TALLER DE CIBERSEGURIDAD

Evolución y mejoras para un BCP (Plan de continuidad del negocio) robusto y adaptable

Paolo Jeldres R.
Jefe de Seguridad de la Información y Ciberseguridad

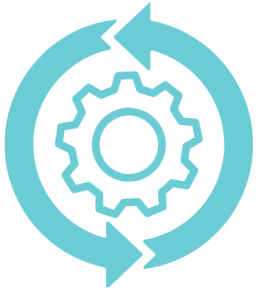
16 Octubre 2024

ChileCompra

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

TALLER DE CIBERSEGURIDAD

¿Qué es un BCP?



Es un **Plan de Continuidad de Negocio** que entrega a la organización la capacidad de continuar con su oferta de productos y servicios dentro de un período de tiempo aceptable a una capacidad predefinida durante una interrupción (por ejemplo, un incidente de ciberseguridad).

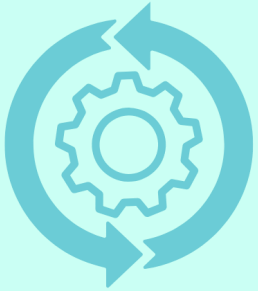
Fuente: Norma ISO 22301:2019

TALLER DE CIBERSEGURIDAD

¿Qué es un BCP?

TALLER DE CIBERSEGURIDAD

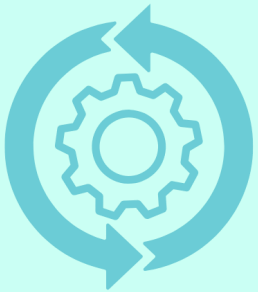
¿Qué es un BCP?



Por lo tanto,
¿Por qué es necesario un BCP?

TALLER DE CIBERSEGURIDAD

¿Qué es un BCP?



"Solo hay dos tipos de empresas: las que ya fueron hackeadas y las que lo van a ser"

Robert Muller, ex director del FBI

TALLER DE CIBERSEGURIDAD

¿Qué es un BCP?

Google incidente de ciberseguridad

Cooperativa.cl

CCU fue víctima de un "incidente de ciberseguridad"

El miércoles 25 de septiembre CCU "tomó conocimiento que algunos de sus sistemas informáticos -en las áreas de venta y distribución- se vieron...

hace 2 semanas

BioBioChile

Isapre Colmena reporta "incidente de ciberseguridad" que afectó servicios a usuarios

Este incidente en Colmena se suma a una falla masiva reportada en varios bancos, incluyendo BancoEstado, Banco Falabella, Banco Santander y...

28 jun 2024

La Tercera

Itaú reporta incidente de ciberseguridad que podría afecta a clientes de RappiCard

Itaú reporta incidente de ciberseguridad que podría afecta a clientes de RappiCard · Quién era José Menéndez, el ejecutivo del entretenimiento...

4 jul 2024

Diario Financiero

CMF asegura que incidente fue informado el 10 de mayo e instruye entregar detalles

La Comisión para el Mercado Financiero (CMF) requirió a Santander Chile informar la profundidad de la afectación, las medidas que está...

14 may 2024

www.revistaeyn.com

Un 30 % de las organizaciones sufrió al menos un incidente de ciberseguridad en 2023

El ESET Security Report (ESR) revela que el 30 % de las organizaciones latinoamericanas sufrió al menos un incidente de seguridad en 2023, y que...

La Cuarta

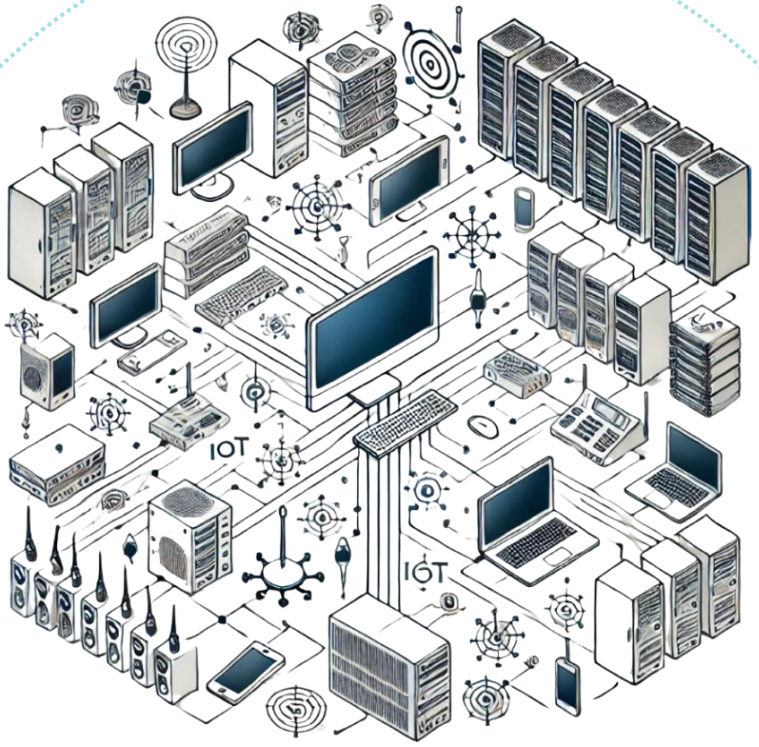
NIC Chile avisa de incidente de ciberseguridad: “Atacante aprovechó debilidad de algunas contraseñas”

NIC Chile avisa de incidente de ciberseguridad: “Atacante aprovechó debilidad de algunas contraseñas” · Supuesto video sexual habla por sí solo:...

4 jul 2024

TALLER DE CIBERSEGURIDAD

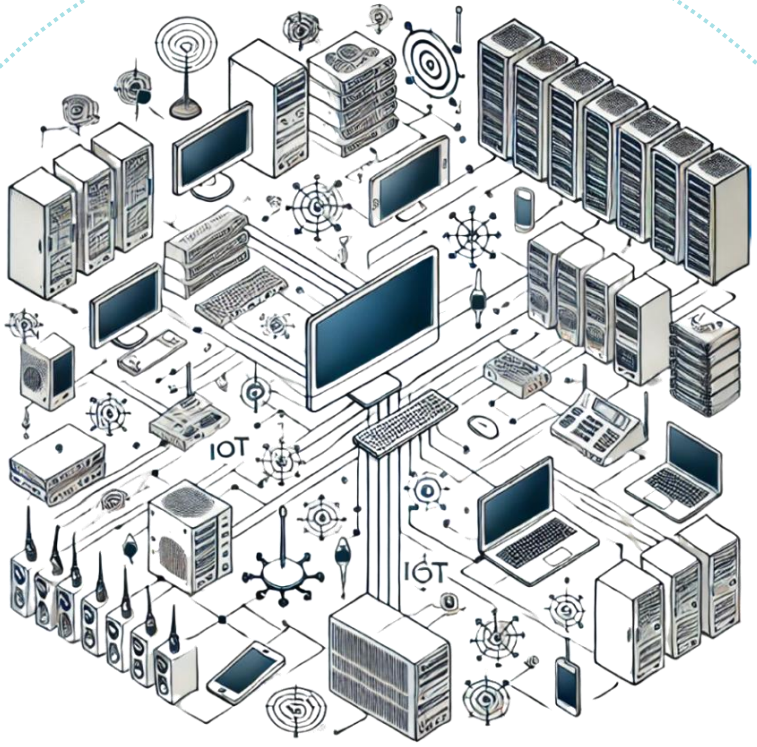
Más y más dispositivos conectados a la red



