Manual de DR/BCP de TLD-OPS

Versión 1.0.2

3 de diciembre de 2019

Índice

Contenidos

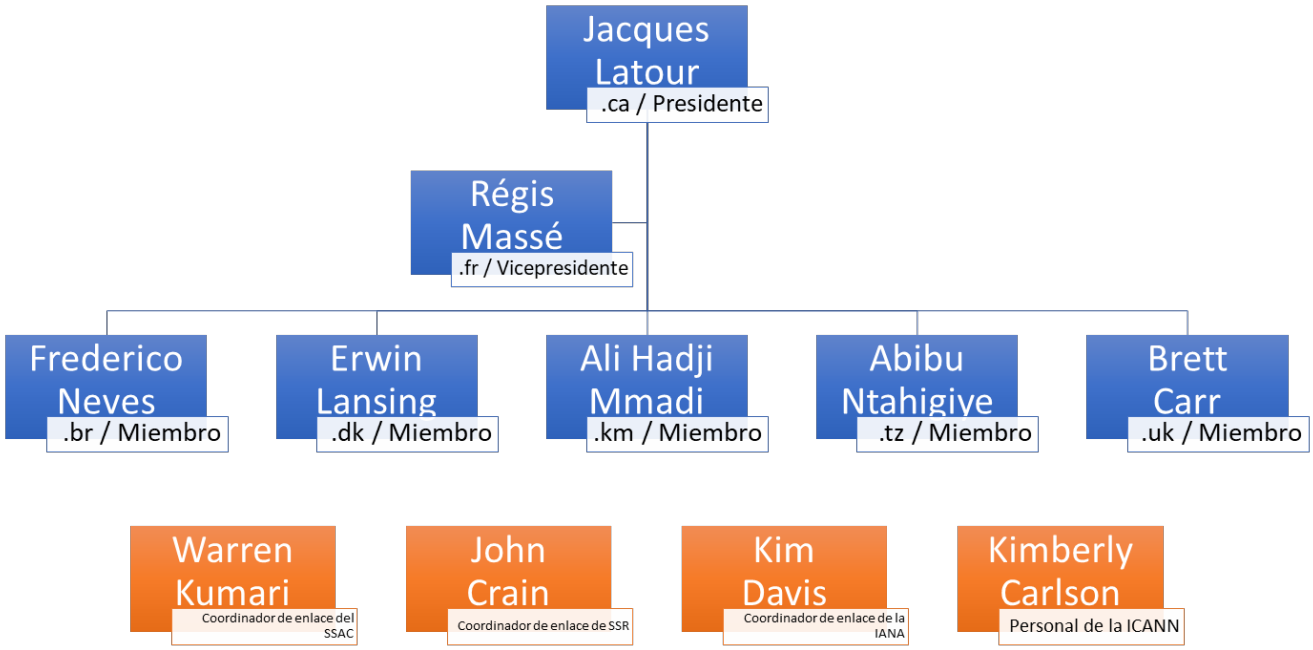
Introducción

Acerca de TLD-OPS: seguridad y estabilidad de ccTLD juntas

TLD-OPS es la comunidad de respuesta ante incidentes por y para los ccTLD y reúne a personas que son responsables de la seguridad y estabilidad operativas de su ccTLD. El objetivo de la comunidad de TLD-OPS es permitir que los operadores de ccTLD de todo el mundo detecten y mitiguen incidentes que puedan afectar la estabilidad y seguridad operativas de los servicios de ccTLD, tales como ataques de DDOS, infecciones de malware y ataques de phishing. La meta de TLD-OPS es continuar extendiendo las estructuras, los procesos y las herramientas de respuesta ante incidentes existentes y no reemplazarlos. La comunidad de TLD-OPS está abierta a todos los ccTLD, independientemente de su afiliación en la ccNSO (Organización de Apoyo para Nombres de Dominio con Código de País).

Acerca de: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

Un agradecimiento especial a Dirk Jumpertz, Gerente de Seguridad de EURid por su sobresaliente contribución a este documento y proyecto.



Comité Permanente de TLD-OPS

Cómo utilizar este documento

Este manual tiene el objetivo de ofrecer pautas prácticas para quien quiera implementar una estrategia de continuidad de operaciones dentro de un operador de registro más pequeño. Su público objetivo está orientado hacia la gerencia superior o media. Supone que el operador de registro tiene el compromiso, patrocinio y misión de su organismo supervisor (ya sea una Junta, representación gubernamental u otro) para desarrollar flexibilidad contra eventos disruptivos en la forma de un plan de continuidad de operaciones.

Dado que este documento intenta ser lo más práctico posible, contiene varias tablas de ejemplos prácticos que pueden copiarse y emplearse en las diversas etapas del desarrollo y de la implementación.

Asimismo, contiene algunos ejemplos que podrían usarse como plantillas o como inspiración para desarrollar planes de continuidad de operaciones/recuperación de desastres.

Por último, el lector encontrará “cuadros de acción” ocasionales en el documento que contienen sugerencias prácticas: una breve descripción de una actividad y quién debería realizarla.

¿Qué es la continuidad de operaciones?

La continuidad de operaciones es la capacidad de una organización de continuar con la entrega de productos o servicios que son importantes para el negocio del operador de registro de ccTLD y de las partes interesadas a niveles predefinidos y aceptables después de un incidente disruptivo.

Tenga en cuenta que la continuidad de operaciones no se centra necesariamente solo en incidentes disruptivos técnicos. Cualquier incidente disruptivo que afecte la preparación operativa de una organización puede impulsar los Planes de Continuidad de Operaciones. Por ende, es importante que una organización comprenda qué impide la preparación operativa.

Continuidad de operaciones vs. recuperación de desastres

Loa planes de continuidad de operaciones (BCP) y los planes de recuperación de desastres (DRP) están relacionados pero no son intercambiables aunque se encontrarán similitudes al buscar plantillas en Google, por ejemplo. El primero consiste en un plan de acción que se centra en entregar operaciones normales durante una crisis; el segundo es un subconjunto y contiene procedimientos para restaurar los sistemas vitales en el plazo más breve posible que el negocio requiera.

Dicho de otro modo, un Plan de Continuidad de Operaciones contendrá referencias a diversos Planes de Recuperación de Desastres. A los efectos de este documento, elaboraremos Planes de Continuidad de Operaciones que contengan un plan de acción para un escenario específico.

¿Cómo lograr este objetivo?

Mediante el uso de algunas pautas de la norma ISO 22301 sobre Continuidad de Operaciones, se puede crear un marco global que ayude a crear, administrar y mejorar los Planes de Continuidad de Operaciones.

Como la misión de los administradores de dominio es prácticamente idéntica dentro del mundo de los ccTLD, se puede usar un enfoque común y simplificado que se centre en la practicidad en vez de técnicas complejas, prolongadas y a veces abstractas para desarrollar los planes de continuidad de operaciones correctos.

Relación con la norma ISO/IEC 27001:2013

La norma ISO 27001 se centra en la seguridad de la información que se limita a desarrollar, implementar, supervisar y mejorar los controles para mantener niveles de confidencialidad, integridad y disponibilidad (abreviados como CIA - *Confidentiality, Integrity and Availability*). Para una empresa de servicios de TI, esto se superpone un poco con la continuidad de operaciones.

Sin embargo, hay una diferencia: mientras la ISO/IEC 27001 se centra en lograr los niveles C, I y A requeridos durante operaciones normales y prevé mitigación necesaria mediante tecnología y procedimientos; la ISO 22301 se centra en incidentes disruptivos que incapacitan a la organización y prevé planes para actuar en función de los incidentes.

Para comprender la diferencia entre el ISMS (Sistema de Gestión de Seguridad de la Información) y el BCMS (Sistema de Gestión de Continuidad de Operaciones), algunos ejemplos para ilustrar podrían ser de gran utilidad:

- *El almacenamiento redundante con protección y duplicación de RAID es generalmente empleado para aumentar la integridad y disponibilidad (ISO/IEC 27001).*
- *Se organizan ejercicios de simulacro de incendio a fin de asegurarse de que las casualidades sean mínimas en caso de que se produzca un incendio real (ISO 22301).*
- *Se implementa protección de punto extremo antivirus para proteger equipos portátiles, equipos de escritorio y dispositivos móviles de ataques cibernéticos (ISO/IEC 27001).*
- *Por otro lado, procedimientos simulados en caso de un ataque de ransomware exitoso forman parte de los Planes de Continuidad de Operaciones (ISO 22301).*

Alcance (de este documento)

Este documento sirve como guía en la implementación de la base de continuidad de operaciones y recuperación de desastres dentro de un operador de registro pequeño.

Debería ser de ayuda responder las siguientes preguntas:

- ¿Cómo determinar el alcance de la continuidad de operaciones?
- ¿Cómo determinar los riesgos?
- ¿Cómo incluir la continuidad de operaciones en el ADNDNA de la compañía?
- ¿Qué se necesita para una estrategia de continuidad de operaciones eficaz?
- ¿Cuáles son los materiales vitales?
- ¿Cómo elaborar un plan de continuidad de operaciones o plan de recuperación de desastres?
- ¿Cómo hacer ejercicios de continuidad de operaciones?
- ¿Cómo realizar mejoras?

Referencias normativas

Este documento se basa en las siguientes normas:

- ISO 22301:2012 – Seguridad societaria – Sistemas de gestión de continuidad de operaciones – Requisitos.
- ISO 31000:2009 – Gestión de riesgos – Principios y pautas.
- ISO/IEC 27001:2013 - Tecnología de la Información -- Técnicas de seguridad -- Sistemas de gestión de seguridad de la información -- Requisitos

Términos y definiciones

Véase la norma ISO 22301:2012 para conocer los términos y definiciones usados en este documento.

Véase el documento RFC2119 para comprender los niveles de requisitos.

Contexto de la organización

Aunque la mayoría de los ccTLD tienen una cartera de servicios y una misión muy similares, siempre hay una diferencia sustancial que se orientará a la Estrategia de Continuidad de

Operaciones. En general, uno podría decir, sin embargo, que la misión operativa de la mayoría de los ccTLD es:

- gestionar la infraestructura de servidores de nombres para su TLD.
- gestionar los servicios públicos, esenciales para un ccTLD. De manera más específica, esto sería un sitio web corporativo y un servicio de búsqueda administrativo como WHOIS o RDAP.
- gestionar algún tipo de servicios de registración que permita la registración directa o indirecta de nombres de dominio. Esto puede ser una interfaz humana como un sitio web o una interfaz de máquina a máquina dedicada como EPP.
- y por último, pero no menos importante, el registro administrará varios sistemas de apoyo de operaciones corporativos que puedan no tener demasiada visibilidad externa, pero que sean esenciales para que la organización funcione (por ejemplo, correo electrónico, intranet, servidor de archivos, etc.)

