

Cuando el servicio se interrumpe, la confianza está en juego

Banca, finanzas y seguros / 8 páginas / 3 de octubre de 2026

Decisión propuesta: tratar la información a los clientes como un componente de la continuidad del servicio.

Lo que debilita la confianza

Una interrupción del servicio deja a los clientes frente a decisiones inmediatas: esperar, intentar, llamar o buscar una alternativa. Si la información no les ayuda a elegir, un fallo técnico también se convierte en una experiencia de abandono. La comunicación debe estar conectada con las operaciones y la relación cliente desde el momento en que se preparan los dispositivos de resiliencia.

Decisión recomendada

El Comité valida una base de hecho única, responsabilidades de publicación y un ritmo de actualización adaptado a la situación. Los equipos competentes determinan las obligaciones reglamentarias; la comunicación organiza la coherencia de las explicaciones a los públicos. La prioridad no es producir una fórmula tranquilizadora, sino dar una información exacta, útil y revisable.

Decisiones necesarias

Designar un responsable del estado de los hechos, un responsable de la información al cliente y un portavoz. Definir los canales de socorro, las modalidades de asistencia a los públicos frágiles y el procedimiento de corrección de los mensajes erróneos. Prever una restitución después de incidente que distinga vuelta del servicio, resolución de las consecuencias individuales y acciones de prevención.

CLAVE PARA DECIDIR

¿Puede un cliente entender lo que debe hacer sin conocer la organización interna de nuestro grupo?

La resiliencia es también una experiencia pública

La disponibilidad del sistema, la continuidad de las operaciones y la comprensión de los clientes deben examinarse conjuntamente.

Un desafío que va más allá del ataque cibernético

El primer panorama de los principales incidentes denunciados en el marco de DORA, publicado por las autoridades europeas en 2026, subraya en particular el papel de las deficiencias de sistemas, de los acontecimientos externos y de las dependencias de los proveedores [1]. Por lo tanto, la preparación no debe limitarse a un escenario de intrusión. Una migración, un fallo de un tercero o un error de configuración también pueden requerir una respuesta coordinada.

Consecuencias diferentes para el público

La misma indisponibilidad puede impedir que un particular pague, una empresa de ejecución de una operación o un empleado responda a una solicitud. El mensaje general debe completarse con instrucciones pertinentes para estas situaciones. El banco o el asegurador debe distinguir también a las personas efectivamente afectadas de las que se preocupan sin estar involucrados.

No confundir tranquilidad con certeza

Una fórmula tal como todo es seguro, puede superar lo que la encuesta permite establecer. Es más útil indicar las características en cuestión, los elementos comprobados y la conducta a seguir. La comunicación puede reconocer la incertidumbre mientras muestra una organización: quien trabaja, qué información se actualizará y cómo acceder a una ayuda.

CLAVE PARA DECIDIR

La confianza también depende de la capacidad de hacer que una situación incierta sea viable para el cliente.

Un estado de los hechos, varias respuestas útiles

La coherencia no consiste en enviar el mismo texto a todos los destinatarios.

Construir la base común

El estado de los hechos menciona la hora de detección, los servicios asignados, el perímetro confirmado, las medidas tomadas y las desconocidas. Se edita y se concede su validación. Los colaboradores que responden a los clientes deben acceder a una versión actualizada sin esperar una circulación informal de correos electrónicos.

Adaptar la respuesta sin alterar los hechos

Los clientes necesitan instrucciones y asistencia. Los trabajadores necesitan saber qué decir y dónde orientar. Los medios de comunicación esperan una explicación pública y una posibilidad de seguimiento. Las autoridades reciben la información determinada por los procedimientos aplicables. Las validaciones y los horarios deben coordinarse, sin presentar una comunicación pública como sustituto de una notificación reglamentaria.