Aumento de superficie de ataque

TALLER DE CIBERSEGURIDAD

Más y más dispositivos conectados a la red



Aumento de superficie de ataque

+ AI

TALLER DE CIBERSEGURIDAD

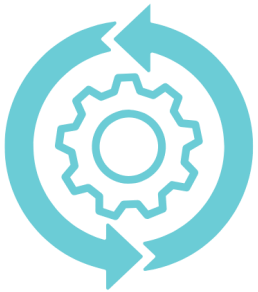
Respondiendo,
¿Por qué es necesario un BCP?

Porque

"Solo hay dos tipos de empresas: las que ya fueron hackeadas (y las van a volver a hackear) y las que lo van a ser"

TALLER DE CIBERSEGURIDAD

¿Cómo funcionó la ejecución del BCP en ChileCompra durante el incidente de septiembre de 2023?



TALLER DE CIBERSEGURIDAD

¿Cómo funcionó la ejecución del BCP en ChileCompra durante el incidente de septiembre de 2023?

El documento del BCP NO funcionó; las personas SI

TALLER DE CIBERSEGURIDAD

¿Qué hicimos posterior al incidente?

Mirada externa

TALLER DE CIBERSEGURIDAD

Diagnóstico

18 oportunidades de mejora en el ámbito de la seguridad de la información o ciberseguridad = **18 iniciativas o proyectos**

TALLER DE CIBERSEGURIDAD

Uno de los proyectos seleccionados a ejecutar:

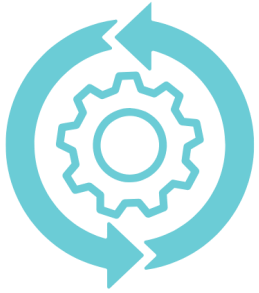
P09	Continuidad	Desarrollar un plan de continuidad se negocios (BCP) que considere el levantamiento de las necesidades de resiliencia de los procesos de la institución. Desarrollar igualmente, plan de recuperación de desastres (DRP).	**A**

TALLER DE CIBERSEGURIDAD

Plan de seguridad institucional

Controles de seguridad

Concientización



Plan de continuidad del negocio

TALLER DE CIBERSEGURIDAD

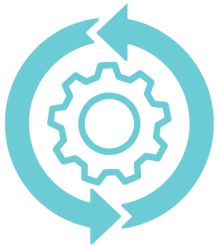
Mes/Año	Hito
Septiembre 2023	Incidente / Recuperación
Octubre 2023	Verificación recuperación
Noviembre – Diciembre 2023	Análisis de oportunidades de mejoras
Enero 2024	Inicio consultorías externas
Febrero – abril 2024	Diagnóstico
Mayo 2024	Presentación resultados diagnóstico y elección proyectos a ejecutar
Junio 2024	Definición de un Plan de seguridad institucional

TALLER DE CIBERSEGURIDAD

Mes/Año	Hito
Septiembre 2023	Incidente / Recuperación
Octubre 2023	Verificación recuperación
Noviembre – Diciembre 2023	Análisis de oportunidades de mejoras
Enero 2024	Inicio consultorías externas
Febrero – abril 2024	Diagnóstico
Mayo 2024	Presentación resultados diagnóstico y elección proyectos a ejecutar
Junio 2024	Definición de un Plan de seguridad institucional
Julio 2024	Desarrollo de la primera versión del BCP
Agosto 2024	Ejecución de la prueba BCP junto al DRP

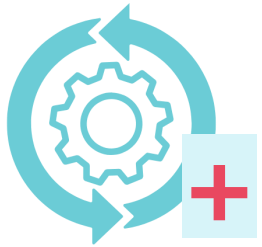
TALLER DE CIBERSEGURIDAD

¿Cómo empezamos el proyecto de evolución del Plan de continuidad del negocio (BCP)?



A

Planificar un sistema de gestión de continuidad del negocio a partir de la Norma ISO 22301

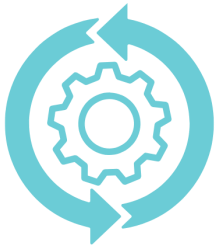


B

Generar un producto mínimo viable de la alternativa a)

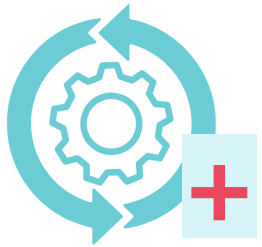
TALLER DE CIBERSEGURIDAD

¿Cómo empezamos el proyecto de evolución del Plan de continuidad del negocio (BCP)?



A

Planificar un sistema de gestión de continuidad del negocio a partir de la Norma ISO 22301.

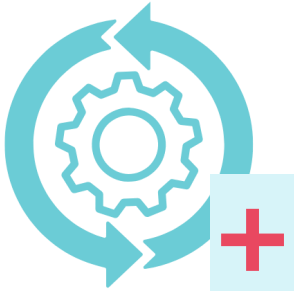


B

Generar un producto mínimo viable de la alternativa a)

TALLER DE CIBERSEGURIDAD

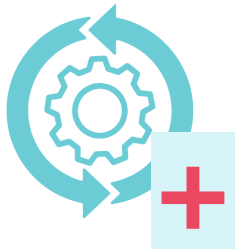
Objetivo



Para el día de la prueba **(10 de agosto)** disponer de un **Plan de continuidad del negocio** que incorpore los siguientes elementos:

TALLER DE CIBERSEGURIDAD

Objetivo



Implementación del Plan de Continuidad del Negocio (BCP)

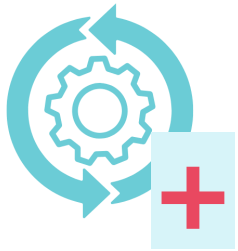
Plataforma: mercadopublico.cl

Versión 1.1 2024.08.09

Escenario: Durante una prueba de Recuperación ante Desastres (DRP) que involucra la migración de los componentes de mercadopublico.cl desde el proveedor 1 al proveedor 2, se produce un incidente que resulta en la indisponibilidad total del sitio web mercadopublico.cl en ambos proveedores. La solución de este incidente tiene tiempos inciertos declarados por la División de Tecnología.