El fin de este primer paso es comprender quién depende de la organización y, por lo tanto, tiene ciertas expectativas que deben cumplirse durante un incidente disruptivo y a quién necesita la organización para cumplir con su misión.

Comprensión de la organización y su contexto

Un primer paso general para crear una estrategia de continuidad de operaciones eficaz es comprender exhaustivamente el negocio y sus partes interesadas. Las partes interesadas tendrán expectativas y requisitos específicos, y formularán obligaciones que deberán tenerse en cuenta dentro del alcance. Por lo tanto, siempre resulta ser una buena práctica enumerar las partes interesadas, describir quiénes o qué son y, por último, analizar sus expectativas con respecto a la flexibilidad operativa y la continuidad de operaciones. Esta actividad debería ser realizada preferentemente por la gerencia para capturar los aportes correctos. La columna “relevancia para BC” captura la relación de la expectativa con la Continuidad de Operaciones (BC). Algunas expectativas pueden no estar relacionadas; mientras que otras podrían ser consideradas muy importantes. A tal efecto, se podría usar ALTA, MEDIA, BAJA Y N/A para indicar la relevancia. Ejemplo: si una expectativa es considerada altamente relevante para la continuidad de operaciones, básicamente significa que la parte interesada tiene altas expectativas – prácticamente, una parte interesada puede esperar que “SIEMPRE funcione”, lo que significa que el DNS siempre está en funcionamiento; entonces la relevancia será ALTA.

En la tabla siguiente, se muestra una lista no exhaustiva con algunos **ejemplos** que pueden utilizarse para ayudar en este ejercicio. En la práctica, se recomienda primero analizar y actualizar la tabla, e identificar las partes interesadas, nombrarlas (para las entrevistas), pensar sobre la redacción de las expectativas en oraciones cortas y, por último, evaluar su relevancia para la continuidad de operaciones.

Parte Interesada	**Expectativas**	**Relevancia para BC**
Gobierno	Disponibilidad total del DNS Integridad de la exactitud del registro Disponibilidad del sistema de registro Centro de experiencia en el DNS Investigación y desarrollo en el DNS Uso indebido de nombres de dominio	ALTA ALTA ALTA n/a n/a n/a
ICANN	Registración de ccTLD de la IANA	n/a
Junta Directiva	Disponibilidad total del DNS Integridad de la exactitud del registro Disponibilidad de sistemas corporativos	ALTA ALTA MEDIA
Público en general	Disponibilidad de DNS Disponibilidad de registración de dominios	ALTA ALTA
c-CERT	Seguridad de la información Acceso a datos de registratario	BAJA n/a
Empleados	Disponibilidad de sistemas corporativos	ALTA
Aplicación de la ley	Integridad de registración de dominios	BAJA
Registradores	Disponibilidad de registración de dominios	MEDIA
Registratarios	Disponibilidad de resolución de dominios Integridad de registración de dominios	BAJA BAJA

ISP local	Resolución de dominios Apoyo de las DNSSEC	ALTA n/a
Comunidad de resolutores	Acceso al archivo de zona	n/a

Tabla 1

Dicha lista ayudará a definir las prioridades generales respecto de la continuidad de operaciones.

La cadena de suministro

En una empresa moderna, las organizaciones dependen de un número de socios, suministradores, proveedores de servicios, etc... estos tienen obviamente un impacto importante en la Estrategia de Continuidad de Operaciones y, por ende, uno debería comprender la dependencia de la organización de su cadena de suministro. Un ejercicio valioso e indispensable es enumerar a todos los proveedores que tienen un impacto en la misión operativa de la organización.

Un modo práctico de crear la lista es solicitarle al departamento de finanzas una lista de todos los proveedores, con una breve descripción de lo que realmente suministran. A partir de esa lista, uno puede determinar qué proveedores tienen un impacto real en la flexibilidad operativa. Ejemplo: un proveedor de centro de datos evidentemente tendrá una relevancia ALTA para la continuidad de operaciones; un proveedor de amoblamiento como “Ikea”, por otro lado, será menos relevante.

Según el efecto de un incidente con el proveedor, usamos una etiqueta de impacto diferente:

Impacto	**Efecto**
CRÍTICO	Inmediato
ALTO IMPACTO	Dentro de una semana o 7 días
MEDIANO IMPACTO	Dentro de un mes o 30 días
BAJO IMPACTO	Más de un mes o 30 días

Tabla 2

En la tabla siguiente, se muestra un **ejemplo** para ayudar a crear esta lista de proveedores:

Proveedor (nombre)	**Descripción**	**Relevancia para BC**	**Impacto**
ISP	Proveedor de	ALTA	CRÍTICO

	Servicios de Internet		
Procesador de tarjetas de crédito	Entidad que facilita la comunicación entre el comerciante y el banco del titular de la tarjeta	MEDIANA- ALTA	ALTO IMPACTO
Compañía de telefonía	Proveedor de telefonía fija	MEDIANA	MEDIANO IMPACTO
Servicio postal	Proveedor de servicio postal (correo)	BAJA	BAJO
Compañía de energía	Restauración de energía		
Compañía de nóminas de pago	Pago a los empleados		
Compañía de servicios informáticos	Compra de equipos de escritorio para empleados, servidores para servicios		
Proveedores de redes/ISP			
Operadores de redes móviles			
Compañías de seguros			

Tabla 3

Determinación del alcance de la continuidad de operaciones

La continuidad de operaciones como concepto básico de la estrategia de BC

La continuidad de operaciones comprende todas las actividades que se requieren para operar “el negocio de manera habitual”. Esto implica respaldar a las partes interesadas tales como registradores, registratarios y el público en general desde un punto de vista técnico, comercial y legal. También implica ejecutar todos los servicios técnicos para registrar y gestionar nombres

de dominio, apoyar el negocio y, por último, pero no menos importante, asegurarse de que el espacio de nombres de TLD esté disponible para todos en Internet.

Gran parte de las implicancias tecnológicas debería ser abordada por prácticas de ingeniería estándar y, por ende, la continuidad de operaciones se centra en evaluar un inventario de incidentes disruptivos y su resultado estimado y supuesto respecto de la preparación operativa. Define la mitigación mediante políticas, procedimientos y, donde sea necesario, tecnología.

El alcance de la continuidad de operaciones puede, por ende, resumirse de la siguiente manera:

> La gestión de medidas **preventivas** y **correctivas** mediante políticas, procedimientos, pruebas y tecnología para garantizar **la preparación y continuidad operativas** frente a eventos **disruptivos**, ya sea de naturaleza **técnica** como **de otra índole**.

Liderazgo

El desarrollo y mantenimiento de una estrategia de continuidad de operaciones eficaz y eficiente es un esfuerzo continuo que requiere apoyo de la administración de más alto nivel. Por lo tanto, el mejor lugar para albergar y apoyar iniciativas relacionadas con la continuidad de operaciones es el equipo de administración o incluso la junta.

Aunque se requieren revisiones periódicas para mantener los planes actualizados y relevantes, la administración debería también tomar la iniciativa de incluir la continuidad de operaciones en todas las capas de operaciones (tecnología, ingeniería, compra, operaciones, etc.).

ACCIÓN: implementar y supervisar al menos un ciclo de revisión anual por el equipo de administración.

Planificación

Esta sección responde a la pregunta de cómo desarrollar planes de continuidad de operaciones prácticos que tengan en cuenta las amenazas y vulnerabilidades que son relevantes para el operador de registro, así como el impacto en la flexibilidad operativa de la organización.

Primero, comenzaremos con la creación de un registro de amenazas/peligros que nos ayude a definir en qué áreas debemos abordar la continuidad de operaciones. Tenga en cuenta que es difícil, e incluso imposible, mitigar algunas amenazas o estar preparados para abordarlas. Resulta útil investigar la amenaza y evaluar las opciones estratégicas. Estas posiblemente no se

traduzcan en un Plan de Continuidad de Operaciones, sino en elecciones estratégicas[1] a largo plazo.

Para traducir las amenazas y peligros en riesgos reales, debemos comprender el impacto sobre la preparación y flexibilidad operativas. Se puede utilizar una metodología de evaluación de riesgos simplificada para ayudar a determinar qué escenarios deberían abordarse. A partir de esta evaluación, diversos escenarios se traducirán en planes de continuidad de operaciones tácticos, mientras otros escenarios conducirán a una estrategia de continuidad de operaciones que puede utilizarse como aporte para la autoridad supervisora y posteriores decisiones estratégicas.

Una vez que resulta claro qué amenazas/peligros requieren un verdadero Plan de Continuidad de Operaciones, se puede crear el plan sobre la base de una plantilla genérica. Esta plantilla debería luego ser utilizada como pauta para todos los departamentos para preparar procedimientos en los casos necesarios.

Desarrollar un registro de amenazas/peligros

El registro de amenazas/peligros es una lista valiosa de orígenes de desastres que podrían tener un impacto drástico en la flexibilidad operativa de la organización. La siguiente lista de amenazas se basa en el libro *Business Continuity Management* (4° edición) - ISBN 978-1-931332-35-4 y se amplió con recientes eventos emergentes.

Al evaluar estas amenazas, una organización debería estimar la probabilidad del evento en función de los datos estadísticos disponibles. La probabilidad de ocurrencia es escalada de la siguiente manera:

1. Muy probable: un evento recurrente de manera anual o con más frecuencia
2. Probable: un evento que sucede cada tres años promedio
3. Ocasional: un evento que sucede cada diez años
4. Poco probable: un evento que sucede una vez cada 50 años o más
5. OoS: Fuera de alcance (OoS, *Out of Scope*) – estos no son considerados en la continuidad de operaciones

La probabilidad no se basa en estadísticas internas sino en estadísticas relevantes para la región, el país, el negocio y el entorno[2]. Es importante destacar que las personas deben calificar la probabilidad (tabla 7 y 8) y el impacto (tabla 6) de los riesgos con los controles de

[1] Un ejemplo típico puede ser la inestabilidad política que puede ser extremadamente difícil de mitigar, incluso como un ccTLD, es importante que esto sea tomado en cuenta en la estrategia de continuidad de operaciones general.

[2] Un ejemplo típico de eventos relacionados con el clima como tornados podrían ser muy relevantes para partes de EE. UU., pero completamente irrelevantes para otras partes de EE. UU.

seguridad actualmente implementados. Las amenazas se basan en estadísticas; sin controles específicos implementados.

