

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

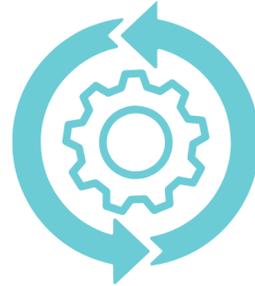
ChileCompra



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

¿Qué es un BCP?



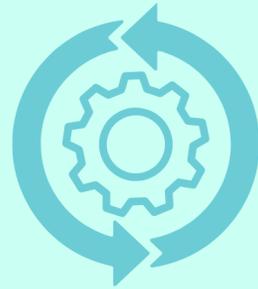
Es un **Plan de Continuidad de Negocio** que entrega a la organización la capacidad de continuar con su oferta de productos y servicios dentro de un período de tiempo aceptable a una capacidad predefinida durante una interrupción (por ejemplo, un incidente de ciberseguridad).

Fuente: Norma ISO 22301:2019

¿Qué es un BCP?

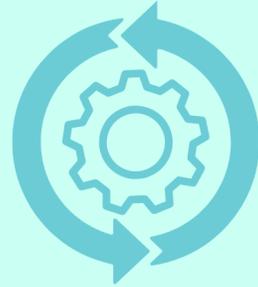


¿Qué es un BCP?



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

¿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?



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:...