TALLER DE CIBERSEGURIDAD

Objetivo



2. Alcance y objetivos

El BCP se aplica a los siguientes procesos de negocio críticos que apalanca la plataforma mercadopublico.cl:

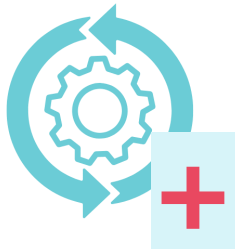
- Orden de Compra
- Licitaciones
- Convenio Marco
- Compra Ágil
- Trato Directo
- Compras por cotización
- Registro de proveedores

Los objetivos del BCP son:

- Mantener la operatividad de los procesos de negocio críticos.
- Comunicar de manera efectiva con todas las partes interesadas.

TALLER DE CIBERSEGURIDAD

Objetivo



3. Medidas inmediatas ante el escenario propuesto

a) Conformación del Comité técnico:

- Jefe de División de Tecnologías
- Jefe de Departamento de Operaciones
- Ingenieros DevOps que se requieran
- Jefe de Seguridad de la Información y Ciberseguridad
- Ingenieros de Ciberseguridad que se requieran
- Proveedores
- Otros profesionales de ChileCompra, proveedores u otros que se requieran

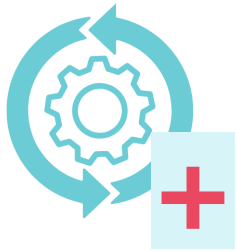
Encargado de convocar y conformar el comité: Jefe de Seguridad de la Información y Ciberseguridad

Listado de contactos proveedores

Lugar: Sala en Teams

TALLER DE CIBERSEGURIDAD

Objetivo



b) Conformación Centro de comando:

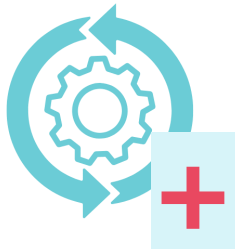
- Directora de ChileCompra
- Jefe de División de Tecnologías
- Jefa de División de Compras Públicas
- Jefe División de Gestión Usuaria
- Jefa Área de Estrategia y Gestión Institucional
- Fiscal
- Jefa de Departamento de Comunicaciones y Participación Ciudadana
- Jefe de Seguridad de la Información y Ciberseguridad
- Jefe de Estudios y Políticas de Compras
- Jefa Departamento Gestión y participación de proveedores
- Jefa Departamento Gestión y asesoría de compradores
- Jefe Departamento Mercado público

Encargado de convocar y conformar el comité: Jefe de Departamento de Seguridad de la Información y Ciberseguridad

En horario laboral: Salón azul / Fuera de horario laboral: Sala de Teams

TALLER DE CIBERSEGURIDAD

Objetivo



d) Activación de comunicados

A CSIRT: Se envía correo electrónico con el siguiente contenido:

Asunto: Notificación de indisponibilidad de la plataforma mercadopublico.cl por incidente técnico

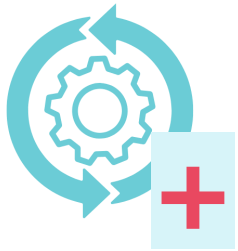
Mensaje:

Estimados,

Informamos que la plataforma mercadopublico.cl se encuentra actualmente indisponible

TALLER DE CIBERSEGURIDAD

Objetivo



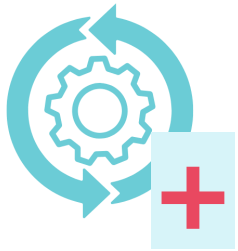
4. Activación del BCP

La activación del BCP será decidida por el Comité de decisiones a partir del diagnóstico del incidente y la solución de éste entregada por la División de Tecnologías.

Si la decisión es activar el BCP se continua con los siguientes pasos:

TALLER DE CIBERSEGURIDAD

Objetivo



5. Planes de Contingencia por Proceso de Negocio

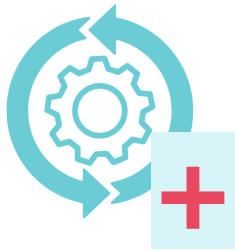
a) Proceso de negocio: Orden de Compra

Plan de Contingencia: Ante la necesidad de realizar una compra y que la plataforma www.mercadopublico.cl no se encuentre disponible, recomendamos lo siguiente:

Crear procesos de compra y recepción total o parcial de ofertas fuera del Sistema de Información en base a lo establecido en el Artículo 62 del Reglamento de la Ley de Compras Públicas 19.886 y sus procedimientos internos.

TALLER DE CIBERSEGURIDAD

Objetivo



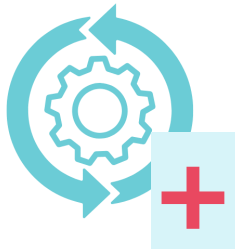
Plan de Comunicación: Chilecompra.cl, Centro de ayuda, Mesa de ayuda y Chat

Centro de Ayuda, el encargado o quien lo reemplace publica en el ayuda.mercadopublico.cl el mensaje validado por comunicaciones.

El Mensaje es propuesto por la Jefa de Atención de Usuarios y aprobado por la Jefa de Comunicaciones.

TALLER DE CIBERSEGURIDAD

Objetivo



6. Puntos de actualización de comunicaciones

- **Comunicación Interna:** Comunicación permanente a los colaboradores de la institución del estado de ejecución del plan de continuidad del negocio.
- **Comunicación Externa:** Comunicación permanente a los compradores y proveedores de Mercado Público del estado de las medidas de contingencia y eventual retorno a la normalidad de mercadopublico.cl.

