Gestión de la continuidad del Negocio

Inicio

Sílabo del curso

Revisamos el sílabo

Universidad Tecnológica del Perú

Logro de aprendizaje

Los estudiantes aprenden el proceso de implementación de un sistema de gestión de la continuidad del negocio, permitiéndoles tener una visión integral de la aplicación de las mejores prácticas utilizadas por las organizaciones.

Universidad Tecnológica del Perú

¿Están las empresas preparadas para afrontar y superar una crisis?

Corte de suministros

Inundaciones

Terremotos / Sismos

Incendios

Huracán / Tornado

Epidemias

Hackers

Sabotaje Terrorismo

Guerra / desorden civil

Usuarios descuidados

Espías

Usuarios malintencionados

Pérdida de Activos

Continuidad de negocio

- La capacidad de la organización para continuar realizando la entrega de productos o servicios a niveles predefinidos aceptables después de un incidente disruptivo.
- Los planes de continuidad de negocio establecen procesos y procedimientos de gestión de riesgos que tienen como objetivo evitar interrupciones en los servicios y procesos más esenciales para restablecer la función completa de la empresa u organización de la forma más rápida y sencilla posible.

https://drii.org/resources/locallaninfo/espanol

¿En qué consiste la continuidad de negocio?

La continuidad de negocio implica un conjunto de procesos que forman la estrategia de una empresa contra la interrupción de la actividad empresarial.

La minimización del riesgo de interrupción después de un evento disruptivo/desastre es directamente proporcional al nivel de su continuidad empresarial.

DRI (Disaster Recovery Institute) Internacional proporciona los estándares y mejores prácticas en la Gestión de la Continuidad de Negocio.

Fue fundada en 1988 en **USA** como una organización **sin fines de lucro** con la misión de preparar al mundo ante situaciones de contingencia. Hay más de **12.000 profesionales** certificados activos en todo el mundo. Tienen presencia en **100 países** y lleva a cabo la capacitación en más de 50 de estos países. Trabaja con numerosos gobiernos y organizaciones en la creación de normas nacionales e internacionales de Continuidad de Negocio, así como, con líderes del sector privado y asociaciones profesionales para promover la Continuidad de Negocio.

SI es certificable para los profesionales.

https://drii.org

- Es la capacidad de una organización de continuar entregando productos y servicios a niveles aceptables pre-definidos, después de un incidente disruptivo (que produce ruptura brusca).

  - Es un conjunto de procedimientos que le permiten a las organizaciones preservar la continuidad operativa de sus **procesos críticos** en caso de presentarse alguna situación de contingencia.

- Conjunto de procedimientos que se accionan para salvaguardar los activos de la empresa y permitir su subsistencia frente a eventos contingentes.

BCI (Business Continuity Institute) Internacional proporciona los estándares y mejores prácticas en la Gestión de la Continuidad de Negocio.

Fue fundada en 1994 en **Inglaterra** como una organización **sin fines de lucro** con la misión de promover un mundo más resiliente. Hay más de
8.000 profesionales certificados activos en todo el mundo. Tienen presencia en **100 países**. Trabaja con más de 3.000 organizaciones en la creación de normas nacionales e internacionales de Continuidad de Negocio, así como, con líderes del sector privado y asociaciones profesionales para promover la Continuidad de Negocio.

- Es un conjunto de procedimientos que le permiten a las organizaciones preservar la continuidad del entorno **Tecnológico** que soporta los procesos críticos de la empresa, en caso de presentarse alguna situación de contingencia.

- Es un conjunto de procedimientos que le permiten a las organizaciones preservar la continuidad de los **sistemas críticos** (TI) que soportan los **procesos críticos** de una empresa en caso de presentarse alguna situación de contingencia.