Prever el funcionamiento en modo degradado

El sitio, la aplicación o la herramienta de envío habitual puede no estar disponible. Es necesario probar los canales de emergencia y los medios de deautenticación de los mensajes. Las comunicaciones de incidente pueden ser explotadas por los estafadores: las instrucciones deben orientar a puntos de contacto conocidos y evitar d hacer que los clientes transmitan secretos o códigos.

Público	Necesidad prioritaria	Responsable de coordinación
Clientes	Impacto y actuación	Relación con clientes y operaciones
Empleados	Instrucciones y orientación	Comunicación interna
Medios	Hechos y próxima actualización	Relaciones con medios
Autoridades	Información requerida	Cumplimiento y equipos autorizados

CLAVE PARA DECIDIR

Una sola cronología de referencia; mensajes adaptados a las necesidades de cada público.

Responder a tres situaciones

Los siguientes escenarios son ilustrativos y sirven para preparar una organización, sin describir un incidente real.

Pagos no disponibles, causa aún desconocida

La primera respuesta explica el impacto constatado, las alternativas realmente disponibles y la hora del siguiente punto. No promete un plazo de resolución no confirmado. El Comité decide el nivel de movilización de la asistencia, los públicos que deben ponerse en contacto directamente e información que puede publicarse antes de la conclusión técnica.

Un rumor de fuga de datos acompaña a la avería

No es suficiente para establecer una exfiltración. Los equipos autorizados evalúan la situación y la comunicación evitan tanto confirmar sin pruebas como desmentir prematuramente. Los mensajes deben especificar el alcance de cada afirmación: - no hemos identificado a - - no es sinónimo de - - - no existe ningún riesgo - . Las personas afectadas reciben las instrucciones adecuadas cuando los hechos lo permiten.

Una decisión comercial impopular reaviva la crítica

Una evolución arancelaria anunciada después de un incidente puede considerarse desconectada de la experiencia del cliente. El Comité debe examinar el calendario, la explicación económica y las posibilidades de recurso o de acompañamiento. La comunicación no puede resolver sola una contradicción entre el servicio prestado y la decisión tomada. Debe hacer visible esta contradicción antes de la publicación.

CLAVE PARA DECIDIR

¿El discurso público sigue siendo defendible ante el cliente que ha sufrido la consecuencia más concreta?

Preservar la relación después de la vuelta del servicio

El final del incidente técnico no siempre es el final del incidente para las personas afectadas.

Distinguir tres pasos

La recuperación describe el retorno de las funciones. Remediación trata las consecuencias individuales, las operaciones que hay que verificar o las reclamaciones. El aprendizaje se centra en las causas y acciones de prevención. Mezclar estos pasos puede llevar a anunciar una resolución completa mientras que los clientes todavía están esperando una respuesta.

Explicar una decisión sensible

El cierre de la agencia, la evolución de la cobertura o una modificación del servicio deberán presentarse con sus motivos, su calendario y sus consecuencias prácticas. El carácter legal o contractualmente posible de una decisión no basta para hacerla comprensible. Los equipos de campo deben poder responder a las situaciones particulares o orientar hacia un procedimiento claramente definido.

Dar cabida a los asuntos públicos

Las relaciones institucionales ayudan a comprender las expectativas del territorio, los retos que plantea el acceso a los servicios y las preocupaciones de los responsables de la toma de decisiones públicas; deben articularse con la experiencia real de los clientes y la comunicación local; el Comité se gana en distinguir entre las obligaciones, los compromisos voluntarios y las opciones sobre las que sigue siendo posible un diálogo.

CLAVE PARA DECIDIR

Un anuncio de resolución debe aclarar lo que se ha restablecido y lo que queda por tratar.

Organizar las pruebas de confianza

Una reputación sólida requiere información que los públicos puedan encontrar, entender y verificar.

Relaciones con los medios de comunicación

El portavoz debe disponer de una cronología, un perímetro y un vocabulario común con los expertos. Las respuestas a los periodistas deben separar los hechos establecidos de las hipótesis. Después del incidente puede ser útil una explicación de las acciones emprendidas; no debe revelar elementos que faciliten un ataque ni anunciar garantías absolutas.