Categoría de amenaza	Amenaza	Aplicable	Probabilidad
Desastres naturales	Incendio	☐	_____
	Inundación	☐	_____
	Huracán/tornado/tifón	☐	_____
	Clima adverso	☐	_____
	Terremoto	☐	_____
	Derrumbe/avalancha	☐	_____
	Actividad volcánica	☐	_____
	Tsunami	☐	_____
	Relámpagos Hundimiento	☐	_____
	Contaminación	☐	_____
	Infestación de insectos	☐	_____
	Roedores	☐	_____
	_____	☐	_____
RR. HH y Medicina	Pérdida de personal clave	☐	_____
	Enfermedad epidémica	☐	_____
	Escasez de aptitudes/personal	☐	_____
	Cuestiones familiares	☐	_____
	Robo	☐	_____
	Daño malicioso (sabotaje)	☐	_____
	Extorsión	☐	_____
	_____	☐	_____
Cibernética	DDOS	☐	_____
	Piratas informáticos	☐	_____
	Pérdida de datos	☐	_____
	Ransomware	☐	_____
	Actividades relacionadas con guerra cibernética	☐	_____
	_____	☐	_____
Externa	Recesión	☐	_____
	Desobediencia civil	☐	_____
	Actividad terrorista	☐	_____
	Guerra/invasión	☐	_____
	Interferencia política/cambios en políticas	☐	_____
	Hurto	☐	_____
	Cambios tecnológicos/relevancia	☐	_____
	_____	☐	_____
Asuntos financieros	Problemas de flujo monetario/liquidez	☐	_____
	Falta de capital	☐	_____

	Malversación financiera	☐	_____
	Deuda incobrable	☐	_____
	Riesgo de intereses	☐	_____
	Riesgo de tipo de cambio	☐	_____
	Exposición de fondos públicos	☐	_____
	_____	☐	_____
Tecnología e infraestructura	Falla de red – global	☐	_____
	Electricidad – fallas de cuadrícula	☐	_____
	Fallas de CA	☐	_____
	Fallas de centros de datos	☐	_____
	Fallas de componentes[3]	☐	_____
	_____	☐	_____
Falla de suministro	Falla a nivel de servicio	☐	_____
	Defectos de calidad	☐	_____
	Pérdida de servicios suministrados	☐	_____
	Tercerización fallida/situaciones de falta de stock de contrato de suministros	☐	_____
	Pérdida de otros activos vitales	☐	_____
	Dependencia del proveedor	☐	_____
	_____		

Tabla 4

Reconoce sin motivo alguno que un operador de registro debería centrarse en las amenazas que son relevantes para su región y su contexto comercial; la lista no exhaustiva mencionada anteriormente sirve como un ejemplo. También es posible comenzar con un conjunto de amenazas/peligros y expandirlo más adelante.

ACCIÓN: el coordinador o gerente de BC debería centrarse en amenazas/peligros conocidos y expandirse a partir de allí en el ciclo de revisión periódica.

Evaluación y gestión de riesgos

¿Qué es riesgo? Tipos de riesgo.

Riesgo, según la definición contenida en la norma ISO 31000 es: “el efecto de incertidumbre en objetivos”, la cual constituye una definición muy genérica y abstracta. Traducido a la

[3] Las fallas de componentes es un marco genérico para hacer referencia al mal funcionamiento de sistemas informáticos, fuentes de alimentación, memoria de computadoras, discos, etc... uno puede decidir incluir esto dentro del alcance de la continuidad de operaciones o suponer que está mitigado en el diseño y arquitectura de la infraestructura de manera predeterminada (por ejemplo, fuentes de alimentación redundantes, sistemas de discos RAID, memoria ECC en servidores, etc...).

continuidad de operaciones y continuidad y flexibilidad operativas, el riesgo sería “el efecto de un evento disruptivo en la misión operativa de un operador de registro de ccTLD”.

Si uno se inclina a realizar una evaluación de riesgos formal pero simple, se puede utilizar la siguiente tabla:

Riesgo	**Descripción**
Asuntos financieros	El evento ocasiona costos directos e indirectos a la organización. Según la estabilidad financiera de la organización, ciertas pérdidas financieras son aceptables.
Operativo	El evento impide que la organización lleve a cabo su misión operativa (por ejemplo, los Servicios de Nombres de Dominios son interrumpidos).
Reputación	El evento puede causar un daño a la reputación que tiene un impacto directo o indirecto en la misión operativa.
Legal	El evento ocasiona desafíos legales que pueden generar sanciones o incluso condenas penales.
Gobernanza	El evento causa repercusiones políticas e incumplimiento, lo que puede generar la terminación de un contrato de concesión o interferencia política.
Humano	El evento ocasiona daño físico a los empleados (o sus familias).

Tabla 5

Cada riesgo tiene evidentemente diferentes niveles y, según el nivel, uno puede decidir considerarlo en los planes de continuidad de operaciones. Algunos ejemplos:

- una pérdida económica de 1 millón de euros puede generar una quiebra fáctica del operador de registro.
- un evento que genere la condena penal de personas no puede ser aceptable para el operador de registro.
- un evento que causa daño físico a los empleados no puede ser aceptable.

La tabla no es exhaustiva y el operador de registro puede decidir qué usar en qué niveles. La siguiente tabla ilustra cinco niveles de riesgo por tipo de riesgo. Depende del operador de registro decidir la aplicabilidad de estos niveles y los valores reales.

Tipo	NULO o n/a	Bajo	Medio	Alto	Crítico
Asuntos financieros	el riesgo no existe o no es aplicable	< 1.000 USD	< 10.000 USD	< 100.000 USD	> 100.000 USD
Operativo		afecta a una persona	afecta a un departamento	afecta al registro	afecta al público
Reputación		interna	grupos de usuarios (ICANN, CENTR)	pública	medios/políticas
Legal		sanción administrativa	multa < 10.000 USD	multa < 100.000 USD	multa > 100.000 USD, responsabilidad personal o condena penal
Gobernanza[4]		junta	gobierno local	escrutinio político	terminación de registro
Humano		no se usa el nivel	no se usa el nivel	familia de compañeros de trabajo	daño personal

Tabla 6

Se recomienda codificar con colores los diferentes niveles ya que esto puede utilizarse con posterioridad para crear un mapa de situación visual de todos los riesgos aplicables frente a los riesgos incurridos.

Evaluación de riesgo simple / Evaluación de impacto en operaciones

La adición de los diferentes riesgos tal como se describe anteriormente a la matriz de riesgos/peligros brinda una herramienta simple para observar el impacto en las operaciones.

A continuación, se brinda un ejemplo para ilustrar esto. El escenario está constituido por los ataques de DDOS en la infraestructura operativa de los ccTLD (incluidos, a mero modo enunciativo, el servidor de nombres de dominio para el .tld, así como los servicios de

[4] Los riesgos de gobernanza son posiblemente los tipos de riesgos más difíciles y, al mismo tiempo, los más específicos. Para algunos registros, el riesgo puede incluso no existir. Esto requiere gestión para definir y describir claramente la forma en que el registro depende de las influencias externas.

registración; suponemos que el operador de registro tiene un pequeño espacio de infraestructura donde todos los servicios se combinan y no se utiliza un proveedor de anycast para el DNS).

Categoría de amenaza	**Amenaza**	**Aplicable (Sí/No)**	**Probabilidad**
Cibernética	DDOS	SÍ	Muy probable
Riesgos	**Nivel**		
Asuntos financieros	MEDIO	El ataque de DDOS no ocasiona costos directos ya que no causa ninguna destrucción física de los bienes. El mayor costo está constituido por las personas que tratan el incidente. Obviamente, se incurre en un costo indirecto ya que no hay nombres de dominio registrados mientras sucede el ataque.	
Operativo	CRÍTICO	Todo el .TLD no está disponible o bien está disponible de manera intermitente. Esto tiene un enorme impacto operativo en Internet. De manera similar, otros servicios como el sitio web corporativo, el WHOIS público y otros servicios de registración se ven afectados.	
Reputación	ALTO/CRÍTICO	El incidente será notado por cualquier persona en Internet.	
Legal	ALTO	Con posterioridad al incidente, los registratarios y registradores pueden presentar denuncias por los ingresos perdidos. (Esto depende de los Términos y condiciones del registro y de la jurisdicción del registro)	
Gobernanza	ALTO	Dado que la mayoría de los ccTLD pueden ser considerados Operadores de Servicios Esenciales (para citar la directiva NIS de la Unión Europea), es seguro suponer que habrá algunas investigaciones del gobierno.	

Humano	NULO	Ningún empleado se verá afectado, directa o indirectamente, con daño físico a causa de este evento.
RTO	Para el DNS es cero; el servicio nunca debería dejar de funcionar. Todos los otros servicios afectados por el DDOS deberían estar disponibles dentro de un día hábil.	
RPO	Para el DNS: la degradación de los servicios al 50 % de la capacidad del servidor de nombre es aceptable; todos los demás servicios deberían estar totalmente accesibles; la degradación de la capacidad es aceptable hasta un 50 %.	

Tabla 7

El RTO u Objetivo de Tiempo de Recuperación define la rapidez con la que el servicio debería restaurarse. Esto refleja la expectativa de las partes interesadas o las obligaciones contractuales o legales. Tenga en cuenta que se pueden definir diferentes RTO para una amenaza o un peligro en función de los servicios afectados.

El RPO u Objetivo de Punto de Recuperación define el nivel en que los servicios deberían restaurarse. Esto puede tomar muchas formas tales como capacidad reducida (menos servidores de nombres disponibles, capacidad reducida de un servidor, etc.), servicios demorados, restauración de datos hasta un cierto punto, etc.

El RTO y el RPO deberían basarse exclusivamente en los aportes del negocio y no depender de “lo que es posible” cuando se produce el incidente.

Esta evaluación brinda una buena indicación de que la amenaza debería ser tenida en cuenta y que se requiere el tratamiento del riesgo.

Tolerancia y tratamiento de riesgos

Existen aproximadamente 5 modos de tratar los riesgos:

1. Aceptar el riesgo (no realizar ninguna acción).
2. Evitar el riesgo (implementar un plan alternativo).
3. Reducir el riesgo (cambiar la ecuación).
4. Contener el riesgo (minimizar el impacto).
5. Transferir el riesgo (entregárselo a otra persona, seguro).

Los Planes de Continuidad de Operaciones consisten en la opción 4, en la cual mediante acciones predefinidas el impacto es contrarrestado y la misión operativa se restaura a un nivel predefinido.

Por otro lado, el resultado de la Evaluación del Impacto en Operaciones también debería ser considerado ya que podría conducir a pasos preliminares (Paso 3, reducir el riesgo) y acciones para reducir el riesgo y alcanzar el RTO y el RPO.

Regresemos al ejemplo anterior e investiguemos qué puede hacerse para reducir el riesgo a un nivel aceptable.

En este caso específico, resulta evidente que el DNS tiene prioridad absoluta, los servicios públicos como el sitio web, corporativo y el funcionamiento del WHOIS público, se ubican en segundo lugar y, por último, pero no menos importante, se encuentran los servicios de registración.