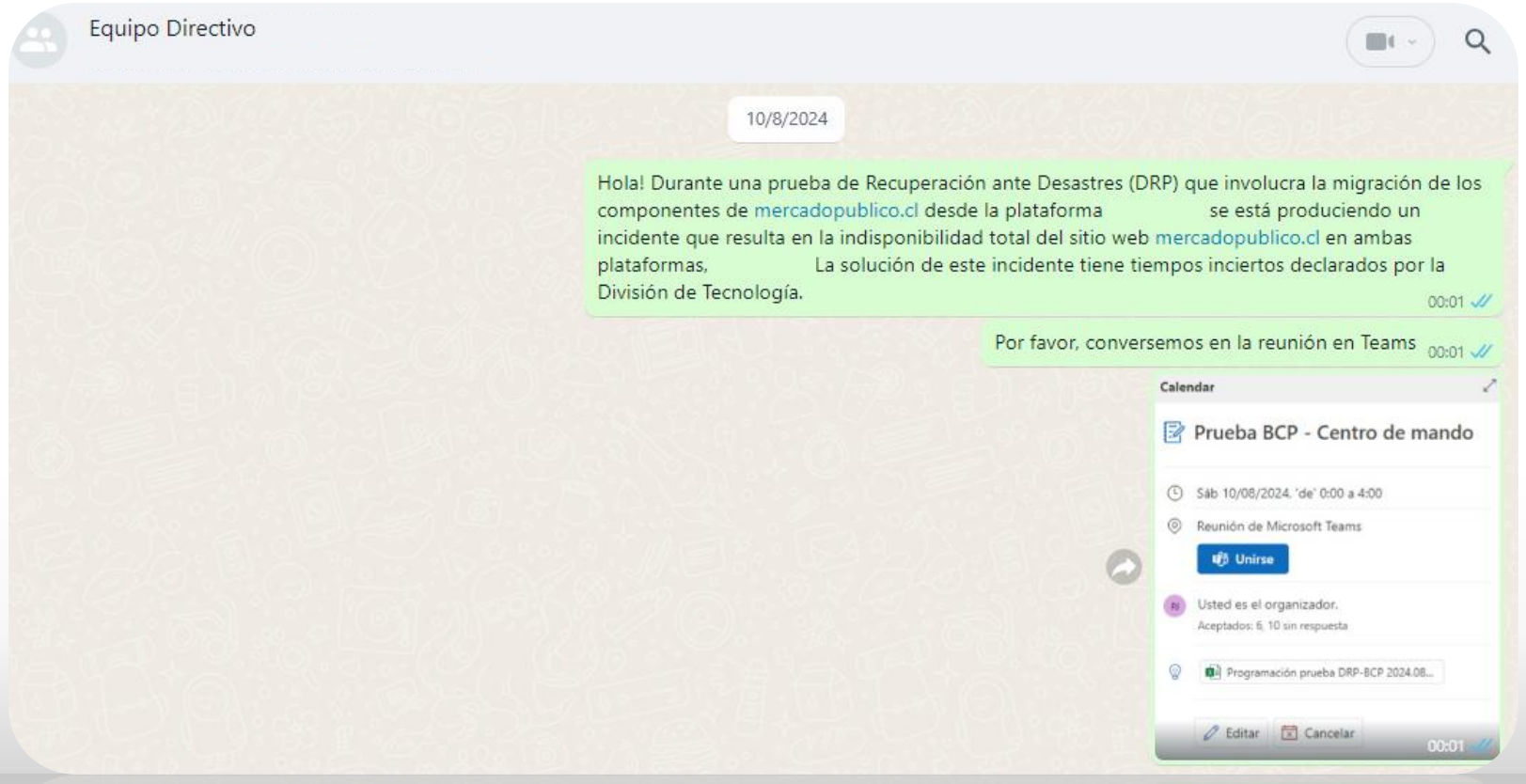
TALLER DE CIBERSEGURIDAD

Objetivo

Prueba general de BCP y DRP
Inicio 00:01 horas
Termino 11:00 horas

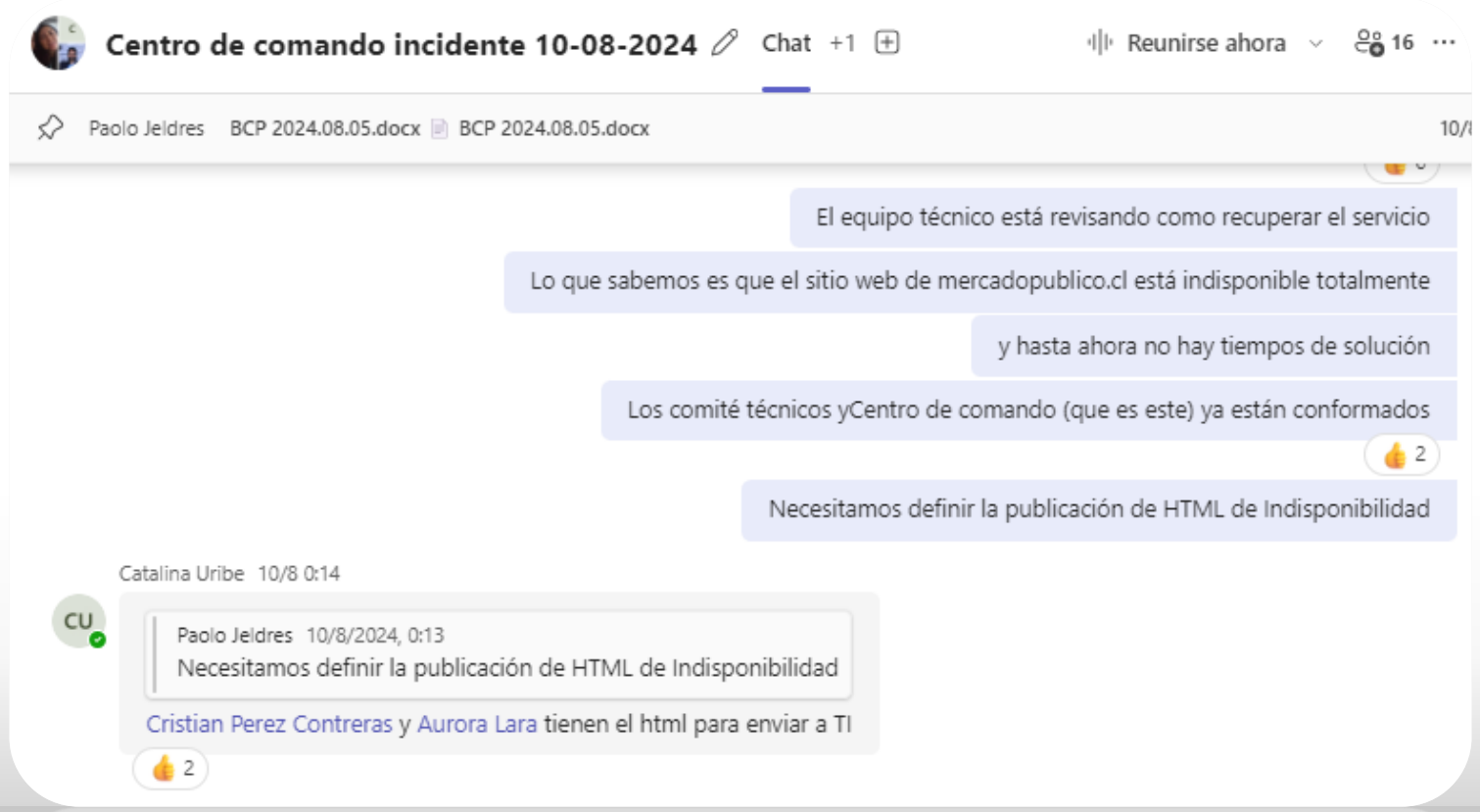
TALLER DE CIBERSEGURIDAD

Inicio de la prueba BCP



TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

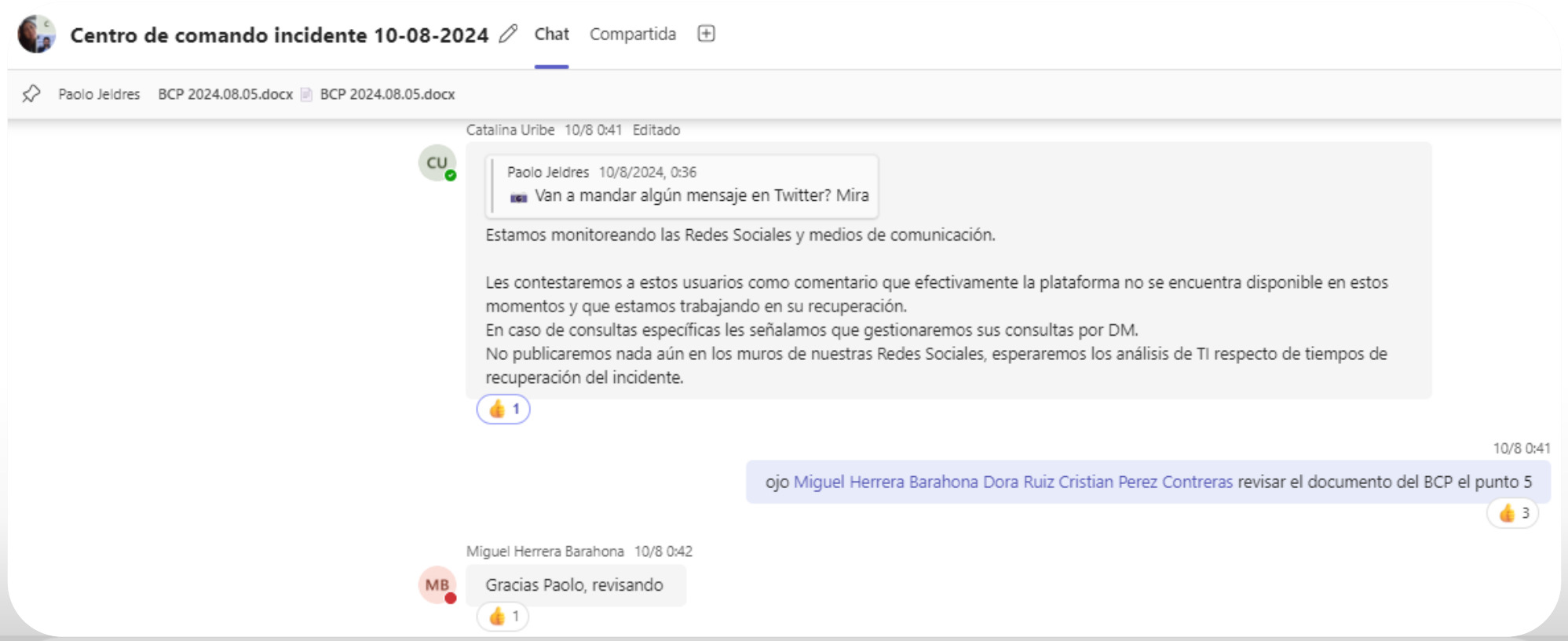


TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

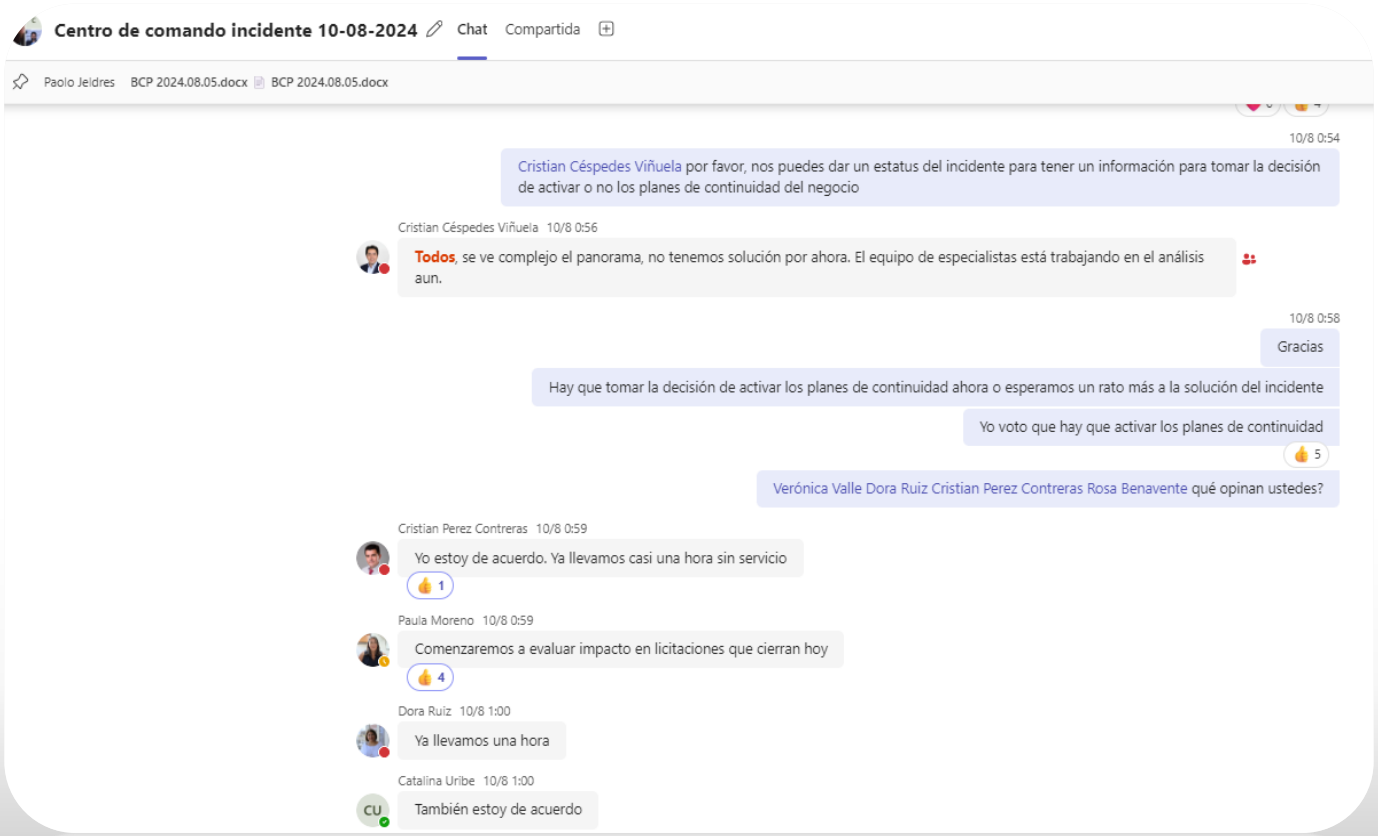
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