Una presencia digital sin contradicciones

Las páginas de ayuda, los mensajes de la aplicación, el sitio institucional y las publicaciones sociales deben remitir a una información de referencia. Las antiguas instrucciones de incidente deben ser fechadas y clausuradas. Un motor o IA puede, de lo contrario, devolver una situación pasada como actual. El trabajo GEO comienza con la exactitud, disponibilidad y coherencia de estos contenidos [2].

Observaciones orientadas a la utilidad

Probar las preguntas que los públicos hacen realmente: servicio disponible, procedimiento de asistencia, distinción entre marcas, modalidades de contacto. Revisar las respuestas erróneas y las fuentes utilizadas, sin reproducir datos personales en las pruebas. La frecuencia de cita de una marca no dice si un cliente recibe una consigna segura y aplicable.

CLAVE PARA DECIDIR

La información correcta, fechada, sobre el perímetro correcto y accesible desde los canales que el cliente utiliza.

90 días para poner en funcionamiento el dispositivo

El programa propuesto debe coordinarse con los procedimientos de continuidad y gestión de los incidentes existentes.

Primer mes: establecer la base

Comparar los procedimientos oficiales con el recorrido real de un cliente durante una interrupción. Identificar los canales no disponibles al mismo tiempo, los responsables no suplidos y los mensajes contradictorios. Examinar también los últimos motivos de reclamación y las preguntas repetidas a los equipos de campo. El diagnóstico debe conducir a una lista de correcciones atribuidas.

Segundo mes: poner a prueba

Realizar un ejercicio que combine operaciones, seguridad, conformidad, relaciones con el cliente, recursos humanos y comunicación. Hacer evolucionar la información durante la sesión. Verificar la publicación de un primer mensaje, su corrección y la coordinación de los canales. Evaluar la capacidad para decidir con una información parcial en lugar de la recitación de un escenario aprendido.

Tercer mes: consolidar el seguimiento

Actualizar las instrucciones, capacitar a los sustitutos y probar los medios de socorro. Preparar un modelo de balance diferenciado consecuencias para los clientes, calidad de la información y mejoras operativas. El Comité sigue las desviaciones no resueltas y valida los medios que faltan. Los ejercicios siguientes deben variar las situaciones para no crear una ilusión de preparación.

CLAVE PARA DECIDIR

El dispositivo se mantiene cuando la herramienta habitual o el titular de un papel clave no está disponible.

Medir lo que protege la relación

Los indicadores deben iluminar la experiencia del público tanto como la velocidad de publicación.

Medidas recomendadas

Seguir el tiempo transcurrido entre la confirmación de un impacto y la información útil, la coherencia entre canales, las solicitudes repetidas por falta de explicación y el tratamiento de las consecuencias individuales. Mantener las bases de cálculo y distinguir los incidentes según su perímetro. Una media global no debe ocultar una situación grave para un público restringido.

Interpretar con precaución

Un aumento de los contactos puede indicar una preocupación, pero también una mayor visibilidad de la asistencia. Una disminución de las menciones públicas nsj no establece por sí sola un retorno de la confianza. El Comité cruza las observaciones de comunicación con los datos de servicio y las devoluciones de los equipos habilitados.

La decisión que debe formalizarse

Validar las responsabilidades del estado de los hechos, los canales de emergencia y las normas de cierre. Solicitar un retorno de ejercicio que muestre un error detectado, una decisión tomada y una mejora efectiva puesta en práctica. El objetivo es hacer que el dispositivo verificable antes del próximo incidente.

La comunicación de confianza da a las personas los medios para comprender y actuar, incluso cuando el servicio está debilitado.

Fuentes y referencias

[1] ESMA, EBA, EIOPA — First report on DORA major ICT-related incidents

[2] Google Search Central — AI features and your website

Análisis y recomendaciones de Belief System. Los escenarios son ilustrativos. Las fuentes aportan contexto; no suponen una validación de nuestras recomendaciones.