Categoría de amenaza	**Amenaza**	**Aplicable (Sí/No)**	**Probabilidad**
Cibernética	DDOS	SÍ	Muy probable
Mitigación de riesgos			
Aceptar el riesgo	no aplicable		
Evitar el riesgo	imposible; los ataques de DDOS son iniciados por adversarios desconocidos.		
Reducir el riesgo	la infraestructura existente no podrá garantizar los requisitos esperados de RTO/RPO. Una solución posible es utilizar una solución anycasting para el DNS o servicios de limpieza para los demás servicios		
Contener el riesgo	desarrollar un Plan de Continuidad de Operaciones para DDOS (mediante el uso del manual para la mitigación de DDOS de la ccNSO como referencia), incluyendo medidas técnicas adicionales (como reubicación temporaria de algunos servicios), plan de comunicaciones y un plan de apoyo		
Transferir el riesgo	no aplicable		

Tabla 8

El plan de tratamiento del riesgo contendrá diferentes acciones que se extraen de la tabla anterior. Algunas pueden implementarse de inmediato, otras pueden requerir presupuesto adicional y posterior aprobación y planificación.

Plan de tratamiento de riesgos

Al hacer la evaluación de riesgos/evaluación inicial del impacto en operaciones, varios escenarios conllevarán a niveles no aceptables de riesgo o los requisitos o expectativas de RTO/RPO no pueden ser garantizados en el presente.

Esta brecha puede cerrarse con acciones específicas para reducir los riesgos. Estas medidas deben registrarse e incluirse en un plan, denominado plan de tratamiento de riesgos. El plan de tratamiento de riesgos no forma parte del plan de continuidad de operaciones, pero existe de manera paralela. Consiste en inversiones adicionales, reingeniería de servicios o infraestructura existentes y tercerización de ciertas actividades, entre otros.

Plan de Continuidad de Operaciones

Antes de poder elaborar el plan, es posible que algunos términos deban ser explicados. Como se mencionó anteriormente, el Plan de Continuidad de Operaciones (BCP) sirve como orientación y como un plan de acción para gestionar una crisis cuando ha ocurrido un evento disruptivo específico.

En general, una crisis es casi siempre manejada del mismo modo:

1. evaluar la situación
2. contener el evento
3. recuperarse a los niveles predefinidos dentro del RTO (Objetivo de Tiempo de Recuperación) y RPO (Objetivo de Punto de Recuperación)
4. retirarse

Tenga en cuenta que el final de una crisis, marcada con el retiro, no implica que la organización haya vuelto a la situación “anterior al incidente”. “Retiro” implica que el equipo de crisis considera que la crisis está bajo control, el servicio se ha restaurado, la organización puede llevar a cabo su misión operativa. Esto no implica que se haya reparado todo el daño.

Un ejemplo puede ilustrar mejor y aclarar esto: durante el fin de semana, vándalos destruyeron y saquearon la oficina principal del registro. *Robaron los equipos de TI, destruyeron los muebles, básicamente la organización no puede trabajar desde la oficina debido a los daños y se están llevando a cabo investigaciones. El BCP se activa y ordena que cuando no se puede acceder a la oficina, los teléfonos se redirigen a dispositivos móviles, se informa a los empleados que permanezcan en sus casas y trabajen desde allí hasta nuevo aviso (esto implica que el teletrabajo no es un problema). El equipo de crisis maneja el contacto inicial con los agentes de aplicación de la ley, el seguro y otras partes, y se asegura de que se ejecute el BCP anterior. Una vez realizado esto, el servicio se restaurará a un nivel aceptable y la organización podrá continuar con su misión operativa. El equipo de crisis asigna recursos para seguir manejando el caso y regresa la oficina a su estado anterior. En ese momento, el equipo de crisis se retira y*

reanuda su rol operativo normal. Evidentemente en una organización pequeña, habrá una superposición simplemente debido a los recursos limitados disponibles.

Materiales vitales es un conjunto de información (digital o física) que es absolutamente necesaria para gestionar el incidente. Estos pueden ser contratos, información de contacto para servicios específicos (por ejemplo, proveedores de redes, servicios de limpieza, el propietario, autoridades, etc.), inicios de sesión y contraseñas, activos físicos tales como llaves, etc... no se olvide de proteger correctamente este material sensible y de mantenerlo accesible durante una crisis.

Plan de Continuidad de Operaciones: una vez identificados los escenarios que tienen el riesgo más alto, es momento de elaborar un plan. Uno puede decidir escribir un plan detallado con cada uno de los pasos a ejecutar durante un desastre. Si bien esto es perfectamente posible, los desastres tienden a generar eventos colaterales no esperados que dificultan escribir cada paso que debe realizarse. Según la experiencia, una guía general que repita los pasos esenciales durante la gestión de la crisis resulta de mayor utilidad. Dicho plan puede entonces utilizarse durante capacitación, pruebas y simulación.

Uno también debería analizar el efecto del escenario. No tiene sentido redactar varios planes de BC que finalmente puedan tener diferentes escenarios, pero conllevan al mismo plan. Un ejemplo típico es un incidente que hace que la oficina no esté disponible/accesible. El motivo (incendio, huelga, apagón eléctrico, inundación, Viernes Negro) no es relevante, el resultado es el mismo. Esto entonces puede traducirse en un plan de BC.

La plantilla que se muestra más abajo es compacta y repasa todos los pasos mencionados anteriormente para manejar el desastre. Asimismo, ayuda a definir algunas tareas preparatorias. **Tenga en cuenta que improvisar durante una crisis es el peor resultado posible.** La plantilla es en definitiva solo una guía de referencia para ayudar al equipo de crisis a tratar la situación y a estar preparado.

PLAN DE CONTINUIDAD DE OPERACIONES (PLANTILLA)			
Referencia:	[REFERENCIA]	Tipo de amenaza	Activos afectados
Escenario:	*Describe las condiciones que activaron el Plan. Esto puede ser un evento, un plazo, una condición específica, etc.*		
ACTIVACIÓN:	*¿Cuándo se activa el plan? Se puede activar inmediatamente al momento de la detección o varias horas después de que el incidente tuvo lugar.*		
RTO:	*Objetivo de Tiempo de Recuperación*		
RPO:	*Objetivo de Punto de Recuperación*		
Equipo de crisis:	*¿Quién es el equipo de crisis? ¿Quién realmente se encargará del incidente? Usar nombres de empleados, socios, proveedores para evitar ambigüedades.*		
Prioridades:	*¿Cuáles son las prioridades? Esto debería ser interpretado como una lista secuencial.*		
Evaluación:	*La etapa inicial de manejar un incidente disruptivo es evaluar el grado del incidente. Describir los factores que deberían tenerse en cuenta.*		
Contención:	*Describir el curso de acción para prevenir un empeoramiento de la situación.*		
Recuperación:	*Describir el curso de acción para restaurar la preparación operativa mínima, considerando las prioridades definidas anteriormente.*		
Retiro:	*Una vez recuperadas las operaciones, el equipo de crisis se retira y deja instrucciones para llevar adelante posteriores acciones para volver a la situación anterior al incidente.*		

Comunicación:	*Definir las comunicaciones internas y externas, incluidos el mensaje y la lista de distribución, así como los medios. Siempre comenzar con la comunicación interna.*
Materiales vitales:	*Lista de recursos necesarios para gestionar el incidente. Esto es parte de la etapa de preparación. El plan no incluye el contenido real, sino que está limitado a referencias (es responsabilidad de los jefes de los diferentes departamentos o socios conservar este contenido, mantenerlo actualizado, y preciso y portable cuando sea posible)*
Registros:	*Los registros que deben elaborarse durante y después de la crisis. Estos registros son útiles para la recopilación de evidencia, lecciones aprendidas y un seguimiento del incidente real.*

Tabla 9

En el anexo, se incluyen ejemplos de Planes de BC.

Apoyo

Recursos

El esfuerzo inicial de configurar un sistema (de gestión) de continuidad de operaciones puede insumir bastante tiempo, pero la metodología descripta anteriormente debería hacerlo más práctico y factible para una organización más pequeña.

Una vez elaborados los inventarios y listas, el esfuerzo se vuelve más sostenible de manera tal que solo se necesitan revisiones anuales para actualizar los planes teniendo en cuenta el cambiante panorama de amenazas y peligros, por ejemplo, los ciberataques estaban en su mayoría en el ámbito de la ciencia ficción a principios de los años 2000; hoy en día, deberían ser considerados como un peligro claro y presente.

En una organización pequeña, el mejor lugar para gestionar y guiar el desarrollo exitoso de un plan de continuidad de operaciones es a nivel de la administración y el proyecto debería recibir suficiente apoyo y enfoque.

No es realmente necesario designar a un gerente dedicado a la continuidad de operaciones; en algunos casos, la estrategia de BC puede ser aun más eficaz al incluir esto en las responsabilidades de toda la organización.

Conocimiento

Una estrategia de continuidad de operaciones exitosa requiere el conocimiento en toda la organización y la comprensión de que debería ser importante para todos.

Por ende, las sesiones de conocimiento periódicas son absolutamente indispensables.

Comunicación

Como se muestra en la plantilla y el ejemplo de Planes de Continuidad de Operaciones, la comunicación (interna y externa) tiene un rol muy importante en la gestión de crisis.

Por ende, es muy importante:

1. decidir los medios de comunicación que se utilizarán. Ejemplo: teléfono, mensajes de texto, mensajería, Twitter, correo electrónico, etc.
2. preparar plantillas de comunicaciones (la comunicación improvisada puede realmente acabar con la credibilidad de una organización durante una crisis).
3. predefinir y preparar a quiénes debería enviarse la comunicación, por ejemplo, “nuestros registradores” no es una definición práctica. Un indicador a una lista de direcciones de correo electrónico que esté actualizado sí lo es.
4. establecer prioridades y cronogramas para la comunicación (por ejemplo, tuitear una actualización cada 60 minutos, enviar un correo electrónico al comienzo y al final del incidente).
5. evaluar la necesidad de un consultor externo para comunicaciones de crisis para ayudar a configurar los planes y estrategia de comunicaciones, pero también para capacitar a la gente que trata con la prensa.

Operación

Una vez elaborado el BCP, debería incluirse en las operaciones nominales y comerciales diarias. Esto significa que la continuidad de operaciones debe tener un rol en todos los procesos y flujos de trabajo de negocio y de ingeniería.

Esto implica que la continuidad de operaciones juega un rol en diferentes áreas tales como: compras, asuntos legales, ingeniería, operaciones, comunicaciones.

