipar y aprender** no están vinculadas a escenarios o áreas y se refieren a la institución en su conjunto.

Es importante que escriba su calificación teniendo en cuenta la manera en que la Institución **hace las cosas** y no lo que cree que “debería hacer” o cómo “deberían ser las cosas”.

Este cuestionario no tiene respuestas correctas o incorrectas. Proceda a valorar cada una de las afirmaciones según su criterio experto, siguiendo la siguiente escala y marcando en el número que Ud. considere que corresponda.

- | | |
|--|--|
| <p>0. No sabe, no conoce</p> <p>1. En ningún caso se presenta</p> <p>2. Casi nunca, en no más del 25% de los casos.</p> | <p>3. Parcialmente, aprox. en la mitad de los casos</p> <p>4. Casi totalmente, en más del 70% de los casos</p> <p>5. Sí, en todos los casos se presenta</p> |
|--|--|

CAPACIDAD PARA RESPONDER

ÍTEM	ESCENARIOS								
	1. En la ejecución de operaciones (mantenimiento, vuelo y entrenamiento)			2. En el entrenamiento de personal operativo: pilotos, controladores, operarios de mantenimiento			3. En la supervisión de procesos operativos (mantenimiento, operaciones y entrenamiento).		
1. La institución cuenta con una lista previa de posibles eventos o condiciones (internas o externas) que podrían ocurrir y afectar la seguridad de las operaciones, ante las cuales debería estar preparada para responder.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
2. Las personas en la institución saben cómo deben actuar cuando ocurre alguno de estos eventos.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
3. Esos procedimientos de respuesta se establecieron con criterio profesional cuidadosamente establecido.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
4. Las personas tienen claros los criterios de activación (indicadores) de la respuesta ante perturbaciones operacionales.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
5. Hay suficiente soporte y recursos para asegurar la preparación para la respuesta (personas, equipos, materiales)	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
6. Se cuenta con una persona o dependencia responsable del mantenimiento de la capacidad de respuesta (capacidad de activar procedimientos ante perturbaciones del funcionamiento).	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5

CAPACIDAD PARA MONITOREAR

ÍTEM	ESCENARIOS								
	1. En la ejecución de operaciones (de mantenimiento, vuelo y entrenamiento)			2. En el entrenamiento de personal operativo: pilotos, controladores, operarios de mantenimiento			3. En la supervisión de procesos operativos (mantenimiento, operaciones y entrenamiento).		
7. La institución cuenta con lista de indicadores de rendimiento utilizados regularmente que le permita saber cómo se están haciendo las cosas en materia de seguridad operacional.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
8. La persona responsable de los indicadores verifica y/o revisa esta lista regularmente.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
9. El análisis de los indicadores permite conocer lo que está ocurriendo en cuanto a seguridad operacional.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
10. Se comunica a los diferentes niveles de la organización los resultados de las mediciones de indicadores.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
11. Los resultados de las mediciones de indicadores son usados para mejorar el desempeño del sistema.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
12. Existe un programa de inspección regular al sistema de seguridad operacional.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5
13. Los resultados de las inspecciones se comunican a las personas adecuadas.	0	1	2	0	1	2	0	1	2
	3	4	5	3	4	5	3	4	5

CAPACIDAD INSTITUCIONAL PARA APRENDER

ÍTEM	ESCALA					
14. Las personas en la institución tienen claro cuáles son los eventos de seguridad operacional que generan aprendizaje organizacional (frecuencia, gravedad, otro).	0	1	2	3	4	5
15. El sistema aprende desde sus éxitos (cosas que hace bien) y no tanto de sus fallas (cosas que salen mal).	0	1	2	3	4	5
16. Hay un responsable y un procedimiento formal para la recolección y análisis de información.	0	1	2	3	4	5
17. El aprendizaje es una actividad continua (no impulsada por eventos adversos de seguridad operacional).	0	1	2	3	4	5
18. Se dispone de recursos (logísticos, tecnológicos, presupuestales, humanos) adecuados para la investigación de los eventos y el aprendizaje.	0	1	2	3	4	5
19. Las lecciones aprendidas se evidencian en mejoras a regulaciones, procedimientos, normas, entrenamiento, instrucción, rediseño, reorganización, etc.	0	1	2	3	4	5

CAPACIDAD INSTITUCIONAL PARA ANTICIPAR

ÍTEM	ESCALA					
20. La cultura de la institución anima a pensar acerca del futuro.	0	1	2	3	4	5
21. Las amenazas y oportunidades futuras se evalúan con frecuencia.	0	1	2	3	4	5
22. Las expectativas (o información pronóstico) acerca del futuro se comunican dentro de la institución.	0	1	2	3	4	5
23. La institución tiene un modelo de futuro (una visión de sí misma y de su funcionamiento futuro) articulado y conocido.	0	1	2	3	4	5
24. Las personas conocen los posibles escenarios futuros que representan “riesgos de seguridad operacional” considerados como aceptables.	0	1	2	3	4	5
25. Existe(n) criterio(s) claro(s) que establece(n) el límite aceptable-inaceptable, en términos de riesgos futuros.	0	1	2	3	4	5

Gracias por su colaboración.

Anexo D. Instrumento para Validación de Expertos de la Escala PoDeRe**UNIVERSIDAD DE PALERMO - ARGENTINA****Doctorado en Psicología****Escala de valoración del Potencial de Desempeño Resiliente
de una institución de aviación****Autores: Reyes-Ávila I. & Poy, M. (2019)****INSTRUMENTO PARA LA EVALUACIÓN PSICOMÉTRICA DE LA VALIDEZ DE APARIENCIA
POR PARTE DE JUECES EXPERTOS**

NOMBRE DEL EXPERTO: _____	PROFESIÓN: _____
----------------------------------	-------------------------

○ **DELIMITACIÓN DEL DOMINIO CONCEPTUAL**

- Población objetivo: Pilotos, aviadores y técnicos de aviación militar
- **Constructo evaluado:** Potencial de Desempeño Resiliente de una institución de aviación militar.
 - Definición: Capacidad intrínseca de la FAC para reajustar su funcionamiento antes, durante o después de cambios o perturbaciones, que permita desarrollar las operaciones luego de un contratiempo significativo o en presencia de presión continua (Hollnagel, 2014). Se contemplan los siguientes tipos de capacidades:
 - Capacidad de responder: saber qué hacer
 - Capacidad de monitorear la situación: saber qué buscar
 - Capacidad de anticipar: saber qué esperar
 - Capacidad de aprender: saber qué ha ocurrido
 - **Escenarios de valoración:** Ámbitos en los que se da la expresión del potencial resiliente
 - Ejecución de operaciones (de mantenimiento, vuelo y entrenamiento)
 - Entrenamiento de personal operativo: pilotos, controladores, operarios de mantenimiento
 - Supervisión de procesos operativos (mantenimiento, operaciones y entrenamiento).
 - En la institución, al más alto nivel

○ **DEFINICIÓN DE ELEMENTOS OPERATIVOS DE LA ESCALA**

- **Estructura de la prueba:** Como instrumento escalar los ítems fueron contruidos con la modalidad Likert referida en la práctica a proporción de ocurrencias de la variable como selección de alternativas, con ítems de selección única.
- **Número de reactivos:** 25 ítems (aunque los ítem 1-13 se valoran referidos específicamente a los cuatro escenarios, lo que corresponde a 64 ítems).
- **Forma de aplicación:** Autoaplicable (cada individuo responde de manera independiente y sin considerar opinión externa).