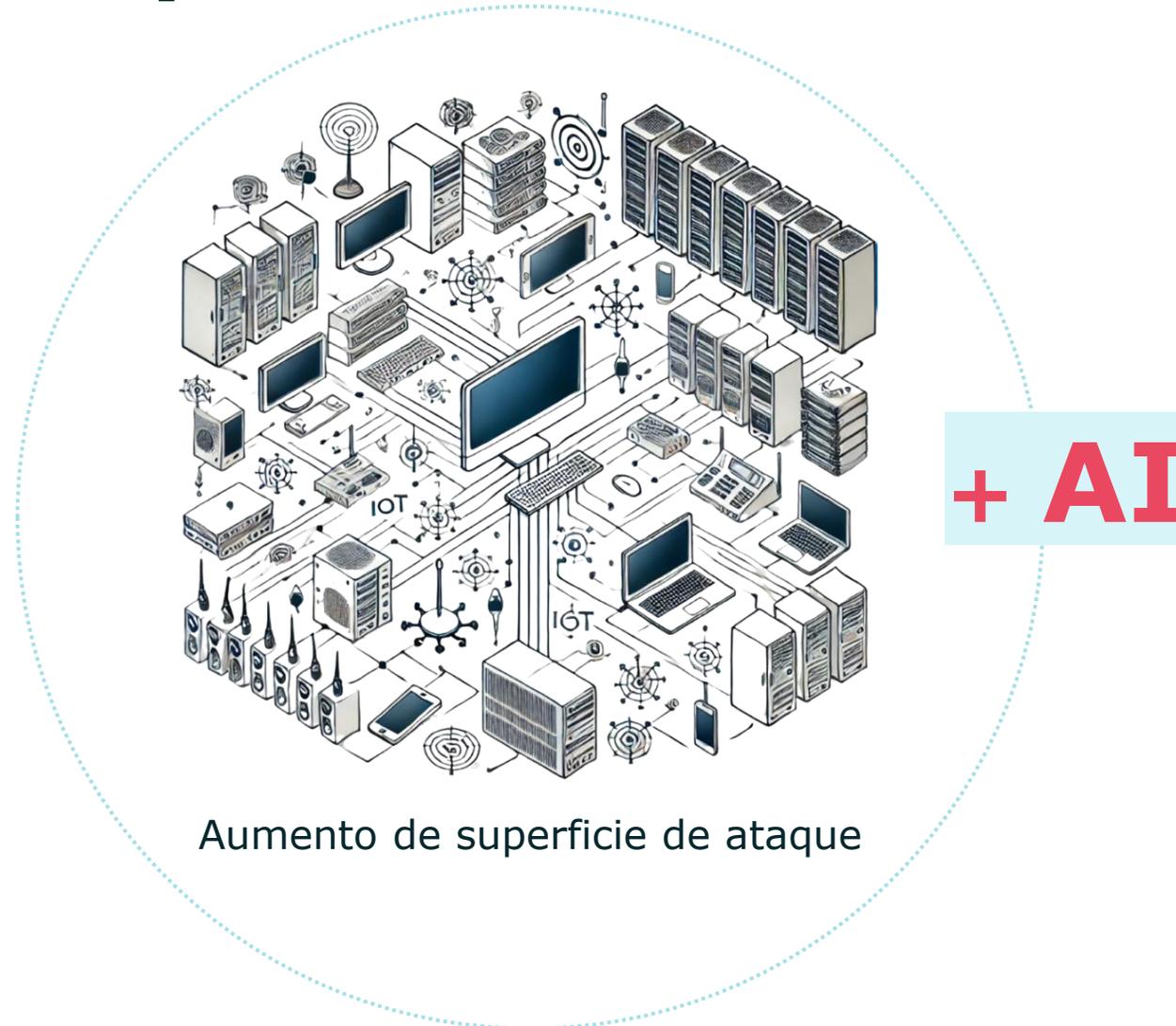
4 jul 2024

Más y más dispositivos conectados a la red



Aumento de superficie de ataque

Más y más dispositivos conectados a la red



Aumento de superficie de ataque

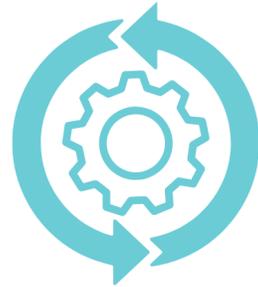
+ AI

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"

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



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

El documento del BCP NO funcionó; las personas SI

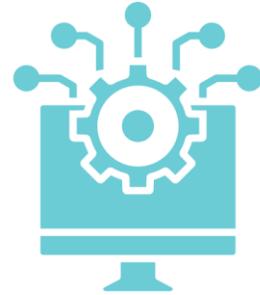


¿Qué hicimos posterior al incidente?



Mirada externa

Diagnóstico



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

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

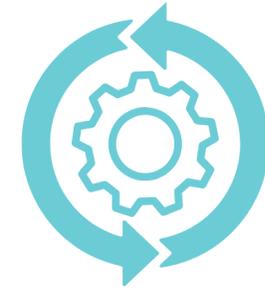
Plan de seguridad institucional



Controles de seguridad



Concientización



Plan de continuidad del negocio

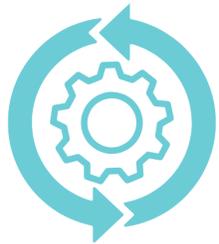
TALLER DE CIBERSEGURIDAD

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

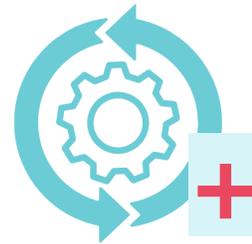
Mes/Año	Hito
Septiembre 2023	Incidente / Recuperación
Octubre 2023	Verificación recuperación
Noviembre – Diciembre 2023	Análisis de oportunidades de mejoras
Enero 2024	Inicio consultorías externas
Febrero – abril 2024	Diagnóstico
Mayo 2024	Presentación resultados diagnóstico y elección proyectos a ejecutar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

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



A

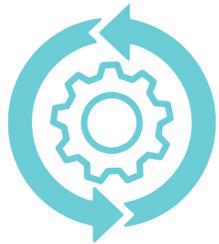
Planificar un sistema de gestión de continuidad del negocio a partir de la Norma ISO 22301



B

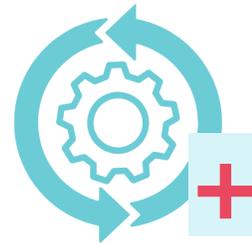
Generar un producto mínimo viable de la alternativa a)

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



A

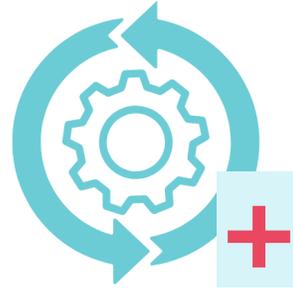
Planificar un sistema de gestión de continuidad del negocio a partir de la Norma ISO 22301.