Algunos ejemplos para aclarar esto:

- se compran algunos servidores y equipos de red. La Solicitud de Propuesta (RFP) que se envía a los proveedores menciona **fuentes de alimentación redundantes** y **tarjetas de interfaz de red** duales para máxima redundancia.

- se **terceriza** un servicio, la RFP menciona explícitamente las medidas de continuidad de operaciones prevista que son esperadas del proveedor de servicios.

Ejercicios de BC

Está bien desarrollar planes para lidiar con un escenario de desastre específico, pero sin ninguna prueba o simulación, el plan es un *tigre de papel*.

Las pruebas y simulación de los planes de BC son, por ende, un componente vital en una estrategia de continuidad de operaciones eficaz. Así como los bomberos se capacitan para combatir incendios, el equipo de crisis debería dedicar tiempo en probar y simular los planes.

Hay dos maneras de hacer esto. Existe el denominado ejercicio de simulación teórica o TTX y la simulación controlada real.

Ejercicios de simulación teórica (TTX)

Estos ejercicios en "papel" tienen el fin de analizar procedimientos y son extremadamente útiles para los equipos de simulación. Requieren relativamente poca preparación.

Un TTX puede ser un ejercicio de juego de roles en el que todas las partes participantes se sientan a la mesa y cada uno juega su rol. **Un "maestro de la ceremonia" independiente** guiará al equipo a través de los diferentes pasos del escenario, intercalados con ocasionales eventos adicionales inesperados.

Una gran desventaja del TTX es la dificultad de darle sentido de urgencia y realidad a los participantes.

ACCIÓN: es esencial que toda la organización revise los planes de BC al menos una vez al año con una visión crítica hacia la factibilidad. Los planes de BC son documentos vivos que deberán ser adaptados a un entorno cambiante.

Simulaciones

De manera ideal, los Planes de Continuidad de Operaciones se prueban con simulaciones reales. Durante estas simulaciones, se comprueba la respuesta de los diferentes equipos o socios a fin de validar la eficacia de los equipos y la factibilidad de los planes.

Al simular los diferentes planes, los equipos se acostumbrarán a lo que necesitarán hacer cuando el evento suceda realmente.

Evidentemente, no siempre resulta sencillo simular realmente el incidente (por ejemplo, falta de suministro eléctrico en el centro de datos), pero se pueden proponer escenarios realistas.

Algunos ejemplos:

- ataque de ransomware Un usuario llama a la mesa de ayuda para preguntar qué hacer ya que la pantalla indica que el equipo portátil ha sido capturado y se exigen algunas bitcoins a cambio de desbloquear el equipo. El propósito de este ejercicio es probar la respuesta del equipo de apoyo.
- la oficina no está accesible debido a una infestación de ratas. Evidentemente no hay ratas, pero el objetivo es probar la comunicación con los empleados.

Mejoras

Una medida esencial para cualquier Estrategia de Continuidad de Operaciones eficaz es revisar los planes, la evaluación de riesgos, la lista de partes interesadas y la lista de amenazas y peligros, entre otros, al menos una vez al año o si se han producido cambios importantes.

Por lo general, estos cambios son iniciados por diversas acciones:

- legislación emergente
- tercerización
- fusiones y adquisiciones
- servicios nuevos
- cambio de partes interesadas
- tecnologías emergentes
- cambio del panorama de amenazas
- un incidente
- ...

Anexo: Resumen de tareas

En este anexo, se resumen las diferentes tareas descriptas en el documento. Se puede usar como una lista de verificación para realizar la implementación.

1. realizar un inventario de todas las **partes interesadas** y sus expectativas, identificar las expectativas que son relevantes para la continuidad de operaciones (tabla 1)
2. realizar un inventario de todos los **proveedores**, describir qué suministrar e identificar la relevancia para la continuidad de operaciones y el impacto (tabla 3)
3. usar la tabla 4 para crear un **registro de amenazas y peligros**, marcar cuáles son aplicables y cuál es la probabilidad
4. usar la tabla 5 para identificar los **riesgos** que son aplicables a la organización; usar la tabla 6 para definir los diferentes niveles por riesgo
5. tomar el registro de amenazas y peligros (tabla 4) y copiar las amenazas y los peligros aplicables en la **evaluación del impacto en operaciones** (tabla 7). Se pueden resumir todas estas tablas en un mapa de situación donde los niveles de riesgo se codifican con colores como se muestra en el ejemplo a continuación:

Categoría de amenaza	**Amenaza**	**Asuntos financieros**	**Operativo**	**Reputación**	**Legal**	**Gobernanza**	**Humana**
Cibernética	DDOS	Media	Crítica	Alta/ Crítica	Alta	Alta	Nula

6. expandir la tabla 7 que se utilizó para la evaluación simple del impacto en operaciones y agregarle el **tratamiento de riesgos** (tabla 8). Habrá un número de amenazas que resultarán en un riesgo inaceptable si no se mitigan; por ende, del tratamiento de riesgos se genera un plan de tratamiento de riesgos que contiene acciones para reducir el riesgo. Esto no implica que los riesgos sean neutralizados; implica que estos sean reducidos.
7. Crear los **Planes de Continuidad de Operaciones** mediante la tabla 9 como plantilla para aquellos peligros y amenazas que sean considerados una amenaza real con un alto impacto para la organización.

Anexo: Ejemplo de Plan de Continuidad de Operaciones

PLAN DE CONTINUIDAD DE OPERACIONES (PLANTILLA)			
Referencia:	[REFERENCIA]	Tipo de amenaza	Activos afectados
Escenario:	*Describe las condiciones que activaron el Plan. Esto puede ser un evento, un plazo, una condición específica, etc.*		
ACTIVACIÓN:	*¿Cuándo se activa el plan? Se puede activar inmediatamente al momento de la detección o varias horas después de que el incidente tuvo lugar.*		
RTO:	*Objetivo de Tiempo de Recuperación*		
RPO:	*Objetivo de Punto de Recuperación*		
Equipo de crisis:	*¿Quién es el equipo de crisis? ¿Quién realmente se encargará del incidente? Usar nombres de empleados, socios, proveedores para evitar ambigüedades.*		
Prioridades:	*¿Cuáles son las prioridades? Esto debería ser interpretado como una lista secuencial.*		
Evaluación:	*La etapa inicial de manejar un incidente disruptivo es evaluar el grado del incidente. Describir los factores que deberían tenerse en cuenta.*		
Contención:	*Describir el curso de acción para prevenir un empeoramiento de la situación.*		

Recuperación:	*Describir el curso de acción para restaurar la preparación operativa mínima, considerando las prioridades definidas anteriormente.*
Retiro:	*Una vez recuperadas las operaciones, el equipo de crisis se retira y deja instrucciones para llevar adelante posteriores acciones para volver a la situación anterior al incidente.*
Comunicación:	*Definir las comunicaciones internas y externas, incluidos el mensaje y la lista de distribución, así como los medios. Siempre comenzar con la comunicación interna.*
Materiales vitales:	*Lista de recursos necesarios para gestionar el incidente. Esto es parte de la etapa de preparación. El plan no incluye el contenido real, sino que está limitado a referencias (es responsabilidad de los jefes de los diferentes departamentos o socios conservar este contenido, mantenerlo actualizado, y preciso y portable cuando sea posible)*
Registros:	*Los registros que deben elaborarse durante y después de la crisis. Estos registros son útiles para la recopilación de evidencia, lecciones aprendidas y un seguimiento del incidente real.*

CIBERNÉTICA: HACKING

PLAN DE CONTINUIDAD DE OPERACIONES			
Referencia:	BCP-xxx.yy	CIBERNÉTICA: HACKING	Global
Escenario:	La evidencia muestra que la infraestructura del registro fue hackeada y comprometida. Un actor desconocido ha instalado software, creado cuentas, herramientas de acceso remoto, etc., para infiltrarse en el registro. Posiblemente, se robaron datos (sensibles). .		
ACTIVACIÓN:	INMEDIATAMENTE AL MOMENTO DE LA DETECCIÓN		
RTO:	24 hs.		
RPO:	Pérdida de datos de 24 hs.		
Equipo de crisis:	Gerente de Asuntos Legales - +CC 123 55 88 - ivan.horvat@registry.tld Gerente de Tecnología – +CC 123 44 55 – juan.perez@registry.tld Gerente de BC – +CC 123 33 66 – jane.doe@registry.tld Gerente General - +CC 123 56 44 - yamado.toro@registry.tld		
Prioridades:	Proteger la disponibilidad e integridad de los servidores de nombres y la zona .tld. Si es necesario, aislar la infraestructura de servidores de nombres. Aislar los sistemas hackeados. Recolectar evidencia.		
Evaluación:	Si se encuentran pruebas de que se filtraron datos, activar también el BCP para filtración de datos. Evaluar y realizar un inventario de los sistemas afectados. ¿Qué servicios se ven afectados? ¿Se vieron afectados el DNS, la plataforma de registración, los servicios internos, el sitio web? Volver a revisar la infraestructura de servidores de nombres.		

	¿El hacker tiene un punto de apoyo permanente? ¿El hacker está presente al momento de la detección? ¿Se necesita ayuda externa de una compañía especializada en incidentes cibernéticos (hay evidencia de actores estatales)?
Contención:	Asegurarse de que la infraestructura de servidores de nombres esté protegida y aislar los servidores de nombres del área afectada. Desactivar o apagar los sistemas afectados. No intentar reparar o corregir los sistemas afectados o combatir al intruso. Concentrarse en aislar los sistemas afectados. Intentar recopilar evidencia; no alterar la evidencia
Recuperación:	Los sistemas afectados deberían reconstruirse y reimplementarse. Si el equipo del usuario final se ve afectado, se implementan sistemas nuevos.
Retiro:	Una vez que los sistemas afectados han sido aislados y desactivados y los servicios restaurados mediante sistemas de reconstrucción y reimplementación, el equipo de crisis asigna un equipo para manejar las actividades siguientes: 1. Contactarse con los agentes de aplicación de la ley y presentar una denuncia. 2. Asegurarse de que los sistemas afectados se almacenen de manera segura y los archivos de registro se separen como evidencia. Analizar la integridad de la base de datos central (¿hay rastros de cambios?).
Comunicación:	Comunicación interna únicamente La comunicación a todos de que nuestros sistemas han sido afectados y que estamos aislando dichos sistemas. Remarcar que la posterior comunicación al mundo exterior será manejada por el Gerente de Comunicaciones, Gerente de Asuntos Legales directamente. Comunicación externa: Informar a las partes interesadas (junta, autoridades)

	Informar a los registradores si los sistemas se desactivarán (por ejemplo, sitio web WHOIS, EPP) e informarles de los futuros pasos que se tomarán. Informar a los agentes de aplicación de la ley.
Materiales vitales:	Documentación de la infraestructura y configuración. Almacenes de contraseñas para tener acceso a los diferentes sistemas. Implementación y preparación de infraestructura para implementar nueva infraestructura. Listas de distribución de comunicaciones (registradores, empleados)
Registros:	Crear un registro del incidente, qué se descubrió, qué acciones se realizaron, qué evidencia se recopiló. Realizar estas acciones durante el manejo de la crisis y no con posterioridad.