○ **Tiempo estimado de aplicación:** 25-30 minutos.

○ **INSTRUCCIONES PARA LA VALIDACIÓN DE CONTENIDO DE LOS ÍTEMS ESTA ESCALA:**

1. **Pertinencia del ítem (Validez):** Se refiere al criterio de validez de contenido o sea que el ítem sí corresponde a la variable respectiva.
2. **Claridad del ítem (Redacción):** este aspecto se refiere a que el ítem este adecuadamente formulado de manera que los términos utilizados sean claros tanto para quien diligencia como para quien contesta el instrumento.
3. **Observaciones y sugerencias:** Si tiene observaciones y sugerencias con respecto a los ítems y al cuestionario en general, por favor regístrelas. Si el espacio es insuficiente, use el reverso de la hoja o la parte inferior que aparece al final.

A continuación, usted encontrará el cuestionario para evaluar las variables de la escala, dentro del cual se encuentran cada uno de los ítems que la conforman. Por favor señale con una X en la opción **SI**, si considera que el ítem cumple con lo estipulado y marque **NO**, en caso contrario.

Agradecemos de antemano su colaboración y el tiempo dedicado al análisis de la escala, el cual pretende facilitar el estudio de condiciones cotidianas en la operación de la Institución.

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Potencial de Desempeño Resiliente de la FAC						
CAPACIDAD PARA RESPONDER (en los escenarios)						
1. La institución cuenta con una lista previa de posibles eventos o condiciones (internas o externas) que podrían ocurrir y afectar la seguridad, para las cuales debería estar preparada para responder.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
2. Las personas en la institución saben cómo deben actuar cuando ocurre alguno de estos eventos.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
3. Esos procedimientos de respuesta se establecieron con un criterio profesional cuidadosamente establecido.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
4. Las personas tienen claros los criterios de activación (indicadores) de la respuesta	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
5. Hay suficiente soporte y recursos para asegurar la preparación para la respuesta (personas, equipos, materiales).	0. no sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
6. Se cuenta con una persona o dependencia responsable del mantenimiento de la capacidad de respuesta.	0. no sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
CAPACIDAD PARA MONITOREAR (en los escenarios)						
7. La institución cuenta con una lista de indicadores de rendimiento utilizados regularmente que le permita saber cómo se están haciendo las cosas.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
8. La persona responsable de los indicadores verifica y/o revisa esta lista regularmente.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Potencial de Desempeño Resiliente de la FAC						
9. El análisis de los indicadores permite conocer lo que está ocurriendo.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
10. Se comunica a la organización los resultados de las mediciones.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
11. Los resultados de las mediciones son usados para mejorar el desempeño del sistema.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
12. Existe un programa de inspección regular al sistema de seguridad operacional.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
13. Los resultados se comunican a las personas adecuadas.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
CAPACIDAD INSTITUCIONAL PARA APRENDER						
14. Las personas en la institución tienen claro cuáles son los eventos de seguridad operacional que generan aprendizaje organizacional (frecuencia, gravedad, valor).	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
15. El sistema aprende desde sus éxitos (cosas que hace bien) y no tanto de sus fallas (cosas que salen mal).	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
16. Hay un responsable y un procedimiento formal para la recolección, análisis y aprendizaje de información.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Potencial de Desempeño Resiliente de la FAC						
17. El aprendizaje es una actividad continua (no impulsada por eventos).	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
18. Se dispone de recursos adecuados para la investigación y el aprendizaje.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
19. Las lecciones aprendidas se evidencian en mejoras a regulaciones, procedimientos, normas, entrenamiento, instrucción, rediseño, reorganización, etc.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
CAPACIDAD INSTITUCIONAL PARA ANTICIPAR						
20. La cultura corporativa anima a pensar acerca del futuro.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
21. Las amenazas y oportunidades futuras se evalúan con una frecuencia aceptable.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
22. Las expectativas (o información pronóstico) acerca del futuro se comunican dentro de la institución.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
23. La institución tiene un modelo de futuro articulado y reconocible.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					
24. Es claro para las personas en el sistema cuál es el riesgo considerado aceptable.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Si. en todos los casos se presenta					

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Potencial de Desempeño Resiliente de la FAC						
25. Existe(n) un(os) criterio(s) claros que establece(n) el límite aceptable-inaceptable.	0. No sabe, no conoce. 1. En ningún caso se presenta. 2. Casi nunca, en máximo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en más del 70% de los casos 5. Sí. en todos los casos se presenta					
OBSERVACIONES Y SUGERENCIAS GENERALES:						

Anexo E. Escala SegOp
UNIVERSIDAD DE PALERMO - ARGENTINA
Doctorado en Psicología

Escala de Seguridad Operacional
en una Institución de Aviación Militar
Autores: Reyes-Ávila I. & Poy, R.M. (2019a)

A continuación, encontrará unas afirmaciones sobre seguridad operacional. No hay respuestas correctas o incorrectas. Lea cuidadosamente cada afirmación y realice su calificación teniendo en cuenta su experiencia y criterio experto y no lo que crea que “debería ser”.

- | | |
|---|---|
| 0. No sabe, no conoce
1. En ningún caso
2. Casi nunca, aprox. 25% de los casos | 3. Parcialmente, aprox. la mitad de los casos
4. Casi en el total, en la mayoría de los casos
5. Sí, en todos los casos. |
|---|---|

ÍTEM	ESCALA					
I. COMPONENTES DE SEGURIDAD						
1.1. Compromiso						
1. La institución busca ser modelo en el sector de la aviación en lo que concierne a buenas prácticas de seguridad operacional.	0	1	2	3	4	5
2. Las decisiones de los comandantes dejan ver su genuino interés por mantener la seguridad operacional.	0	1	2	3	4	5
3. La institución aporta recursos humanos, técnicos y presupuestales idóneos para gestionar la seguridad operacional.	0	1	2	3	4	5
4. Independiente de los evesos, las acciones en seguridad operacional son continuas y permiten reformar y reforzar las defensas del sistema.	0	1	2	3	4	5
1.2. Gestión de la información						
5. El sistema de información de seguridad operacional produce información pertinente para la seguridad y permite sacar las conclusiones correctas (medidas reactivas).	0	1	2	3	4	5
6. El sistema de información de seguridad operacional proporciona chequeos regulares sobre procesos organizativos básicos (medidas proactivas) que puedan usarse para guiar acciones correctivas dirigidas a objetivos específicos.	0	1	2	3	4	5
7. Se difunden los resultados de las investigaciones de eventos de seguridad operacional a todo nivel en un tiempo oportuno.	0	1	2	3	4	5
8. Los resultados de las investigaciones se focalizan en hallar responsables en la primera línea de las operaciones y las medidas correctivas colocan un sobre-énfasis en los sucesos singulares.	0	1	2	3	4	5
9. Las personas en la institución conocen ampliamente los peligros que amenazan sus operaciones como resultado de la gestión de la información en seguridad operacional.	0	1	2	3	4	5
II. COMPONENTES DE GESTIÓN DE LA SEGURIDAD Y OPERACIONES						
10. La gestión de la seguridad es flexible (se ajusta) frente a los cambios institucionales y del entorno que podrían afectar su operación.	0	1	2	3	4	5
11. Las políticas institucionales de seguridad operacional hacen parte de la toma de decisiones del Alto Mando.	0	1	2	3	4	5
12. El soporte logístico de las operaciones se realiza de manera oportuna y eficaz.	0	1	2	3	4	5
13. El entrenamiento integral (reciente, suficiente y pertinente) del personal operativo es una prioridad de la institución.	0	1	2	3	4	5
14. Existe un adecuado equilibrio entre protección (seguridad) y producción (operaciones).	0	1	2	3	4	5
15. Se cuenta con procedimientos estándar para la ejecución de operaciones de vuelo, mantenimiento y entrenamiento.	0	1	2	3	4	5
16. El nivel de supervisión posee los estándares y entrenamiento necesario para realizar su labor de supervisión.	0	1	2	3	4	5