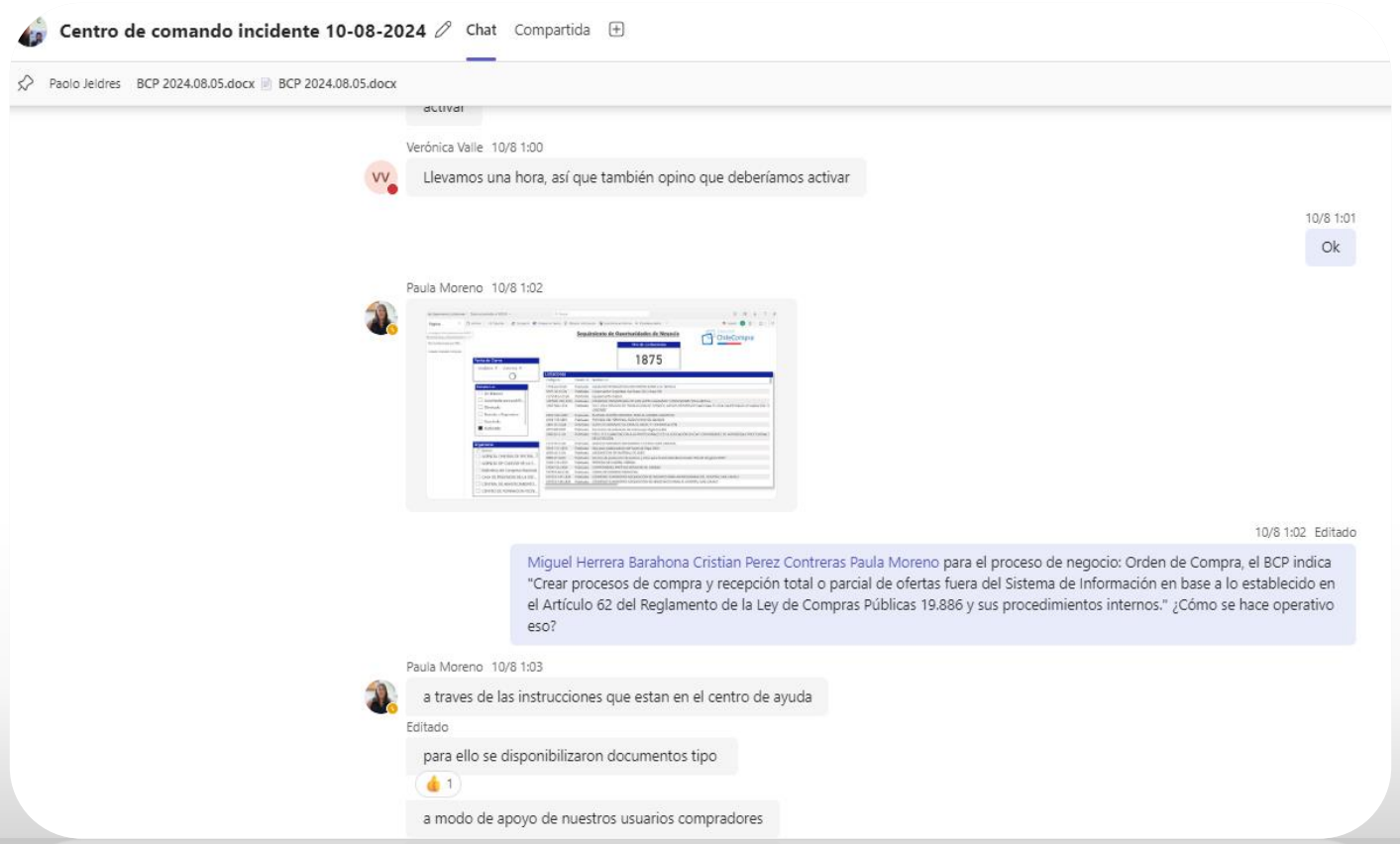
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



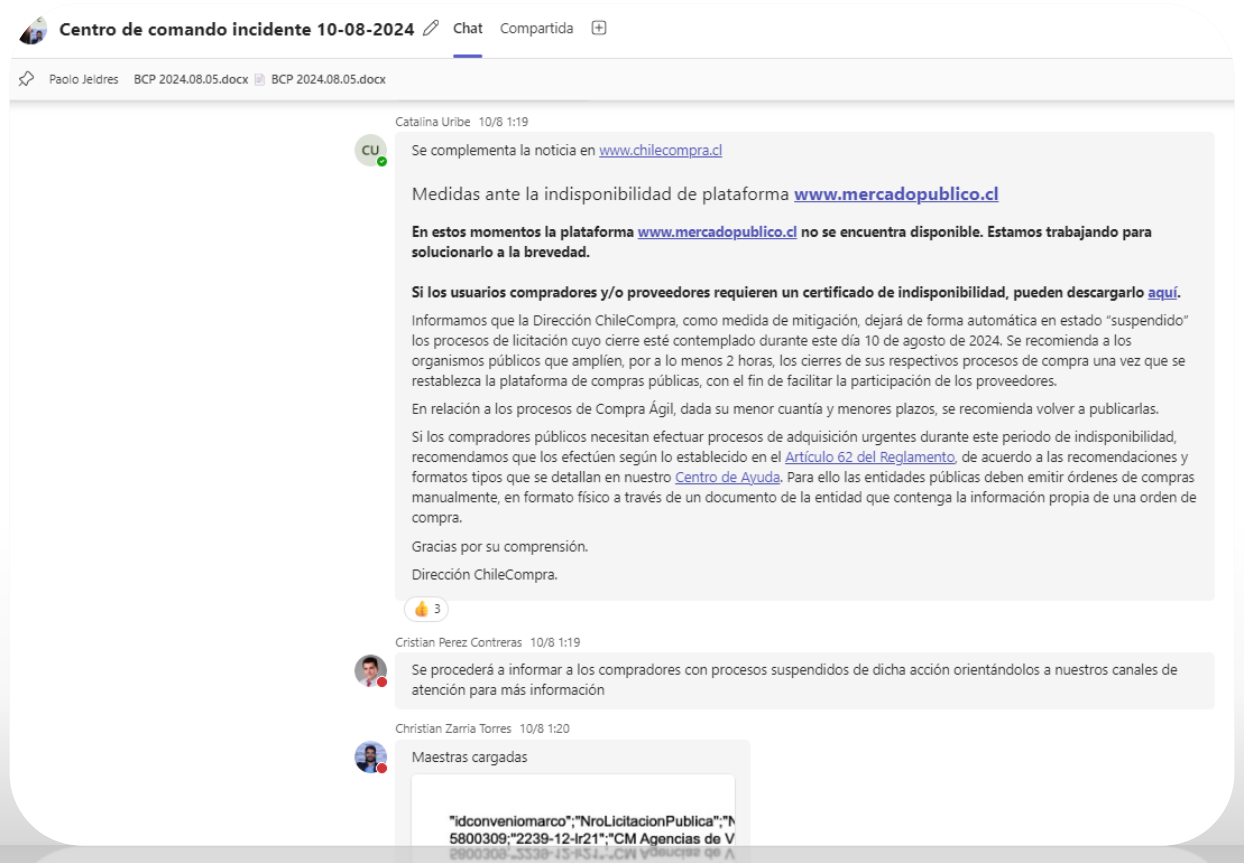
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