EXTERNA: ATAQUE TERRORISTA

PLAN DE CONTINUIDAD DE OPERACIONES			
Referencia:	BCP-xxx.yy	EXTERNA: ATAQUE TERRORISTA	Oficina
Escenario:	Se produjo un ataque terrorista cerca de la oficina corporativa del registro. Cerca significa en la misma ciudad o dentro de un radio de 25 km. Este plan es aplicable las 24 horas, los 7 días de la semana.		
ACTIVACIÓN:	DE INMEDIATO		
RTO:	No definido		
RPO:	No definido		
Equipo de crisis:	Oficina responsable - +CC 123 44 55 - jan.modaal@registry.tld Gerente de RR. HH. - +CC 123 66 23 - maija.meikalainen@registry.tld Gerente de BC – +CC 123 33 66 – jane.doe@registry.tld Gerente General - +CC 123 56 44 - yamado.toro@registry.tld		
Prioridades:	Seguridad de los empleados.		
Evaluación:	Según la gravedad del ataque, las consecuencias pueden ser problemáticas (cierre de emergencia de transporte público, despliegue de equipos SWAT, etc.). Primero y principal, los empleados y sus familias deben estar seguros. Dado que el registro está a favor del trabajo desde casa, los trabajadores no deberían permanecer ni concurrir a la oficina.		
Contención:	Si la situación lo permite, se cerrará la oficina de inmediato y se enviará a los empleados a sus casas. Si el ataque es demasiado cerca de la oficina, se les recomendará a los empleados que permanezcan allí y sigan las instrucciones de los agentes gubernamentales y de aplicación de la ley.		

Recuperación:	La oficina responsable verificará que todos los empleados estén informados y contabilizados. Informará a todos los empleados que la oficina está cerrada y vedada hasta nuevo aviso. La oficina responsable informará la situación al Gerente de RR.HH. o al Gerente de BC. El Gerente de RR. HH. o el Gerente de BC informará a los departamentos y gerentes pertinentes para que se encarguen de las actividades en los casos aplicables
Retiro:	La oficina responsable seguirá las instrucciones de los agentes oficiales y de aplicación de la ley, e informará a los empleados cuando se reabra la oficina.
Comunicación:	Comunicación interna únicamente Comunicación inicial, ya sea verbalmente o por mensaje de texto (SMS) por la oficina responsable a los empleados afectados. Comunicación de seguimiento por correo electrónico enviado por la oficina responsable, Gerente de RR. HH. o de BC.
Materiales vitales:	Lista de empleados con números de teléfono y direcciones de correo electrónico.
Registros:	Registro de empleados de todos los trabajadores que han sido informados y contabilizados.

CIBERNÉTICA: RANSOMWARE

PLAN DE CONTINUIDAD DE OPERACIONES			
Referencia:	BCP-xxx.yy	CIBERNÉTICA: RANSOMWARE	Equipo de oficina y usuario final
Escenario:	Una infección de ransomware provocó que un número limitado de equipos portátiles con MS Windows no puedan usarse y estén bloqueados. La infección puede centrarse en una oficina o se está propagando a toda la organización.		
ACTIVACIÓN:	INMEDIATAMENTE AL MOMENTO DE LA DETECCIÓN		
RTO:	Dentro de un día hábil.		
RPO:	Pérdida de datos de un día hábil.		
Equipo de crisis:	Gerente de Tecnología – +CC 123 44 55 – juan.perez@registry.tld Gerente de BC – +CC 123 33 66 – jane.doe@registry.tld Gerente General - +CC 123 56 44 - yamado.toro@registry.tld		
Prioridades:	Proteger la disponibilidad e integridad de la infraestructura de Windows Server. Aislar los sistemas infectados. Volver a poner en funcionamiento los sistemas infectados.		
Evaluación:	¿La infección se está propagando? ¿Quién fue/es el paciente cero? ¿Se puede aislar la infección?		
Contención:	Aislar las máquinas infectadas (es decir, desactivar los enlaces de red al centro de datos); Apagar los sistemas no infectados ya sea en forma remota o, si parece posible, hacer que los usuarios apaguen sus sistemas.		

Recuperación:	Los sistemas infectados deben ser considerados como perdidos y deberán ser reinstalados. Posiblemente algunos empleados pueden estar fuera de línea durante unos pocos días.
Retiro:	El equipo de crisis asigna un equipo para: 1. Identificar el ransomware y verificar firmas u otros métodos de detección; 2. Identificar la tensión inicial... ¿de qué manera se infectó el paciente cero? 3. Crear entornos de red aislados (conectados por cable o inalámbricos) donde la infección tuvo lugar; los sistemas no infectados deberían iniciarse y ser verificados para observar si realmente no fueron infectados por el malware; 4. Crear un plan para reinstalar los equipos portátiles infectados. Para las oficinas remotas, esto puede ser un problema y puede ser necesario enviar un ingeniero al sitio. 5. Presentar una demanda formal ante las autoridades de aplicación de la ley u otras autoridades según las recomendaciones/obligaciones legales.
Comunicación:	<u>Comunicación interna únicamente</u> Informar a todos los empleados del ataque de ransomware e instruirlos a que inmediatamente apaguen los equipos portátiles (Windows) (usar correo electrónico, teléfono o mensajería).
Materiales vitales:	Documentación de la infraestructura y configuración. Almacenes de contraseñas para tener acceso a los diferentes sistemas. Listas de distribución de comunicaciones (empleados).
Registros:	Crear un registro del incidente, qué se descubrió, qué acciones se realizaron, qué evidencia se recopiló. Realizar estas acciones durante el manejo de la crisis y **no** con posterioridad.

Anexo: El taller

Cronograma del taller

	Descripción	Plazo en min.	Quién
1	Presentación del manual - Distribuir el documento Plan de DR/BCP	45	
2	Preguntas y respuestas sobre el manual	15	
3	Completar los formularios - BIA - BCP - en función de su propio ccTLD - Distribuir la plantilla de DR/BCP	45	
4	Analizar el resultado del formulario	30	
5	Armar los equipos (máximo de 5 equipos) - Distribuir tarjetas, Registro de OK y Plan de BCP de Hacking cibernético	5	
6	Familiarizarse con las tarjetas	10	
7	5 rondas de ejercicio de simulación real (TTX)	60	
8	Resumen del ejercicio	30	

(240 minutos)

Ejercicio de presentación y relleno de formularios

Realizar una presentación de 45 minutos + sesión de preguntas y respuestas de 15 minutos sobre el documento para señalar los temas principales.

Durante 45 minutos, permitimos a los participantes

1. realizar una lista de partes interesadas y redactar sus expectativas
2. Revisar el registro de amenazas - ¿cuáles son aplicables?
3. Cuáles son los riesgos importantes para la organización e identificar los niveles.
4. Seleccionar una amenaza y llevar a cabo una Evaluación del Impacto en Operaciones (BIA) sobre ella.
5. En función de dicha amenaza, definir un Plan de Continuidad de Operaciones (BCP); enumerar los elementos de los Materiales vitales

Lista de partes interesadas

Las partes interesadas incluidas en esta lista son solo ejemplos. No dude en agregar partes interesadas que no han sido mencionadas y que considera relevantes. Relevancia para BC: ALTA, MEDIA, BAJA, n/a

Parte Interesada	**Expectativas**	**Relevancia para BC**
Gobierno	_____ _____ _____	_____ _____ _____
ICANN	_____ _____ _____	_____ _____ _____
Junta Directiva	_____ _____ _____	_____ _____ _____
Público en general	_____ _____ _____	_____ _____ _____
Aplicación de la ley	_____ _____ _____	_____ _____ _____
Registradores	_____ _____ _____	_____ _____ _____
Registratarios	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____

Registro de amenazas

Verificar cuáles son las amenazas aplicables y cuál es la probabilidad en función de información estadística.

Categoría de amenaza	Amenaza	Aplicable (Sí/No)	Probabilidad
Desastres naturales	Incendio Inundación Huracán/tornado/tifón Clima adverso Terremoto Derrumbe/avalancha Actividad volcánica Tsunami Relámpagos Hundimiento Contaminación Infestación de insectos Roedores _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
RR. HH y Medicina	Pérdida de personal clave Enfermedad epidémica Escasez de aptitudes/personal Cuestiones familiares Robo Daño malicioso (sabotaje) Extorsión _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Cibernética	DDOS Piratas informáticos Pérdida de datos Ransomware Actividades relacionadas con guerra cibernética _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Externa	Recesión Desobediencia civil Actividad terrorista Guerra/invasión Interferencia política/cambios en políticas Hurto Cambios tecnológicos/relevancia _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Asuntos financieros	Problemas de flujo monetario/liquidez Falta de capital Malversación financiera Deuda incobrable Riesgo de intereses Riesgo de tipo de cambio Exposición de fondos públicos _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Tecnología e infraestructura	Falla de red – global Electricidad – fallas de cuadrícula Fallas de CA Fallas de centros de datos Fallas de componentes[5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Falla de suministro	Falla a nivel de servicio Defectos de calidad Pérdida de servicios suministrados Tercerización fallida/situaciones de falta de stock de contrato de suministros Pérdida de otros activos vitales Dependencia del proveedor _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Probabilidad:

1. Muy probable: un evento recurrente de manera anual o con más frecuencia
2. Probable: un evento que sucede cada tres años promedio
3. Ocasional: un evento que sucede cada diez años
4. Poco probable: un evento que sucede una vez cada 50 años o más
5. OoS: Fuera de alcance (OoS, *Out of Scope*) – estos no son considerados en la continuidad de operaciones

[5] Las fallas de componentes es un marco genérico para hacer referencia al mal funcionamiento de sistemas informáticos, fuentes de alimentación, memoria de computadoras, discos, etc... uno puede decidir incluir esto dentro del alcance de la continuidad de operaciones o suponer que está mitigado en el diseño y arquitectura de la infraestructura de manera predeterminada (por ejemplo, fuentes de alimentación redundantes, sistemas de discos RAID, memoria ECC en servidores, etc...).

Matriz de riesgos

Tipo	NULO o n/a	Bajo	Medio	Alto	Crítico
Asuntos financieros	el riesgo no existe o no es aplicable				
Operativo					
Reputación					
Legal					
Gobernanza[6]					
Humano					

[6] Los riesgos de gobernanza son posiblemente los tipos de riesgos más difíciles y, al mismo tiempo, los más específicos. Para algunos registros, el riesgo puede incluso no existir. Esto requiere gestión para definir y describir claramente la forma en que el registro depende de las influencias externas.