B

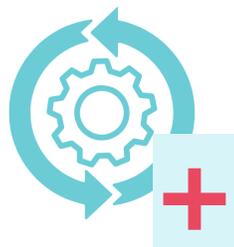
Generar un producto mínimo viable de la alternativa a)

Objetivo



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

Objetivo



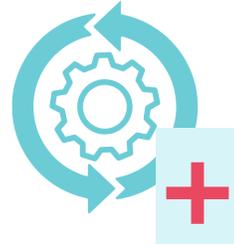
Implementación del Plan de Continuidad del Negocio (BCP)

Plataforma: [mercadopublico.cl](https://www.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](https://www.mercadopublico.cl) desde el proveedor 1 al proveedor 2, se produce un incidente que resulta en la indisponibilidad total del sitio web [mercadopublico.cl](https://www.mercadopublico.cl) en ambos proveedores. La solución de este incidente tiene tiempos inciertos declarados por la División de Tecnología.

Objetivo



2. Alcance y objetivos

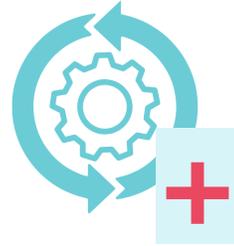
El BCP se aplica a los siguientes procesos de negocio críticos que apalanca la plataforma mercadopublico.cl:

- 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.

Objetivo



3. Medidas inmediatas ante el escenario propuesto

a) Conformación del Comité técnico:

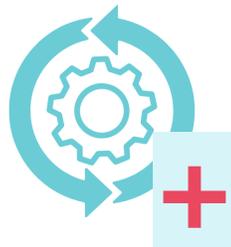
- Jefe de División de Tecnologías
- Jefe de Departamento de Operaciones
- Ingenieros DevOps que se requieran
- Jefe de Seguridad de la Información y Ciberseguridad
- Ingenieros de Ciberseguridad que se requieran
- Proveedores
- Otros profesionales de ChileCompra, proveedores u otros que se requieran

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

[Listado de contactos proveedores](#)

Lugar: Sala en Teams

Objetivo



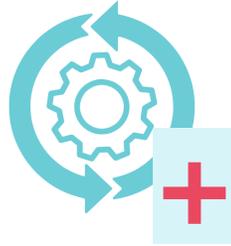
b) Conformación Centro de comando:

- 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

Objetivo



d) Activación de comunicados

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

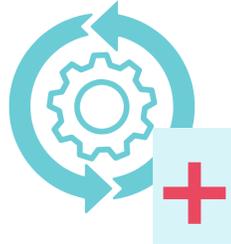
Asunto: Notificación de indisponibilidad de la plataforma mercadopublico.cl por incidente técnico

Mensaje:

Estimados,

Informamos que la plataforma mercadopublico.cl se encuentra actualmente indisponible

Objetivo

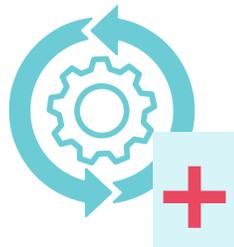


4. Activación del BCP

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:

Objetivo



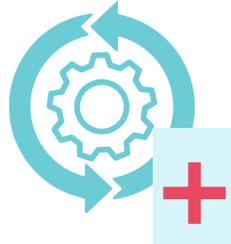
5. Planes de Contingencia por Proceso de Negocio

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.

Objetivo

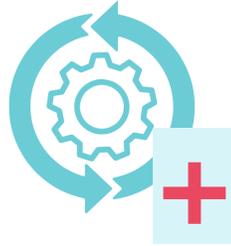


Plan de Comunicación: Chilecompra.cl, Centro de ayuda, Mesa de ayuda y Chat

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.