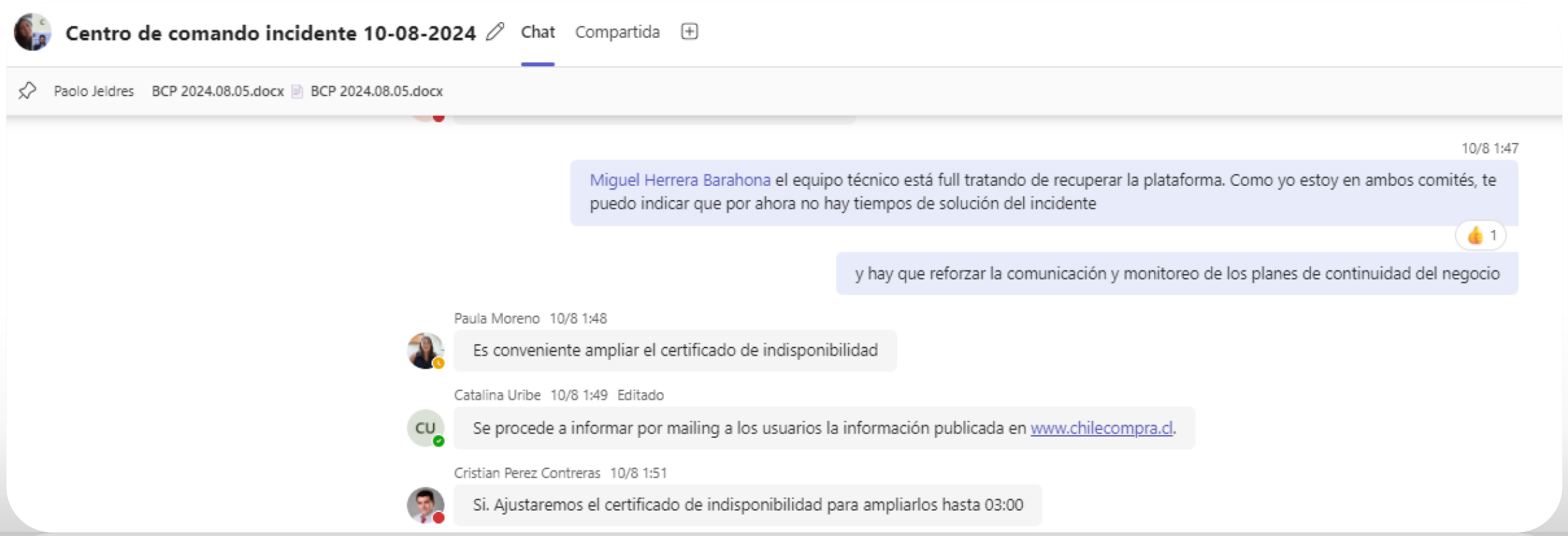
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



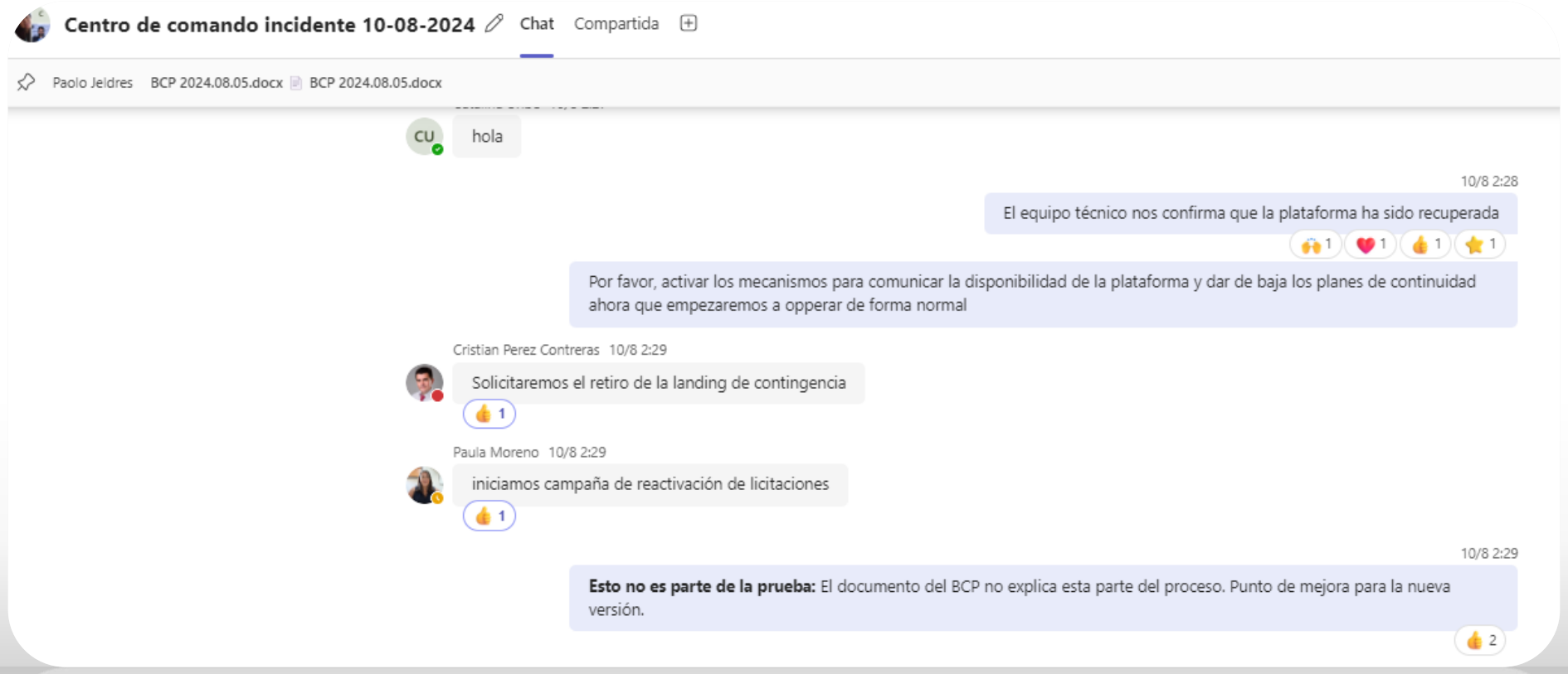
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