Evaluación del impacto en operaciones

Tomar una de las amenazas definidas en el registro de amenazas que tenga un claro impacto en la continuidad de operaciones y evaluar el impacto en los diferentes riesgos basándose en la matriz de riesgos. La probabilidad se repite del registro de amenazas.

Probabilidad:

1. Muy probable: un evento recurrente de manera anual o con más frecuencia
2. Probable: un evento que sucede cada tres años promedio
3. Ocasional: un evento que sucede cada diez años
4. Poco probable: un evento que sucede una vez cada 50 años o más
5. OoS: Fuera de alcance (OoS, *Out of Scope*) – estos no son considerados en la continuidad de operaciones

El RTO (Objetivo de Tiempo de Recuperación o cuán rápido el negocio debe volver a funcionar después de la interrupción) y el RPO (qué cantidad de pérdida de datos podemos aceptar) son definidos por el negocio (esto puede ser un requisito contractual, legal o de gobernanza); no debería considerarse qué es técnicamente posible o imposible.

Categoría de amenaza	**Amenaza**	**Aplicable (Sí/No)**	**Probabilidad**
		Sí	
Riesgos	**Nivel**	**Motivación/descripción/explicación**	
Asuntos financieros			
Operativo			
Reputación			
Legal			

Gobernanza		
Humano		
RTO		
RPO		
Mitigación de riesgos	“n/a” o describir planes para mitigar el riesgo	
Aceptar el riesgo		
Evitar el riesgo		
Reducir el riesgo		
Contener el riesgo		
Transferir el riesgo		

Plan de continuidad de operaciones

PLAN DE CONTINUIDAD DE OPERACIONES (PLANTILLA)			
Referencia:	[REFERENCIA]	Tipo de amenaza	Activos afectados
Escenario:	*Describe las condiciones que activaron el Plan. Esto puede ser un evento, un plazo, una condición específica, etc.*		
ACTIVACIÓN:	*¿Cuándo se activa el plan? Se puede activar inmediatamente al momento de la detección o varias horas después de que el incidente tuvo lugar.*		
RTO:	*Objetivo de Tiempo de Recuperación*		
RPO:	*Objetivo de Punto de Recuperación*		
Equipo de crisis:	*¿Quién es el equipo de crisis? ¿Quién realmente se encargará del incidente? Usar nombres de empleados, socios, proveedores para evitar ambigüedades.*		
Prioridades:	*¿Cuáles son las prioridades? Esto debería ser interpretado como una lista secuencial.*		
Evaluación:	*La etapa inicial de manejar un incidente disruptivo es evaluar el grado del incidente. Describir los factores que deberían tenerse en cuenta.*		
Contención:	*Describir el curso de acción para prevenir un empeoramiento de la situación.*		
Recuperación:	*Describir el curso de acción para restaurar la preparación operativa mínima, considerando las prioridades definidas anteriormente.*		
Retiro:	*Una vez recuperadas las operaciones, el equipo de crisis se retira y deja instrucciones para llevar adelante posteriores acciones para volver a la situación anterior al incidente.*		

Comunicación:	*Definir las comunicaciones internas y externas, incluidos el mensaje y la lista de distribución, así como los medios. Siempre comenzar con la comunicación interna.*
Materiales vitales:	*Lista de recursos necesarios para gestionar el incidente. Esto es parte de la etapa de preparación. El plan no incluye el contenido real, sino que está limitado a referencias (es responsabilidad de los jefes de los diferentes departamentos o socios conservar este contenido, mantenerlo actualizado, y preciso y portable cuando sea posible)*
Registros:	*Los registros que deben elaborarse durante y después de la crisis. Estos registros son útiles para la recopilación de evidencia, lecciones aprendidas y un seguimiento del incidente real.*

Plan de continuidad de operaciones

PLAN DE CONTINUIDAD DE OPERACIONES (PLANTILLA)			
Referencia:	[REFERENCIA]	Tipo de amenaza	Activos afectados
Escenario:			
ACTIVACIÓN:			
RTO:			
RPO:			
Equipo de crisis:			
Prioridades:			
Evaluación:			
Contención:			
Recuperación:			
Retiro:			

Comunicación:	
Materiales vitales:	
Registros:	

Descripción de ejercicio de simulación (TTX)

El ejercicio está totalmente guionado y consiste en 5 rondas de 10 minutos cada una. Al comienzo de cada ronda, el equipo recibe aportes y debe reaccionar respecto de los aportes brindados usando el Plan de Continuidad de Operaciones adecuado.

Para facilitar esto, se distribuye un conjunto de tarjetas entre cada equipo. Estas tarjetas contienen acciones prácticas que se ejecutan como reacción a los aportes recibidos al comienzo de la ronda.

El participante puede seleccionar hasta 3 acciones (tarjetas) por ronda que se reservan para analizarlas más tarde. Las tarjetas se agrupan en 4 categorías: ASUNTOS TÉCNICOS; ASUNTOS LEGALES; GOBERNANZA; COMUNICACIÓN, las cuales representan básicamente al departamento técnico, departamento de asuntos legales, gerencia general y departamento de comunicaciones.

Durante una ronda, se puede agregar información adicional al ejercicio; dicha información debería ser procesada por el equipo y puede conducir a un cambio de acción.

Después de las 5 rondas, las tarjetas se recopilan y analizan en función de diversos temas para recolectar comentarios del participante.

Descripción del registro

Usted está empleado en el "**Registro de OK**", el operador de registro para el ccTLD .ok. OK, también conocido como Old Kontry, es un pequeño país europeo con aproximadamente 50 000 habitantes. Debido a sus políticas liberales, el dominio de alto nivel .ok es bastante popular y tiene 372 304 nombres de dominio registrados al 1 de noviembre de 2019. Los nombres de dominio .ok se venden mediante una red mundial de aproximadamente 250 registradores.

Old Kontry es una monarquía constitucional parlamentaria y unitaria.

Old Kontry no forma parte de la Unión Europea.

El registro está ubicado en la capital y forma parte de la "**Universidad de OK**", pero es operado independientemente (administración, asuntos financieros y técnico); no obstante, la universidad es la autoridad supervisora.

Para sus servicios backend, utiliza MegaRyCorp. Inc., un proveedor de servicios de registro de DE especializado en servicios backend para registros. 1 proveedor anycast de EE. UU. está a cargo de los servicios de DNS, pero el registro tiene 3 servidores de nombres unicast más antiguos que se ejecutan desde la red universitaria.

Para su presencia web (sitio web corporativo, redes sociales, etc.), el registro depende mucho de su agencia creativa, de datos y tecnología local, parte de un grupo internacional.

Además del servidor de nombre maestro oculto y los servidores de nombres autoritativos, el registro ejecuta un servidor EPP, un servidor de WHOIS y una extranet de registrador que tiene las mismas características que el EPP, entre otros.

Debido a su popularidad e importancia para la economía global, el gobierno de OK ha adoptado legislación durante los últimos años que está en consonancia con el GDPR europeo sobre protección de datos personales y la directiva de NIS sobre la protección de infraestructura crítica y operadores de servicios esenciales. Asimismo, asignó al Ministerio de Telecomunicaciones como la autoridad de supervisión de políticas y cumplimiento.

El "**registro de OK**" es una pequeña organización en la que trabajan 7 personas directamente para el registro. Puede depender de apoyo de TI para equipos portátiles/equipos de escritorio/correo electrónico/etc. de la universidad.

Emplea a 3 ingenieros (1 desarrollador, 2 administradores de sistemas, 1 ingeniero en redes) que se encargan del portal web del registrador, supervisión, servidores de nombres legados, firewalls, (W)LAN, apoyo para los registradores y presentación de informes técnicos.

Hay un Gerente General, un Gerente de Ventas y Marketing, un Gerente de Finanzas y un Gerente de Asuntos Legales; el equipo técnico está bajo las órdenes directas del Gerente General. La administración de la continuidad de operaciones recae en la responsabilidad del Gerente de Asuntos Legales.

Plan de BCP para asuntos cibernéticos: HACKING

PLAN DE CONTINUIDAD DE OPERACIONES			
Referencia:	BCP-101.01	CIBERNÉTICA: HACKING	Global
Escenario:	La evidencia muestra que la infraestructura del registro fue hackeada y comprometida. Un actor desconocido ha instalado software, creado cuentas, herramientas de acceso remoto, etc., para infiltrarse en el registro. Posiblemente, se robaron datos (sensibles).		
ACTIVACIÓN:	INMEDIATAMENTE AL MOMENTO DE LA DETECCIÓN		
RTO:	24 hs.		
RPO:	Pérdida de datos de 24 hs.		
Equipo de crisis:	Gerente de Asuntos Legales - +CC 123 55 88 - ivan.horvat@registry.tld Gerente de Tecnología – +CC 123 44 55 – juan.perez@registry.tld Gerente de BC – +CC 123 33 66 – jane.doe@registry.tld Gerente General - +CC 123 56 44 - yamado.toro@registry.tld		
Prioridades:	Proteger la disponibilidad e integridad de los servidores de nombres y la zona .ok. Si es necesario, aislar la infraestructura de servidores de nombres. Aislar los sistemas hackeados. Recolectar evidencia.		
Evaluación:	Evaluar y realizar un inventario de los sistemas afectados. ¿Qué servicios se ven afectados? ¿Se vieron afectados el DNS, la plataforma de registración, los servicios internos, el sitio web? Volver a revisar la infraestructura y el servicio de servidores de nombres. ¿El hacker tiene un punto de apoyo permanente? ¿El hacker está presente al momento de la detección? ¿Se necesita ayuda externa de una compañía especializada en incidentes cibernéticos (hay evidencia de actores estatales)? ¿Se han filtrado datos? De ser así, ¿qué tipo de datos se filtraron? ¿Cuál es el impacto de los datos filtrados?		