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

AGOSTO							
SM	LU	MA	MI	JU	VI	SA	DO
31				1	2	3	4
32	5	6	7	8	9	10	11
33	12	13	14	15	16	17	18
34	19	20	21	22	23	24	25
35	26	27	28	29	30	31	

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

Inicio de la prueba BCP

Equipo Directivo

10/8/2024

Hola! Durante una prueba de Recuperación ante Desastres (DRP) que involucra la migración de los componentes de [mercadopublico.cl](#) desde la plataforma se está produciendo un incidente que resulta en la indisponibilidad total del sitio web [mercadopublico.cl](#) en ambas plataformas. La solución de este incidente tiene tiempos inciertos declarados por la División de Tecnología. 00:01 ✓

Por favor, conversemos en la reunión en Teams 00:01 ✓

Calendar

Prueba BCP - Centro de mando

Sáb 10/08/2024, 'de' 0:00 a 4:00

Reunión de Microsoft Teams

Unirse

Usted es el organizador.
Aceptados: 6, 10 sin respuesta

Programación prueba DRP-BCP 2024.08...

Editar Cancelar 00:01 ✓

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

Centro de comando incidente 10-08-2024 Chat +1 + Reunirse ahora 16

Paolo Jeldres BCP 2024.08.05.docx BCP 2024.08.05.docx 10/1

El equipo técnico está revisando como recuperar el servicio

Lo que sabemos es que el sitio web de mercadopublico.cl está indisponible totalmente

y hasta ahora no hay tiempos de solución

Los comité técnicos y Centro de comando (que es este) ya están conformados

2

Necesitamos definir la publicación de HTML de Indisponibilidad

Catalina Uribe 10/8 0:14

CU

Paolo Jeldres 10/8/2024, 0:13

Necesitamos definir la publicación de HTML de Indisponibilidad

Cristian Perez Contreras y Aurora Lara tienen el html para enviar a TI

2

5

Cristian Perez Contreras y Aurora Lara tienen el html para enviar a TI

Necesitamos definir la publicación de HTML de indisponibilidad

Paolo Jeldres 10/8/2024, 0:13

CU

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

 **Centro de comando incidente 10-08-2024**  Chat  Compartida 

 Paolo Jeldres  BCP 2024.08.05.docx  BCP 2024.08.05.docx

Catalina Uribe 10/8 0:26 Editado

 **Paolo Jeldres** de acuerdo a los análisis que hagan desde TI respecto de los tiempos de solución del incidente iremos complementando los mensajes, con respecto al uso del artículo 62. 

 1

Marcelo Espejo 10/8 0:26

 Paolo Jeldres 10/8/2024, 0:19
Marcelo Espejo por favor, enviar mensaje al CSIRT del incidente que tenemos

Esto se envió al CSIRT.

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

Estimados,

Informamos que la plataforma mercadopublico.cl se encuentra actualmente indisponible debido a un incidente técnico que se presentó el 10-08-2024 a las 00:01am. Nuestro equipo de tecnología ya está trabajando para identificar y resolver la causa de este incidente con la mayor prontitud posible.

Mantendremos a su equipo informado sobre los avances en la resolución del incidente y proporcionaremos una actualización tan pronto como la plataforma esté nuevamente operativa.

 1



tan pronto como la plataforma esté nuevamente operativa.

Informamos que la plataforma mercadopublico.cl se encuentra actualmente indisponible debido a un incidente técnico que se presentó el 10-08-2024 a las 00:01am. Nuestro equipo de tecnología ya está trabajando para identificar y resolver la causa de este incidente con la mayor prontitud posible.

Mantendremos a su equipo informado sobre los avances en la resolución del incidente y proporcionaremos una actualización tan pronto como la plataforma esté nuevamente operativa.

Informamos que la plataforma mercadopublico.cl se encuentra actualmente indisponible debido a un incidente técnico que se presentó el 10-08-2024 a las 00:01am. Nuestro equipo de tecnología ya está trabajando para identificar y resolver la causa de este incidente con la mayor prontitud posible.

Mantendremos a su equipo informado sobre los avances en la resolución del incidente y proporcionaremos una actualización tan pronto como la plataforma esté nuevamente operativa.