ÍTEM	ESCALA					
17. Los indicadores de seguridad operacional permiten mejorar procesos de la institución: ejecución de operaciones, entrenamiento, formación, procedimientos de operación, planificación, comunicación.	0	1	2	3	4	5
III. CULTURA DE SEGURIDAD						
3.1 Accesibilidad						
18. El informe de riesgos tiene una estructura sencilla y amigable.	0	1	2	3	4	5
19. Las personas sienten confianza en la institución para informar los riesgos de seguridad.	0	1	2	3	4	5
20. La dependencia que recopila y analiza los informes tiene autonomía respecto de aquella que determina las acciones correctivas o sanciones.	0	1	2	3	4	5
21. Se realiza una retroalimentación rápida, útil, accesible e inteligente a la institución.	0	1	2	3	4	5
22. Los informes proveen una información válida sobre los factores locales (a nivel unidades) e institucionales que promueven errores.	0	1	2	3	4	5
3.2 Legitimidad						
23. La institución tiene principios consensuados que trazan la frontera entre acciones aceptables e inaceptables.	0	1	2	3	4	5
24. Se imparten acciones correctivas independientemente de la(s) persona(s) involucrada(s) en el evento.	0	1	2	3	4	5
25. Las acciones correctivas se realizan a tiempo y responden a un orden lógico.	0	1	2	3	4	5
3.3 Adaptabilidad						
26. El mando jerárquico y centralizado cede el paso a la competencia técnica en momentos en que es preciso una toma de decisiones de nivel descentralizado y profesional, pero de amplia experticia técnica.	0	1	2	3	4	5
27. Las personas que ocupan cargos de supervisión están formadas para ser capaces de dirigir el trabajo de manera segura y productiva aun en ausencia de procedimientos estándar.	0	1	2	3	4	5
28. El nivel de supervisión se considera experto y confiable; tienen el respeto de la fuerza de trabajo y el respaldo del Alto Mando.	0	1	2	3	4	5
29. El personal de operaciones está entrenado en técnicas diseñadas para detectar la amenaza y evaluar el riesgo.	0	1	2	3	4	5
3.4 Aprendizaje						
30. Se pueden apreciar las mejoras a la organización y sus procesos (procedimientos, funciones, prácticas) como resultado de lecciones de seguridad aprendidas.	0	1	2	3	4	5

Gracias por su colaboración.

Anexo F. Instrumento para Validación de Expertos Escala SegOp

UNIVERSIDAD DE PALERMO - ARGENTINA

Doctorado en Psicología

Escala de valoración de la Percepción de seguridad operacional
en una institución de aviación militar

Autor: Reyes-Ávila I. & Poy, M. (2019a)

INSTRUMENTO PARA LA EVALUACIÓN PSICOMÉTRICA DE VALIDEZ DE APARIENCIA POR PARTE DE JUECES EXPERTOS	
NOMBRE DEL EXPERTO: _____ PROFESIÓN: _____	
○ DELIMITACIÓN DEL DOMINIO CONCEPTUAL ▪ Población objetivo: Pilotos, aviadores y técnicos de aviación militar ▪ Constructo evaluado: Percepción de seguridad operacional. ▪ Definición: Apreciación del estado en el que la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable mediante un proceso continuo de identificación de peligros y gestión de riesgos de la seguridad operacional. Se contemplan las siguientes componentes: ▪ Componente de Seguridad (9 ítems) ▪ Componente de Gestión de la seguridad y operaciones (8 ítems) ▪ Componente de Cultura de la seguridad (13 ítems)	
○ DEFINICIÓN DE ELEMENTOS OPERATIVOS DE LA ESCALA ▪ Estructura de la prueba: como instrumento escalar los ítems fueron contruidos con modalidad Likert referida en la práctica a proporción de ocurrencias de la variable como selección de alternativas, con ítems de selección única. ▪ Numero de reactivos: 30 ítems ▪ Forma de aplicación: Autoaplicable, (Cada individuo responde de manera independiente y sin considerar opinión externa). ○ Tiempo estimado de aplicación: 10-15 minutos.	
○ INSTRUCCIONES PARA LA VALIDACIÓN DE CONTENIDO DE LOS ÍTEMS ESTA ESCALA: 1. Pertinencia del ítem (Validez): Se refiere al criterio de validez de contenido o sea que el ítem sí corresponde a la variable respectiva. 2. Claridad del ítem (Redacción): este aspecto se refiere a que el ítem este adecuadamente formulado de manera que los términos utilizados sean claros tanto para quien diligencia como para quien contesta el instrumento. 3. Observaciones y sugerencias: Si tiene observaciones y sugerencias con respecto a los ítems y al cuestionario en general, por favor regístrelas. Si el espacio es insuficiente, use el reverso de la hoja o la parte inferior que aparece al final. A continuación, usted encontrará el cuestionario para evaluar las variables de la escala, dentro del cual se encuentran cada uno de los ítems que la conforman. Por favor señale con una X en la opción SI, si considera que el ítem cumple con lo estipulado y marque NO, en caso contrario. Agradecemos de antemano su colaboración y el tiempo dedicado al análisis de la escala, el cual pretende facilitar el estudio de condiciones cotidianas en la operación de la Institución.	

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Escala de Percepción de la seguridad operacional						
COMPONENTE DE SEGURIDAD						
-Compromiso						
26. La institución busca ser modelo en el sector de la aviación, en lo que concierne a buenas prácticas de seguridad.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Sí	No	Sí	No	
Escala de Percepción de la seguridad operacional						
27. Las decisiones de los comandantes dejan ver su genuino interés por mantener la seguridad.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
28. La institución aporta recursos humanos, técnicos y presupuestales idóneos para gestionar la seguridad.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
29. Independiente de los evesos, las acciones en seguridad operacional son continuas y permiten reformar y reforzar las defensas del sistema.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
-Gestión de la información						
30. El sistema de información de seguridad operacional produce información pertinente para la seguridad y permite sacar las conclusiones correctas (medidas reactivas).	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
31. El sistema de información de seguridad operacional proporciona chequeos regulares sobre procesos organizativos básicos (medidas proactivas) que puedan usarse para guiar acciones correctivas dirigidas a objetivos específicos.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
32. Se difunden los resultados de las investigaciones de eventos de seguridad operacional a todo nivel en un tiempo oportuno.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
33. Los resultados de las investigaciones se focalizan en hallar responsables en la primera línea de las operaciones y las medidas correctivas colocan un sobre énfasis en los sucesos singulares.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
34. Las personas en la institución conocen ampliamente los peligros que amenazan sus operaciones como resultado de la gestión de la información en seguridad.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
COMPONENTE DE GESTIÓN DE LA SEGURIDAD Y OPERACIONES						