Contención:	Asegurarse de que la infraestructura de servidores de nombres esté protegida y aislar los servidores de nombres del área afectada. Desactivar o apagar los sistemas afectados. No intentar reparar o corregir los sistemas afectados o combatir al intruso. Concentrarse en aislar los sistemas afectados. Intentar recopilar evidencia; no alterar la evidencia
Recuperación:	Los sistemas afectados deberían reconstruirse y reimplementarse. Si el equipo del usuario final se ve afectado, se implementan sistemas nuevos.
Retiro:	Una vez que los sistemas afectados han sido aislados y desactivados y los servicios restaurados mediante sistemas de reconstrucción y reimplementación, el equipo de crisis asigna un equipo para manejar las actividades siguientes: 1. Contactarse con los agentes de aplicación de la ley y presentar una denuncia. 2. Asegurarse de que los sistemas afectados se almacenen de manera segura y los archivos de registro se separen como evidencia. Analizar la integridad de la base de datos central (¿hay rastros de cambios?).
Comunicación:	**Comunicación interna:** La comunicación a todos de que nuestros sistemas han sido afectados y que estamos aislando dichos sistemas. Remarcar que la posterior comunicación al mundo exterior será manejada por el Gerente de Ventas y Marketing o el Gerente de Asuntos Legales directamente. **Comunicación externa:** Informar a las partes interesadas (junta, autoridades de la universidad) Informar a los registradores si los sistemas se desactivarán (por ejemplo, sitio web WHOIS, EPP) e informarles de los futuros pasos que se tomarán. Informar a los agentes de aplicación de la ley. Publicar de manera periódica el progreso en cuentas de redes sociales y el sitio web público.
Materiales vitales:	Documentación de la infraestructura y configuración. Almacenes de contraseñas para tener acceso a los diferentes sistemas. Implementación y preparación de infraestructura para implementar nueva infraestructura. Listas de distribución de comunicaciones (registradores, empleados, partes interesadas)

Registros:	Crear un registro del incidente, qué se descubrió, qué acciones se realizaron, qué evidencia se recopiló. Realizar estas acciones durante el manejo de la crisis y no con posterioridad.

Escenario del ejercicio

RONDA 1: aportes viernes, 05:00 PM

- un investigador de seguridad se pone en contacto con el gerente general del operador de registro para comentarle que descubrió pruebas sobre pastebin de un extracto de una base de datos que parecen señalar a la extranet del registro usada por sus registradores.
- el investigador verificó las contraseñas con hash en pastebin y logró con facilidad “averiguar” algunas de ellas. Como es de esperarse, “contraseña123” es muy común. Él confirma que inició sesión en la extranet del registrador en algunas horas específicas (le brinda esas horas al gerente).
- El pastebin aún está en línea y el investigador también descubrió algunas pruebas de que alguien está vendiendo las credenciales en la Internet profunda.
- Él cree que hay prueba suficiente para suponer que alguien ha hackeado el registro y que el delincuente ha comenzado a sacar provecho de su trabajo.

Esta es la información inicial que recibió el registro. ¿Cómo reaccionará el gerente? ¿Qué hará? A partir de aquí, el gerente debe recibir información adicional según su curso de acción. Recuerde controlar el reloj. Los participantes solo tienen 15 minutos por ronda.

ELEGIR 3 CARTAS

RONDA 2: aportes viernes, 08:00 PM

- Han transcurrido 3 horas desde el descubrimiento inicial
- alguien tuitea el enlace a otro pastebin con el hashtag #DominiosLibresParaTodos#largaVida.OK; es una copia del pastebin original.
- el tuit es recogido y retuiteado; el hashtag es modificado con #Funciona.

ELEGIR 3 CARTAS

RONDA 3: aportes viernes, 10:00 PM

- Han transcurrido 2 horas
- la prensa se comunica con el operador de registro; desea saber qué sucede y solicita una declaración formal.
- el administrador del operador de registro recibe una llamada telefónica de la televisión nacional.
- los ingenieros aún están analizando el problema, pero no han descubierto aún de dónde provino la filtración.

ELEGIR 3 CARTAS

RONDA EXTRA: aportes (3 minutos antes de finalizar la ronda)

Para hacer que el ejercicio sea más interesante, se puede agregar más información. En la vida real, los eventos no siguen un patrón previsible, no durante una crisis. Las rondas extra solo brindan información adicional que debe ser analizada y respecto de la cual se debe actuar antes de finalizar la ronda.

- los ingenieros tienen noticias buenas y algunas realmente malas.
- han descubierto por dónde habían ingresado al sistema los hackers y qué había cambiado.
- también notaron que más de 50 000 nombres de dominio adicionales habían sido registrados y un número indefinido de nombres de dominio existentes habían sido alterados; algunos de ellos son nombres de dominio de alto perfil.
- sugieren revertir el DNS y llegar a los principales proveedores de servicios de Internet para volver a cargar sus resolutores

ACTUALIZAR 3 CARTAS

RONDA 4: aportes SÁBADO, 06:00 AM

- Han transcurrido 8 horas
- El CERT nacional se comunica con el operador de registro; ha recibido algo de inteligencia sobre el origen del ataque
- las redes sociales del operador de registro son bombardeadas con preguntas por registradores y titulares de nombres de dominio preocupados
- las casillas de correo genéricas han explotado con más de 5000 correos electrónicos recibidos
- los medios se ponen en contacto nuevamente con el operador de registro para recibir información actualizada y preguntar por qué se demora tanto tiempo en corregir el problema
- el ministerio supervisor pertinente (por ejemplo, telecomunicaciones) se pone en contacto con el gerente general del operador de registro; desea información actualizada sobre el estado y un resumen del impacto del incidente

ELEGIR 3 CARTAS

RONDA 5: cierre DOMINGO, 09:00 AM

- Han transcurrido 21 horas
- los ingenieros han revertido la base de datos al jueves 11:47 PM., que es el respaldo más reciente sin evidencia de los nombres de dominio modificados
- se han vuelto a cargar los servidores de nombres
- se corrigió la vulnerabilidad, explotada por los hackers
- se han restablecido todas las credenciales de los registradores
- apoyo recibió una lista de los nombres de dominio, registradores y registratarios que fueron afectados
- hay trabajos pendientes atrasados en apoyo con más de 10 000 correos electrónicos en los tickets de apoyo e innumerables tuits que muestran enojo
- varios bloggers y vloggers se han percatado del problema y han publicado sus opiniones

ELEGIR 3 CARTAS

FIN DEL EJERCICIO - PAUSA

El participante necesitará un descanso

RESUMEN

Cada equipo presenta sus tarjetas.

Para un ejercicio eficaz y eficiente, es importante resumir correctamente y debatir las acciones del equipo. Por lo tanto, el resultado del equipo de crisis deber ser capturado por escrito o en grabaciones. El resumen debería centrarse en varios temas:

1. ¿cuál es la reacción general respecto del ejercicio?
2. ¿cuán bien se siguió el plan de continuidad de operaciones?
3. ¿en qué momento el equipo comenzó a improvisar?
4. ¿se sintió cómodo y a la altura de la tarea?
5. ¿qué aprendió?
6. ¿qué mejoras se necesitan?

Tarjetas

Imprimir estas tarjetas en tamaño de tarjetas comerciales, eventualmente usar diferentes colores por categoría.

	TÉCNICO	ADMINISTRACIÓN DE ASUNTOS LEGALES / BC	COMUNICACIONES	GOBERNANZA / ADMINISTRACIÓN
1	Apagar los servidores de nombres autoritativos	Llamar a los agentes de aplicación de la ley	Publicar información actualizada del estado en redes sociales	Declarar una situación de desastre
2	Contactarse con el operador de servicios de registro e informarle el problema	Recomendar a la administración sobre la estrategia de comunicaciones	Publicar un mensaje en redes sociales	Reunir al equipo de crisis
3	Contactarse con el operador de servicios de registro e informarle el problema	Contactarse con un compañía de repuesta ante incidentes externa para recibir ayuda para tratar el problema	Responder a la prensa	Abrir el Plan de Continuidad de Operaciones
4	Desactivar la plataforma de registración	Asesorar para minimizar la comunicación	Preparar la comunicación sobre la reversión	Contactarse con la junta/autoridad supervisora
5	Comenzar a analizar los archivos de registro disponibles	Recomendar total transparencia a la administración	Escribir comunicados de prensa	Informar a los organismos supervisores gubernamentales
6	Restaurar la base de datos principal	Ponerse en contacto con los proveedores de telecomunicaciones locales para que reinicien sus resolutores	Escribir plantillas para la comunicación de la crisis	Comunicarse con el CERT del país e informar el incidente
7	Reinstalar los sistemas afectados	Comunicar los hallazgos a los agentes de aplicación de la ley	Enviar declaraciones de prensa sobre el impacto	Dar una conferencia de prensa

8	Evaluación técnica y recopilar evidencia de los sistemas hackeados	Contactarse con los registradores para cambiar las contraseñas	No realizar comunicaciones en canales públicos hasta que no lo confirme el gerente general y de asuntos legales	Brindar información actualizada sobre el estado a los organismos supervisores gubernamentales
9	Comenzar a responder tickets u otras solicitudes recibidas por medio de la dirección de correo electrónico de asistencia	Informar al Comité Europeo de Protección de Datos sobre el problema	Enviar información actualizada sobre el estado de manera interna	Declarar el fin de la crisis y retiro - vuelta a las operaciones habituales
10	Crear una lista de nombres de dominio modificados para identificar a las víctimas	Presentar el incidente ante los agentes de aplicación de la ley	Contratar un vocero de comunicaciones de crisis	Solicitar asistencia del CERT nacional
11	Crear una lista de nombres de dominio agregados	Informar a la compañía de seguros	Negar la filtración	Informar a la ICANN
12	Bloquear el acceso al sistema de registración	Informar a los registratarios afectados	Enviar un correo electrónico a TLD-OPS para asistencia	Contactar a la línea de emergencia 24/7 de la IANA
13	Cambiar las contraseñas	Informar a otros registros mediante la lista de correo electrónico de TLD-OPS		Culpar a TLD-OPS :-)
14	Descargar la lista de contraseñas del pastebin	Solicitar asistencia de otros registros mediante la lista de correo electrónico de TLD-OPS		
15	Instalar un SIEM			

El mazo de tarjetas está disponible para descarga en el sitio web de TLD-OPS en formato Adobe Indesign, listo para ser enviado a la imprenta.

SUGERENCIAS Y TRUCOS DEL TALLER

En esta sección, se incluyen sugerencias y trucos para el ejercicio de DR/BCP; envíe un correo electrónico a TLD-OPS si tiene alguna opinión nueva sobre cómo mejorar el TTX.

- La identificación de partes interesadas, amenazas y riesgos no es un trabajo para una sola persona. Siga manifestando esto.
- Algunas amenazas son “aterradoras”; ese es el motivo principal para documentarla y tener un plan para combatirla.
- Haga que el ejercicio individual también identifique qué funciones/grupos/personas dentro de cada TLD realmente actúa como Gerente de BCP; identifique sus partes interesadas reales
- Algunos pueden lidiar con impactos financieros – haciendo que las personas comerciales ayuden con esto; la continuidad de operaciones es un ejercicio colectivo
- Aclare dentro de su organización quién cumple el rol de Gerente de BCP, ¿es el gerente de Asuntos Legales, Finanzas, PMO, Director de Tecnologías de la Información, CSO, Director Ejecutivo, Director de Operaciones?
- Quizá puede comenzar el juego entregando las 3 cartas siguientes a cada equipo