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

Centro de comando incidente 10-08-2024 Chat Compartida

Paolo Jeldres BCP 2024.08.05.docx BCP 2024.08.05.docx

Catalina Uribe 10/8 0:41 Editado

CU

Paolo Jeldres 10/8/2024, 0:36

Van a mandar algún mensaje en Twitter? Mira

Estamos monitoreando las Redes Sociales y medios de comunicación.

Les contestaremos a estos usuarios como comentario que efectivamente la plataforma no se encuentra disponible en estos momentos y que estamos trabajando en su recuperación.

En caso de consultas específicas les señalamos que gestionaremos sus consultas por DM.

No publicaremos nada aún en los muros de nuestras Redes Sociales, esperaremos los análisis de TI respecto de tiempos de recuperación del incidente.

👍 1

10/8 0:41

ojo Miguel Herrera Barahona Dora Ruiz Cristian Perez Contreras revisar el documento del BCP el punto 5

👍 3

Miguel Herrera Barahona 10/8 0:42

MB

Gracias Paolo, revisando

👍 1

MB

Gracias Paolo, revisando

👍 1

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

Centro de comando incidente 10-08-2024 Chat Compartida

Paolo Jeldres BCP 2024.08.05.docx BCP 2024.08.05.docx

10/8 0:54

Cristian Céspedes Viñuela por favor, nos puedes dar un estatus del incidente para tener un información para tomar la decisión de activar o no los planes de continuidad del negocio

Cristian Céspedes Viñuela 10/8 0:56

Todos, se ve complejo el panorama, no tenemos solución por ahora. El equipo de especialistas está trabajando en el análisis aun.

10/8 0:58

Gracias

Hay que tomar la decisión de activar los planes de continuidad ahora o esperamos un rato más a la solución del incidente

Yo voto que hay que activar los planes de continuidad

5

Verónica Valle Dora Ruiz Cristian Perez Contreras Rosa Benavente qué opinan ustedes?

Cristian Perez Contreras 10/8 0:59

Yo estoy de acuerdo. Ya llevamos casi una hora sin servicio

1

Paula Moreno 10/8 0:59

Comenzaremos a evaluar impacto en licitaciones que cierran hoy

4

Dora Ruiz 10/8 1:00

Ya llevamos una hora

Catalina Uribe 10/8 1:00

También estoy de acuerdo

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

Centro de comando incidente 10-08-2024 Chat Compartida

Paolo Jeldres BCP 2024.08.05.docx BCP 2024.08.05.docx

Verónica Valle 10/8 1:00

Llevamos una hora, así que también opino que deberíamos activar

10/8 1:01
Ok

Paula Moreno 10/8 1:02



10/8 1:02 Editado

Miguel Herrera Barahona Cristian Perez Contreras Paula Moreno para el proceso de negocio: Orden de Compra, el BCP indica "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." ¿Cómo se hace operativo eso?

Paula Moreno 10/8 1:03

a través de las instrucciones que estan en el centro de ayuda

Editado

para ello se disponibilizaron documentos tipo

👍 1

a modo de apoyo de nuestros usuarios compradores

a modo de apoyo de nuestros usuarios compradores

👍 1

para ello se disponibilizaron documentos tipo

Editado

a través de las instrucciones que estan en el centro de ayuda

Paula Moreno 10/8 1:03

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

Centro de comando incidente 10-08-2024 Chat Compartida

Paolo Jeldres BCP 2024.08.05.docx BCP 2024.08.05.docx

Catalina Uribe 10/8 1:19

CU Se complementa la noticia en www.chilecompra.cl

Medidas ante la indisponibilidad de plataforma www.mercadopublico.cl

En estos momentos la plataforma www.mercadopublico.cl no se encuentra disponible. Estamos trabajando para solucionarlo a la brevedad.

Si los usuarios compradores y/o proveedores requieren un certificado de indisponibilidad, pueden descargarlo [aquí](#).

Informamos que la Dirección ChileCompra, como medida de mitigación, dejará de forma automática en estado "suspendido" los procesos de licitación cuyo cierre esté contemplado durante este día 10 de agosto de 2024. Se recomienda a los organismos públicos que amplíen, por a lo menos 2 horas, los cierres de sus respectivos procesos de compra una vez que se restablezca la plataforma de compras públicas, con el fin de facilitar la participación de los proveedores.