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Escala de Percepción de la seguridad operacional						
35. La gestión de la seguridad es flexible (se ajusta) frente a los cambios institucionales y del entorno que podrían afectar su operación.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
36. Las políticas institucionales de seguridad hacen parte de la toma de decisiones del alto nivel.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
37. El soporte logístico de las operaciones se realiza de manera oportuna y eficaz.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
38. El entrenamiento integral (reciente, suficiente y pertinente) del personal operativo es una prioridad de la organización.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
39. Existe un adecuado equilibrio entre protección (seguridad) y producción (operaciones).	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
40. Se cuenta con procedimientos estándar para la ejecución de operaciones de vuelo, mantenimiento y entrenamiento.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
41. El nivel de supervisión posee los estándares y entrenamiento necesario para realizar su labor de supervisión.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
42. Los indicadores de seguridad operacional permiten mejorar procesos institucionales: ejecución de operaciones, entrenamiento, formación, procedimientos de operación, planificación y comunicación.	0. No sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
CULTURA DE LA SEGURIDAD						
- Accesibilidad						

Ítem	Opciones de respuesta	Pertinencia		Claridad		Observaciones
		Si	No	Si	No	
Escala de Percepción de la seguridad operacional						
43. El informe de riesgos tiene una estructura sencilla y amigable.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
44. Las personas sienten confianza en la institución para informar los riesgos de seguridad.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
45. La dependencia que recopila y analiza los informes tiene autonomía respecto de aquella que determina las acciones correctivas o sanciones.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
46. Se realiza una retroalimentación rápida, útil, accesible e inteligente a la institución.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
47. Los informes proveen una información válida sobre factores locales y organizacionales que promueven errores.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
- Legitimidad						
48. Se tiene principios consensuados que tracen la frontera entre acciones aceptables e inaceptables.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
49. Se imparten acciones correctivas independientemente de la persona que protagoniza el evento.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
50. Las acciones correctivas se realizan a tiempo y responden a un orden lógico.	0. no sabe, no conoce. 1. En ningún caso. 2. Casi nunca, en solo el 25% de los casos. 3. Parcialmente, casi en la mitad de los casos. 4. Casi totalmente, en la mayoría de los casos 5. Sí. en todos los casos					
-Adaptabilidad						

OBSERVACIONES Y SUGERENCIAS GENERALES:

Anexo G. Guía para la Realización de Grupos Focales y Entrevistas Semiestructuradas

Fase Cualitativa de Investigación

Se toma para la elaboración de esta guía, el formato general presentado por Hernández, Fernández y Baptista (2010).

Recomendaciones de Inicio

- Apague su teléfono celular, preséntese, platique sobre algún tema de interés.
- Comente al grupo focal o entrevistado sobre el proyecto, su objetivo general, el motivo por el cual fue seleccionado para realizar la entrevista y cómo se va a utilizar los datos.
- Háblele sobre la confidencialidad de la información y de sus datos, cuánto tiempo va a durar la entrevista. Una vez establecido el acuerdo, entregue el consentimiento informado, espere mientras cada persona lo lee y luego, pida verbalmente la aceptación de participación. En el caso de las entrevistas telefónicas, haga la lectura del consentimiento y pregúntele al entrevistado si desea participar voluntariamente en la investigación.

Durante la realización de la Entrevista y el Grupo Focal

Escuche atentamente y mantenga el flujo de la conversación demostrando interés por lo que dice el entrevistado y valorando sus respuestas. Tome notas y, si el entrevistado se lo ha permitido, grabe la entrevista.

Presente los resultados de la investigación e indague: si la información tiene sentido de acuerdo con su vivencia en la organización, si puede explicar el hallazgo, si tiene(n) ejemplos acerca del hallazgo, aspectos organizacionales que sostienen el hallazgo, dificultades de la organización para movilizar el hallazgo.

Al Final de la Entrevista y el Grupo Focal

Pregunte al entrevistado o al grupo focal si existe algo más que quiera agregar o alguna duda. Agradezca su tiempo y participación en el proceso.

Después de la Entrevista y el Grupo Focal

Haga un resumen de la información relevante obtenida durante la entrevista o grupo focal. Contextualice a quien entrevistó, revise sus notas de entrevista y trate de transcribir la

entrevista lo más rápido posible.

Revise la guía utilizada y realice mejoras si así lo considera.

Información Sociodemográfica

Fecha: _____ Hora: _____
Tiempo en la organización _____
Jerarquía del cargo: _____

Preguntas

1. ¿Cuál es su opinión general acerca de la seguridad operacional en su Unidad? ¿Y en la organización?
2. En la práctica ¿qué importancia percibe que le da la organización a la seguridad operacional?
3. En su concepto, ¿qué es lo que hace segura a una unidad operativa?
4. ¿Cuáles son las principales fisuras que usted puede identificar en el sistema de aviación que disminuye su nivel de seguridad operacional?

Con referencia a cada hallazgo específico, se siguió el siguiente protocolo de preguntas: ¿cómo pueden entender este hallazgo a la luz de la dinámica de la organización? ¿Pueden contarnos un ejemplo donde se pueda apreciar esta situación?

A partir de esta generalidad, se estableció una conversación que buscó ampliar la comprensión de conceptos e ítems.

Listado de hallazgos cuantitativos específicos indagados en la intervención

1. Baja percepción de desempeño resiliente.
2. Baja percepción de seguridad operacional.
3. Baja capacidad para anticipación.
4. Baja capacidad para aprender.
5. Baja Gestión de la información.
6. Entendimiento de relación entre clúster de incidentalidad y las variables PoDeRe y SegOp: Unidades con mayor incidentalidad puntúan más alto en PoDeRe y SegOp e inversamente.

7. Inexistencia de diferencia significativa en la percepción de PoDeRe y SegOp entre grupos que dirigen operaciones y operadores.
8. Relación entre antigüedad y percepción de PoDeRe y SegOp.
9. Apreciaciones sobre los resultados de correlación fuerte, positiva y predictiva entre PoDeRe y SegOp.

Los grupos focales duraron alrededor de dos horas; las entrevistas, en promedio, una hora.

Nota: La transcripción de esta fase con la casuística citada por los participantes solo se menciona parcialmente o no se menciona dentro de este documento, debido a que la institución no autorizó su difusión por considerarse de reserva institucional.

Anexo H. Consentimiento Informado

Estos cuestionarios hacen parte del proyecto doctoral “Relación entre el Potencial de Desempeño Resiliente y la Seguridad Operacional: Factores Organizacionales Contribuyentes”, realizado por la psicóloga Imelda Reyes Ávila, quien está optando al título de PhD en la Universidad de Palermo en Buenos Aires, (Argentina). El trabajo se desarrolla al interior de la organización de aviación militar y está respaldado por la dependencia responsable de la seguridad operacional.

El objetivo es establecer las relaciones entre potencial de desempeño resiliente y seguridad operacional y describir factores organizacionales contribuyente, para aportar un diagnóstico en términos de resiliencia, generar un modelo de seguridad operacional para la organización y sugerir acciones en pro de la seguridad operacional desde la perspectiva de función organizacional.