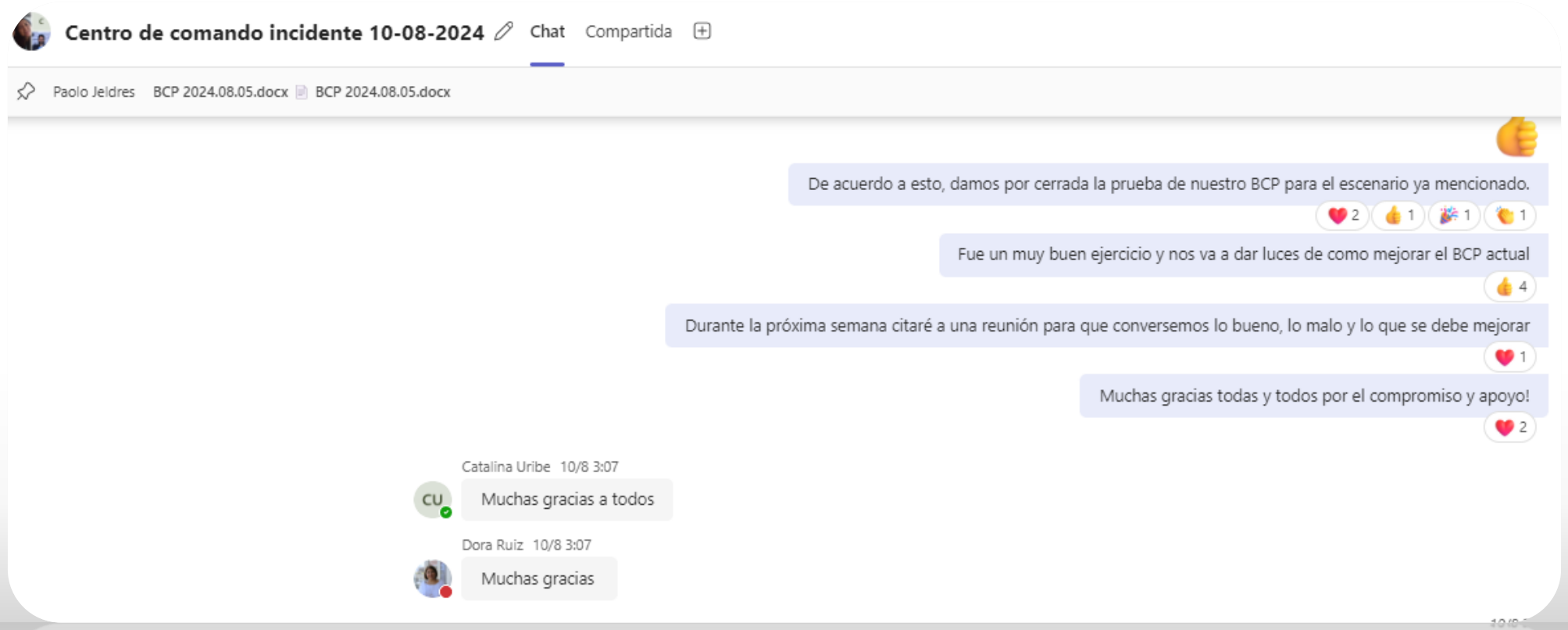
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba



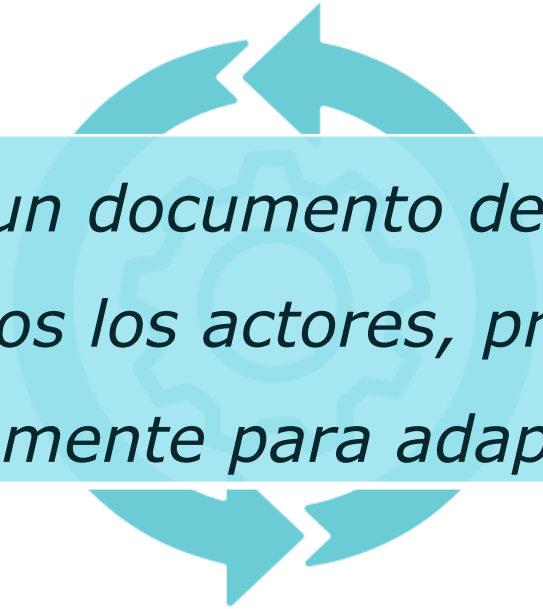
TALLER DE CIBERSEGURIDAD

Recomendaciones para construir una primera versión de un BCP

- Contar con el apoyo de la alta dirección de la institución.
- Establecer fechas límite cercanas.
- Mantener la simplicidad del documento.
- Involucrar a todas las áreas clave.
- Definir los procesos de negocio críticos.
- Documentar lecciones aprendidas y ajustes.

TALLER DE CIBERSEGURIDAD

¿Qué aprendimos en el ámbito de la continuidad de negocio post incidente de ciberseguridad?

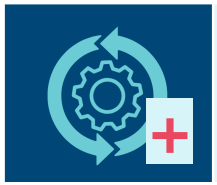


No basta con tener un documento de BCP, sino que es crucial concientizar a todos los actores, probarlo regularmente y perfeccionarlo continuamente para adaptarlo a diversos escenarios.

TALLER DE CIBERSEGURIDAD

¿Cómo seguimos?

Mejorar el BCP actual.



Generar nuevos BCPs de acuerdo a la criticidad de los procesos de cada unidad de negocio de ChileCompra.

Establecer un sistema de gestión de continuidad del negocio a partir de la Norma ISO 22301.