En relación a los procesos de Compra Ágil, dada su menor cuantía y menores plazos, se recomienda volver a publicarlas.

Si los compradores públicos necesitan efectuar procesos de adquisición urgentes durante este periodo de indisponibilidad, recomendamos que los efectúen según lo establecido en el [Artículo 62 del Reglamento](#), de acuerdo a las recomendaciones y formatos tipos que se detallan en nuestro [Centro de Ayuda](#). Para ello las entidades públicas deben emitir órdenes de compras manualmente, en formato físico a través de un documento de la entidad que contenga la información propia de una orden de compra.

Gracias por su comprensión.

Dirección ChileCompra.

3

Cristian Perez Contreras 10/8 1:19

Se procederá a informar a los compradores con procesos suspendidos de dicha acción orientándolos a nuestros canales de atención para más información

Christian Zarría Torres 10/8 1:20

Maestras cargadas

"idconveniomarco";"NroLicitacionPublica";"N
5800309";"2239-12-Ir21";"CM Agencias de V

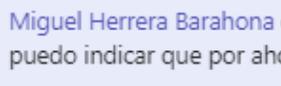
TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

 **Centro de comando incidente 10-08-2024**  Chat  Compartida 

 Paolo Jeldres  BCP 2024.08.05.docx  BCP 2024.08.05.docx

10/8 1:47

 Miguel Herrera Barahona el equipo técnico está full tratando de recuperar la plataforma. Como yo estoy en ambos comités, te puedo indicar que por ahora no hay tiempos de solución del incidente  1

y hay que reforzar la comunicación y monitoreo de los planes de continuidad del negocio

Paula Moreno 10/8 1:48

 Es conveniente ampliar el certificado de indisponibilidad

Catalina Uribe 10/8 1:49 Editado

 CU Se procede a informar por mailing a los usuarios la información publicada en www.chilecompra.cl.

Cristian Perez Contreras 10/8 1:51

 Si. Ajustaremos el certificado de indisponibilidad para ampliarlos hasta 03:00

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

The screenshot shows a chat window titled "Centro de comando incidente 10-08-2024". The chat history includes:

- A message from "CU" saying "hola".
- A system message at 10/8 2:28: "El equipo técnico nos confirma que la plataforma ha sido recuperada", which has received 1 thumbs up, 1 heart, 1 thumbs down, and 1 star.
- A system message: "Por favor, activar los mecanismos para comunicar la disponibilidad de la plataforma y dar de baja los planes de continuidad ahora que empezaremos a operar de forma normal".
- A message from Cristian Perez Contreras at 10/8 2:29: "Solicitaremos el retiro de la landing de contingencia", with 1 thumbs up.
- A message from Paula Moreno at 10/8 2:29: "iniciamos campaña de reactivación de licitaciones", with 1 thumbs up.
- A system message at 10/8 2:29: "Esto no es parte de la prueba: El documento del BCP no explica esta parte del proceso. Punto de mejora para la nueva versión.", with 2 thumbs up.

The interface also shows a header with "Paolo Jeldres" and two document attachments: "BCP 2024.08.05.docx".

TALLER DE CIBERSEGURIDAD

Desarrollo de la prueba

 **Centro de comando incidente 10-08-2024**  Chat  Compartida 

 Paolo Jeldres  BCP 2024.08.05.docx  BCP 2024.08.05.docx



De acuerdo a esto, damos por cerrada la prueba de nuestro BCP para el escenario ya mencionado.

 2  1  1  1

Fue un muy buen ejercicio y nos va a dar luces de como mejorar el BCP actual

 4

Durante la próxima semana citaré a una reunión para que conversemos lo bueno, lo malo y lo que se debe mejorar

 1

Muchas gracias todas y todos por el compromiso y apoyo!

 2

Catalina Uribe 10/8 3:07

 CU  Muchas gracias a todos

Dora Ruiz 10/8 3:07

 Muchas gracias

10/8

 Muchas gracias

10/8 3:07

 CU  Muchas gracias a todos

10/8 3:07

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.

¿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.

¿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.