Se le invita a participar de manera activa y reflexiva, sus respuestas contribuirán al mejoramiento de la seguridad operacional desde la perspectiva de la ingeniería de la resiliencia. Si desea ampliar el alcance de este proyecto, diríjase a la entidad que rige la seguridad operacional.

La seguridad operacional es crucial en una organización cuya columna son las operaciones aéreas. Hace mucho tiempo, la seguridad dejó de ser una reflexión organizativa y pasó a ser una función de la organización que debe ser gestionada eficientemente para lograr sus objetivos.

Usted es considerado por la organización un piloto experimentado y conocedor tanto de las operaciones como de la seguridad operacional. Por lo tanto, queremos invitarlo a participar en esta investigación. Tenga en cuenta que su participación es totalmente voluntaria. Así que puede elegir participar, o no hacerlo de manera libre. Para su decisión, tome en cuenta que su participación es confidencial y anónima.

He leído la información proporcionada o me ha sido leída. He tenido la oportunidad de preguntar sobre ella y se me han contestado satisfactoriamente las preguntas que he realizado. Consiento voluntariamente participar en esta investigación como participante y entiendo que tengo el derecho de retirarme de la investigación en cualquier momento sin que me afecte en ninguna manera.

Nombre del Participante _____ Firma _____

Fecha _____ (Día/mes/año)

En el caso de las entrevistas y grupos focales, el investigador presentó a los participantes voluntarios el objetivo de la actividad, leyó el consentimiento y preguntó por su voluntariedad para participar. La información presentada proviene de las personas que manifestaron su consentimiento; sin embargo, no se obtuvo autorización de la organización para grabar las conversaciones derivadas de esta fase de la investigación.

Anexo I. Respuestas Directas de los Ítems de la Escala PoDeRe

➤ Capacidad responder

	No sabe		En ningún caso		Casi nunca <25%		Parcial. aprox. 50%		Casi total > 70%		Sí. todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Ítem1.1	13	2,4	5	,9	13	2,4	96	17,6	214	39,3	204	37,4	545
Ítem1.2	12	2,2	10	1,8	19	3,5	102	18,7	221	40,6	181	33,2	545
Ítem1.3	11	2,0	11	2,0	23	4,2	102	18,7	230	42,2	168	30,8	545
Ítem2.1	7	1,3	5	,9	21	3,9	115	21,1	244	44,8	153	28,1	545
Ítem2.2	6	1,1	7	1,3	20	3,7	98	18,0	266	48,8	148	27,2	545
Ítem2.3	7	1,3	6	1,1	22	4,0	111	20,4	260	47,7	139	25,5	545
Ítem3.1	13	2,4	8	1,5	18	3,3	80	14,7	258	47,3	168	30,8	545
Ítem3.2	14	2,6	5	,9	18	3,3	90	16,5	241	44,2	177	32,5	545
Ítem3.3	16	2,9	6	1,1	21	3,9	91	16,7	250	45,9	161	29,5	545
Ítem4.1	16	2,9	9	1,7	35	6,4	142	26,1	245	45,0	98	18,0	545
Ítem4.2	15	2,8	13	2,4	34	6,2	135	24,8	244	44,8	104	19,1	545
Ítem4.3	14	2,6	11	2,0	41	7,5	138	25,3	241	44,2	100	18,3	545
Ítem5.1	9	1,7	20	3,7	70	12,8	184	33,8	187	34,3	75	13,8	545
Ítem5.2	9	1,7	17	3,1	72	13,2	184	33,8	191	35,0	72	13,2	545
Ítem5.3	10	1,8	17	3,1	73	13,4	181	33,2	195	35,8	69	12,7	545
Ítem6.1	19	3,5	10	1,8	33	6,1	113	20,7	232	42,6	138	25,3	545
Ítem6.2	20	3,7	8	1,5	31	5,7	95	17,4	258	47,3	133	24,4	545
Ítem6.3	20	3,7	10	1,8	30	5,5	105	19,3	243	44,6	137	25,1	545

➤ Capacidad monitorear

	No sabe		En ningún caso		Casi nunca <25%		Parcial. aprox. 50%		Casi total > 70%		Sí. todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Ítem7.1	17	3,1	6	1,1	18	3,3	99	18,2	238	43,7	167	30,6	545
Ítem7.2	18	3,3	5	,9	24	4,4	87	16,0	243	44,6	168	30,8	545
Ítem7.3	18	3,3	5	,9	21	3,9	97	17,8	233	42,8	171	31,4	545
Ítem8.1	45	8,3	5	,9	20	3,7	91	16,7	236	43,3	148	27,2	545
Ítem8.2	46	8,4	6	1,1	19	3,5	99	18,2	234	42,9	141	25,9	545
Ítem8.3	46	8,4	5	,9	20	3,7	101	18,5	233	42,8	140	25,7	545
Ítem9.1	17	3,1	9	1,7	31	5,7	105	19,3	235	43,1	148	27,2	545
Ítem9.2	19	3,5	9	1,7	30	5,5	115	21,1	225	41,3	147	27,0	545
Ítem9.3	19	3,5	10	1,8	39	7,2	110	20,2	221	40,6	146	26,8	545
Ítem10.1	19	3,5	11	2,0	42	7,7	124	22,8	223	40,9	126	23,1	545
Ítem10.2	18	3,3	46	8,4	96	17,6	157	28,8	176	32,3	52	9,5	545
Ítem10.3	19	3,5	16	2,9	43	7,9	124	22,8	226	41,5	117	21,5	545
Ítem11.1	14	2,6	11	2,0	24	4,4	127	23,3	236	43,3	133	24,4	545
Ítem11.2	13	2,4	14	2,6	26	4,8	118	21,7	242	44,4	132	24,2	545
Ítem11.3	13	2,4	12	2,2	27	5,0	129	23,7	228	41,8	136	25,0	545
Ítem12.1	23	4,2	7	1,3	19	3,5	88	16,1	242	44,4	166	30,5	545
Ítem12.2	24	4,4	2	,4	21	3,9	90	16,5	245	45,0	163	29,9	545
Ítem12.3	26	4,8	4	,7	22	4,0	87	16,0	244	44,8	162	29,7	545
Ítem13.1	29	5,3	10	1,8	26	4,8	114	20,9	221	40,6	145	26,6	545
Ítem13.2	29	5,3	13	2,4	20	3,7	120	22,0	222	40,7	141	25,9	545
Ítem13.3	30	5,5	11	2,0	24	4,4	122	22,4	219	40,2	139	25,5	545

➤ **Capacidad de anticipar**

	No sabe		En ningún caso		Casi nunca <25%		Parcial. aprox. 50%		Casi total > 70%		Sí. todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Ítem14	11	2,0	13	2,4	37	6,8	126	23,1	221	40,6	137	25,1	545
Ítem15	17	3,1	34	6,2	53	9,7	158	29,0	192	35,2	91	16,7	545
Ítem16	11	2,0	6	1,1	20	3,7	96	17,6	243	44,6	169	31,0	545
Ítem17	8	1,5	8	1,5	26	4,8	102	18,7	224	41,1	177	32,5	545
Ítem18	12	2,2	29	5,3	70	12,8	181	33,2	178	32,7	75	13,8	545
Ítem19	5	,9	11	2,0	31	5,7	129	23,7	209	38,3	160	29,4	545

➤ **Capacidad de aprender**

	No sabe		En ningún caso		Casi nunca <25%		Parcial. aprox. 50%		Casi total > 70%		Sí. todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Ítem20	7	1,3	28	5,1	57	10,5	128	23,5	212	38,9	113	20,7	545
Ítem21	9	1,7	18	3,3	48	8,8	140	25,7	240	44,0	90	16,5	545
Ítem22	13	2,4	24	4,4	55	10,1	157	28,8	223	40,9	73	13,4	545
Ítem23	13	2,4	24	4,4	37	6,8	125	22,9	229	42,0	117	21,5	545
Ítem24	13	2,4	16	2,9	49	9,0	149	27,3	230	42,2	88	16,1	545
Ítem25	21	3,9	16	2,9	37	6,8	136	25,0	230	42,2	105	19,3	545

Anexo J. Respuestas Directas de los Ítems de la Escala SegOp y sus Subescalas

➤ I. Componentes de Seguridad

• Subescala: 1. Compromiso

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg1	9	1,7	6	1,1	20	3,7	74	13,6	216	39,6	220	40,4	545
Preg2	9	1,7	0	,0	51	9,4	109	20,0	225	41,3	151	27,7	545
Preg3	11	2,0	21	3,9	50	9,2	167	30,6	204	37,4	92	16,9	545
Preg4	7	1,3	6	1,1	24	4,4	104	19,1	274	50,3	130	23,9	545

• Subescala: 2. Gestión de la información

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg5	13	2,4	7	1,3	32	5,9	109	20,0	284	52,1	100	18,3	545
Preg6	19	3,5	13	2,4	27	5,0	121	22,2	260	47,7	105	19,3	545
Preg7	19	3,5	38	7,0	68	12,5	135	24,8	196	36,0	89	16,3	545
Preg8	28	5,1	26	4,8	47	8,6	125	22,9	218	40,0	101	18,5	545
Preg9	6	1,1	4	,7	31	5,7	138	25,3	255	46,8	111	20,4	545

➤ II. Componente de Gestión Seguridad y Operaciones

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg10	10	1,8	14	2,6	38	7,0	140	25,7	228	41,8	115	21,1	545
Preg11	9	1,7	7	1,3	26	4,8	90	16,5	226	41,5	187	34,3	545
Preg12	9	1,7	29	5,3	56	10,3	154	28,3	228	41,8	69	12,7	545
Preg13	8	1,5	16	2,9	51	9,4	133	24,4	219	40,2	118	21,7	545
Preg14	7	1,3	9	1,7	38	7,0	105	19,3	269	49,4	117	21,5	545
Preg15	2	,4	6	1,1	13	2,4	56	10,3	248	45,5	220	40,4	545
Preg16	7	1,3	6	1,1	16	2,9	99	18,2	266	48,8	151	27,7	545
Preg17	15	2,8	6	1,1	28	5,1	116	21,3	260	47,7	120	22,0	545

➤ III. Componente de Cultura de la Seguridad

• Subescala: 3.1 Accesibilidad

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg18	41	7,5	11	2,0	40	7,3	120	22,0	231	42,4	102	18,7	545
Preg19	28	5,1	61	11,2	74	13,6	149	27,3	163	29,9	70	12,8	545
Preg20	33	6,1	31	5,7	55	10,1	134	24,6	197	36,1	95	17,4	545
Preg21	19	3,5	22	4,0	62	11,4	157	28,8	199	36,5	86	15,8	545
Preg22	22	4,0	18	3,3	27	5,0	135	24,8	247	45,3	96	17,6	545

• Subescala: 3.2 Legitimidad

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg23	9	1,7	8	1,5	25	4,6	91	16,7	239	43,9	173	31,7	545
Preg24	17	3,1	21	3,9	41	7,5	108	19,8	236	43,3	122	22,4	545
Preg25	19	3,5	18	3,3	41	7,5	136	25,0	225	41,3	106	19,4	545

• Subescala: 3.3 Adaptabilidad

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg26	26	4,8	14	2,6	48	8,8	133	24,4	230	42,2	94	17,2	545
Preg27	8	1,5	14	2,6	22	4,0	110	20,2	273	50,1	118	21,7	545
Preg28	13	2,4	9	1,7	23	4,2	93	17,1	274	50,3	133	24,4	545
Preg29	7	1,3	11	2,0	25	4,6	123	22,6	250	45,9	129	23,7	545

• Subescala: 3.4 Aprendizaje

	No sabe		Ningún caso		Casi nunca <25%		Parcial, aprox 50%		La mayoría >70%		Sí, todos los casos		Total
	N	%	N	%	N	%	N	%	N	%	N	%	N
Preg30	4	,7	10	1,8	18	3,3	108	19,8	270	49,5	135	24,8	545

Anexo K. Análisis Cualitativo: Informe resumen de Segmentos Codificados (editado)

Tabla K1

Resumen con segmentos codificados (editado) – Transcripciones.mx20

Código	Segmentos codificados	Resumen
Baja percepción de desempeño resiliente	baja percepción de desempeño resiliente organización con amplia variedad de aeronaves multiplicidad de misiones no se perciban claramente las capacidades reales	La organización no ha pensado la seguridad desde el paradigma de la ingeniería de la resiliencia. No ha desarrollado consciente y sistemáticamente sus capacidades resilientes.
Baja percepción de desempeño resiliente \ características de la organización	acá la mentalidad no cambia con el grado; [... menor grado] No nos paramos a pensar por qué”. Toda esa carreta puede influenciar el pensamiento de la gente porque pueden pensar que la seguridad está para perseguirlos y tomar acciones con las personas “La percepción en el ambiente es que para qué se hace una junta de seguridad si hay otra persona tomando decisiones y no valida la decisión del cuerpo colegiado” “...La actitud es: pilas porque cualquier cosa me puede pasar”. “...Con cultura justa tiene que haber un responsable, pero ¿qué tan bueno sea para la organización? No debería buscarse una persona culpable sino ir más allá de eso. [...] No va a mejorar el sistema”. en ese escenario tratan de generar confianza, a sabiendas que las acciones de seguridad sobre el individuo no son bien recibidas. medidas más drásticas son justificables y se derivan de la pérdida de confianza de la organización en el operador y su toma de decisiones. quienes asesoran son los más antiguos y eso puede significar que el mando no esté bien retroalimentado [...] Poco se piensa en la idoneidad y no hay políticas claras con personas tan flotantes.	La cultura de la organización revela inflexibilidad en sus paradigmas. Se cuenta con procedimientos para actuar en seguridad operacional, pero muchas decisiones están sometidas a criterios temporales emitidos por cargos críticos. Es probable que se cuiden los parámetros de seguridad, más por evitar consecuencias sobre las personas que por evitar la consecuencia de los eventos.
Baja percepción de seguridad	las personas no valoran de manera positiva la gestión ...contamos con un SMS (Manual de Gestión de	Se cuenta con un SMS (Manual de Gestión de Seguridad Operacional) pero no hay una

Código	Segmentos codificados	Resumen
operacional	Seguridad Operacional) que es “bueno” hay mucho que aprender con el fin de seguir mejorando cambiar la manera de la institución de valorar la seguridad [...] no es fácil un accidente significa que no se está haciendo el trabajo. siempre se piensa en seguridad operacional reciclaje de comportamientos que entraña cierta dificultad [...] ...es sencillo tirarse una persona” “No hay claridad de cómo funcionan los procedimientos de seguridad de la organización...” hay una afectación real a la percepción de seguridad: [Las recomendaciones]...las plasmamos en un sistema de seguridad que manejan las personas responsables, pero eso la gente no lo sabe”. [...] “La percepción en el ambiente es que para qué se hace una junta de expertos si hay otra persona tomando decisiones y no valida la decisión del cuerpo colegiado” [...] [...] les falta educación en seguridad en ese escenario tratan de generar confianza, a sabiendas que las acciones de seguridad sobre el individuo no son bien recibidas. medidas más drásticas son justificables y se derivan de la pérdida de confianza de la organización en el operador y su toma de decisiones. quienes asesoran son los más antiguos y eso puede significar que el mando no esté bien retroalimentado [...] Poco se piensa en la idoneidad y no hay políticas claras con personas tan flotantes.	percepción positiva de la gestión en seguridad. Sistema en continuo aprendizaje, pero quizá no ha tenido momentos de estabilidad que le permitan definir hacia dónde dirigir sus mejoras. Las personas no tienen acceso al impacto organizacional de las decisiones de quienes dirigen la seguridad. Se debe desarrollar pensamiento crítico en el nivel de la toma de decisiones.
Capacidad para anticipación	el sistema tiene fortalezas en gestionar riesgos debilidad importante en su capacidad para identificarlos oportunamente gran desafío institucional evalúa los riesgos hace el panorama [...] de las pistas donde opera hay un diagnóstico de seguridad para cada [lugar]	Se percibe dificultad para anticiparse tanto a los riesgos como a las amenazas y oportunidades. No conocen el límite entre aceptable y no aceptable. No parece existir un modelo

Código	Segmentos codificados	Resumen
	y cada equipo [...]” riesgos adicionales y que tienen que ver con la antigüedad de la flota, los criterios para la ampliación de su vida útil y los mecanismos organizacionales utilizados para enfrentar esta realidad institución es reactiva no se anticipa reacciona a lo que pasa en el momento hay insuficiente personal y el que está atiende el “día a día”. Manifiestan preocupación porque “el día a día nos está comiendo” Las personas encargadas de proyectar la organización también están en el día a día. práctica normal restringir más que evaluar y gestionar riesgos difícil observar la gestión de los líderes A futuro, muchas realidades más que riesgos se convertirán en limitaciones. las personas no saben con claridad qué es aceptable y qué no, en términos de riesgo	claro de futuro. Las personas responsables de la seguridad operacional realizan sus tareas para gestionar los riesgos, pero hay otras variables externas que afectan significativamente la operación y que, al momento, no han sido gestionadas por el nivel directivo. La organización es reactiva. Las personas que deberían estar pensando estratégicamente la seguridad están envueltas en tareas administrativas rutinarias.
Capacidad para aprender	convertirse en una comunidad de aprendizaje capaz de analizar lo que le pasa modificarse pasar de acumular datos a conocer qué le ocurre como sistema para modificar su propio comportamiento el aprendizaje solo se recoge de los eventos que salen mal se construyen alertas necesarias para evitar situaciones similares se ha incrementado la cultura de reporte reportes pueden ser muchos y eso hace que se pierda el aprendizaje la organización valora mejor las unidades que reportan más eventos y eso puede causar ese incremento en el número de reportes responsabilidades administrativas disminuyen la capacidad de aprender. personas deben estar en las operaciones y en el funcionamiento administrativo de la organización, culturalmente se favorece más lo segundo que lo primero En ese desbalance, se pueden sacrificar prácticas clave para la seguridad de las operaciones. más crítico en la medida en que las personas	La Fuerza proyecta convertirse en una comunidad de aprendizaje capaz de transformar datos en información que le permita transformarse. En el momento, el aprendizaje gira alrededor de los eventos adversos. Hay cultura de reporte, pero se cuestiona su eficacia en la prevención porque pueden ser muchos y no se conoce su impacto práctico en la seguridad. El aprendizaje no es oportuno y a veces, no es efectivo pues eleva temporalmente el nivel de alerta y luego vuelve a bajar. El cúmulo de responsabilidades administrativas también disminuye la capacidad para aprender: entre más tiempo en la organización, más tiempo en lo administrativo y menos

Código	Segmentos codificados	Resumen
	avanzan en su desarrollo dentro de la organización el tiempo de permanencia en la organización es inversamente proporcional al tiempo en que se está en las operaciones y en contacto con la seguridad “la gente se queja mucho de que no les contamos lo que pasó con los accidentes”. No se sabe si se hizo algo efectivo, [...] No hay un análisis de amenazas y oportunidades”. la institución aún es muy reactiva las personas hacen un aprendizaje y como efecto inmediato se incrementa el estado de alerta, pero luego se vuelve a relajar “Hace 50 años tuvimos el mismo accidente, ¿cómo es posible que vuelva a suceder? Entonces no tenemos esas características de resiliencia”, dejar las recomendaciones de las investigaciones de eventos plasmadas en algo que no se pierda en el tiempo, como procedimientos estándar de operación.	tiempo en las operaciones. Sin embargo, la organización privilegia lo administrativo sobre lo operacional.
Gestión de la información	manejo de la información [...] buscar mayor oportunidad y precisión básico para gestionar la capacidad de aprendizaje se sube la información de eventos y contiene la data de muchos años y, en ese sentido, se ha mejorado no es tan evidente que haya proceso de análisis Existe posibilidad de que en el ámbito académico se retome esta información, calidad del dato como otro tema que preocupa Preguntarse si se están recogiendo datos que aporten a la seguridad porque si no es así, el resultado tampoco va a ser de valor para la seguridad importancia de auditar este sistema de información, actividad que no saben si la contempla el sistema o no no saben dónde reposa el análisis del sistema en un evento [...] altamente probable que no se evalúe al sistema El hecho de buscar una persona, oculta que la responsabilidad también es de quien está buscando al culpable En evento menores se mira la persona. En accidentes sí se mira la organización”. sí se realizan, pero sobre los briefings de vuelo en la preparación del vuelo, se sigue operando sin	El manejo de información necesita ganar oportunidad y precisión. El manejo de información también está supeditado a políticas institucionales del momento. El nivel directivo de la organización no comunica las acciones y conclusiones derivadas de los accidentes. El sistema contiene datos de muchos años de eventos, pero no es tan evidente el proceso de análisis o el impacto que esto ha tenido en el mejoramiento de procesos y a la seguridad operacional. No se conoce si existe un procedimiento de auditoría al sistema que permita su mejoramiento. La orientación de las investigaciones se dirige a las personas, pero no claramente a procesos y procedimientos que generen seguridad.

Código	Segmentos codificados	Resumen
	despacho y con información limitada La organización creó un mecanismo para dar más información al operador de primera línea, pero se utiliza solo como medio de consulta accesibilidad depende del líder personas se sienten cohibidas para informar por su deseo de evitar dificultades cosas estén sometidas a criterio de unos pocos hace que no haya claridad respecto de lo que puede suceder cuando se ve incurso en un evento adverso “No hay claridad de cómo funcionan los procedimientos de seguridad de la organización...” Los reportes son vistos como una radiografía de una realidad institucional, reportar es algo que la gente hace, pero no siempre Hay temor a reportar debería ser anónimo debería difundirse ampliamente el resultado de esa información sobre la mejora de procesos, lo cual no es muy claro. los resultados de las investigaciones se centran en factores humanos o de mantenimiento. poco frecuente ver en un informe un análisis sobre factores organizacionales involucrados.	Se percibe temor para informar por falta de claridad en la objetividad de los procedimientos de seguridad. Los reportes pueden no ser una radiografía de la organización porque las personas no siempre reportan.
Clúster de incidentalidad H2	cuando alguien tiene una vivencia adversa, tiende a aprender de ello “Ese tipo de cosas hace que las personas piensen más en lo que están haciendo”. “sí podríamos decir que entre más incidentalidad, mayor aprendizaje, pero en el corto plazo”. alta rotación [...] cuando les ocurre algo adverso, logran adquirir esa cultura de seguridad: “...y ellos pueden tener ese sentimiento más bajo de percepción de seguridad porque se creen invulnerables” cuando ocurre un evento, es más probable que las personas perciban cómo toda la dinámica organizacional Si no ocurre un evento adverso, las personas pueden saber que el sistema está ahí pero no ven cómo se manifiesta es posible que frente a los eventos y a la incidentalidad haya más conciencia porque se	A juicio de los participantes, varias lógicas institucionales dan cuenta del hallazgo de la hipótesis 2. Por un lado, encuentran una relación entre mayor percepción de PoDeRe y SegOp en unidades con mayor incidentalidad basados en el factor aprendizaje: los eventos adversos generan aprendizaje, aunque muchas veces este se da en el corto plazo. De otro, muchas personas no requieren que pase algo para que cuiden sus parámetros de seguridad. Esta es una realidad cuyas implicaciones no ha sido abordada por la organización. Otro aspecto importante es que la ocurrencia de un evento

Código	Segmentos codificados	Resumen
	puede apreciar la interacción de todos los elementos de seguridad. [...] [...] práctica del alto mando dirigida a responsabilizar a las personas de sus acciones o inacciones evitar que esta manera de intervenir no sea vivida como punitiva por las personas en la organización: “No está mal que las personas deban responder por sus acciones sin querer decir que nos vamos a volver totalmente punitivos o que vamos a desconocer la naturaleza humana...” “cultura justa”, orientado a que esa imputación de responsabilidad se dirija a aquellas personas que cometan violaciones o faltas muy extremas “Tiene que ser así. El día que la organización o la autoridad no se demuestre o sea blanda, el sistema o la percepción de cultura de seguridad de la gente se cae”. conscientes de que hay una afectación real a la percepción de seguridad “Toda esa carreta puede influenciar el pensamiento de la gente porque pueden pensar que la seguridad está para perseguirlos y tomar acciones con las personas y no con la organización porque ellos no saben qué acciones tomamos con la organización... [...].” pareciera que el procedimiento de cultura justa es para sancionar, no para tomar acciones correctivas anteriormente las acciones se tomaban sobre los procedimientos, no sobre las personas. “Con cultura justa tiene que haber un responsable, pero ¿qué tan bueno sea para la organización? No debería buscarse una persona culpable sino ir más allá de eso. [...] No va a mejorar el sistema”.	adverso evidencia el funcionamiento del sistema y esto puede contribuir a percibir mayor seguridad operacional. La política institucional de “cultura justa” también puede contribuir a incrementar la percepción de seguridad por cuanto se toman acciones sobre personas y esto funciona de manera disuasiva en el personal operativo.
Dirección vs Operadores H3	todas las personas que lideran las operaciones “Él vivió lo mismo que el que está operando y por eso no percibe ninguna diferencia El comandante de aeronave es comandante desde pequeño y él también lidera la operación. Por eso no se presentan diferencias”. El grupo de menor antigüedad no ha vivido tantos eventos adversos y, si les ocurre, pueden recuperarse rápidamente. Los de antigüedad intermedia, perciben menos resiliencia y seguridad porque “...recuerdan los accidentes”.	A juicio de los participantes, varias lógicas institucionales dan cuenta del hallazgo de la hipótesis 3. Por un lado, quienes dirigen las operaciones, también son operadores. De otra parte, las personas de menor antigüedad militar no han experimentado la complejidad de la operación y sus riesgos inherentes por lo

Código	Segmentos codificados	Resumen
	Una persona con mayor tiempo en la organización tiene “una carga de accidentes desde el más obvio hasta el más inverosímil”, “lo hemos vivido una y otra vez” [...] [...] A medida que va conociendo se da cuenta que el accidente más inverosímil puede pasar. Los nuevos son muy confiados, después llega el periodo de desconfianza y luego se da cuenta que la [...] organización tiene muchas cosas y recupera la confianza”. “Los recién llegados no conocen tanto. Creen que con lo que hay es suficiente. experiencia en la operación ya se dan cuenta que las operaciones son mucho más complejas de lo que se pensaba. Cuando avanza se va dando cuenta que la [...] institución no es perfecta, pero sí tiene muchos controles que me ayudan a ser resiliente”. [...] Las personas que están en la mitad de su carrera conocen el antes y el después de la seguridad, pueden establecer un valor diferencial. [...] “Como llegaron [los menos antiguos] ya tienen un sistema de seguridad, entonces eso ni me va ni me viene: ya tienen un sistema. Los de la mitad sí lo cuestionan porque siempre viene la comparación. Ya los altos están buscando algo que tienen que apoyar el cambio...” los menos antiguos están más conectados con el tema operacional y eso les puede permitir ver lo que está bien. Los más antiguos tienen más experiencia, pero otra visión de las cosas porque están inmersos en otras tareas propias de la organización. el miembro poco antiguo de la organización no es tan consciente de las implicaciones de todo. Los más antiguos perciben las cosas a su nivel, casi como si todo estuviera bien Los de antigüedad intermedia, ven cómo funciona la institución y las dificultades provenientes de arriba y debajo de ellos en la jerarquía de la institución. [...] [...]	que puede percibir mayor seguridad operacional. Los de antigüedad intermedia, pueden percibir mayor probabilidad de que algo pueda ocurrir lo que disminuye su percepción de seguridad. Por último, los de mayor antigüedad se encuentran más al frente de tareas administrativas que operativas por lo que su percepción de seguridad operacional puede ser media.

Código	Segmentos codificados	Resumen
	toda estructura militar las personas son de “quitar y poner” [...]	
Resiliencia y seguridad (H1 y H4)	adquirir la capacidad de detectar riesgos, o sea, anticipar. más capacidad de anticipación se adquiriera como institución, mejores van a ser los resultados en seguridad: El resto de las cosas, las hacemos bien. No hay un riesgo que no le hagamos nada. Una vez diagnosticado los gestionamos los resultados nos muestran lo que ya sabíamos, pero ahora está sobre datos interesante aporte el poder precisar las acciones de seguridad sobre funciones específicas de la organización.	La relación entre la variable potencial de desempeño resiliente y seguridad operacional no suscitó mayores comentarios por el desconocimiento del concepto. Los escenarios presentados como función predictiva corresponden, según los participantes, a observaciones ya conocidas por ellos, pero la investigación les permite precisar acciones de seguridad sobre funciones específicas de la organización.