CONTINUIDAD DEL NEGOCIO

- *Business Continuity Management (BCM).*
- Capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades comerciales en un nivel aceptable previamente definido. (BCI GROUP, 2007)
- Proceso de gestión holístico que identifica las amenazas potenciales de una organización y los impactos que pueden causar en las operaciones del negocio si esas amenazas se materializan.
- "Proporciona un marco de trabajo para construir una organización más resistente con capacidad para responder de forma efectiva y proteger los intereses de las partes interesadas clave, su reputación, imagen de marca y actividades de valor añadido". (BUREAU VERITAS, 2012)

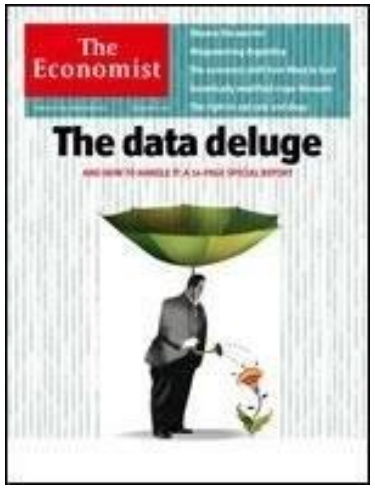
https://www.crisis-response.com/Articles/685591/The_British_Library.aspx

Al igual que otras normas ISO, la 22301 es un estándar desarrollado por ISO (International Organization for Standarization) e IEC (International Electrotechnical Commission), que proporciona un Sistema de Gestión de la Continuidad del Negocio y Seguridad de las Sociedades, utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La norma se crea en el 2012 en su primera versión, utilizando el anexo SL, el cual, fue creado para estandarizar todas las normas utilizando la estructura definida en dicho anexo para su creación o actualización.

SI es certificable para los profesionales y empresas

Reseñas Históricas



Durante los **10 últimos** años ha habido un incremento de eventos contingentes a nivel mundial, entre los que podemos mencionar como los más importantes:

- Terremotos ocurridos en todas partes del mundo, siendo los de mayor escala los ocurridos en Haití, Chile, Japón y Nepal.
- Tsunamis ocurrido en Indonesia y en Japón que afectó a muchas localidades.
- Huracanes, siendo el de Katrina y Sandy los más destructivos.
- Atentados terroristas cometidos contra las Torres Gemelas en USA, estación de trenes de Atocha en España, Editorial en Francia, Maratón de Boston, entre otros.
- Incendios como el ocurrido en la Torre Windsor en España.
- Erupciones volcánicas. Lluvia de cenizas.
- Inundaciones en todo el mundo, siendo este el evento que más se repite en el mundo causado por la naturaleza.
- Temporadas de sequías en varios países.
- Pandemias (Ebola – H1N1)

- **Salvaguardar la vida de los empleados.**
- Asegurar la continuidad de los sistemas y procesos críticos.
- Proporcionar protección a los activos de la empresa incluyendo la infraestructura de TI.
- Mitigar los riesgos y exposiciones a escenarios contingentes.
- Planificar la recuperación en caso de una contingencia.
- Reducir las pérdidas de datos, ingresos y clientes.
- Reducir la confusión y permitir decisiones efectivas en tiempos de crisis, tomando el control ante cualquier interrupción.

- Capacidad de adaptación de una organización en un entorno complejo y cambiante.

- Capacidad que tiene una persona o un grupo de recuperarse frente a la adversidad para continuar proyectándose hacia el futuro.

- Capacidad para afrontar eventos contingentes y lograr resistir, sobrevivir y adaptarse, permitiendo volver a la normalidad una vez que estos pasen.

- Cualquier actividad o función esencial sin la cual, la
  - organización no puede entregar sus producto y/o servicios.

  - Actividades que son las mínimas necesarias para poder operar en una situación de contingencia.
  - Conjunto de actividades indispensables de una empresa que permiten a las organizaciones subsistir en situaciones de contingencia.

Cualquier objeto, servicio o activo que sea necesario utilizar durante una situación de contingencia para poder operar.

Algunos ejemplos de recursos críticos:

- Personas
- Sellos húmedos, papel membretado, etc.
- Laptops, impresoras, teléfonos.
- Proveedores
- Red VPN, Internet, Aplicativos Core.

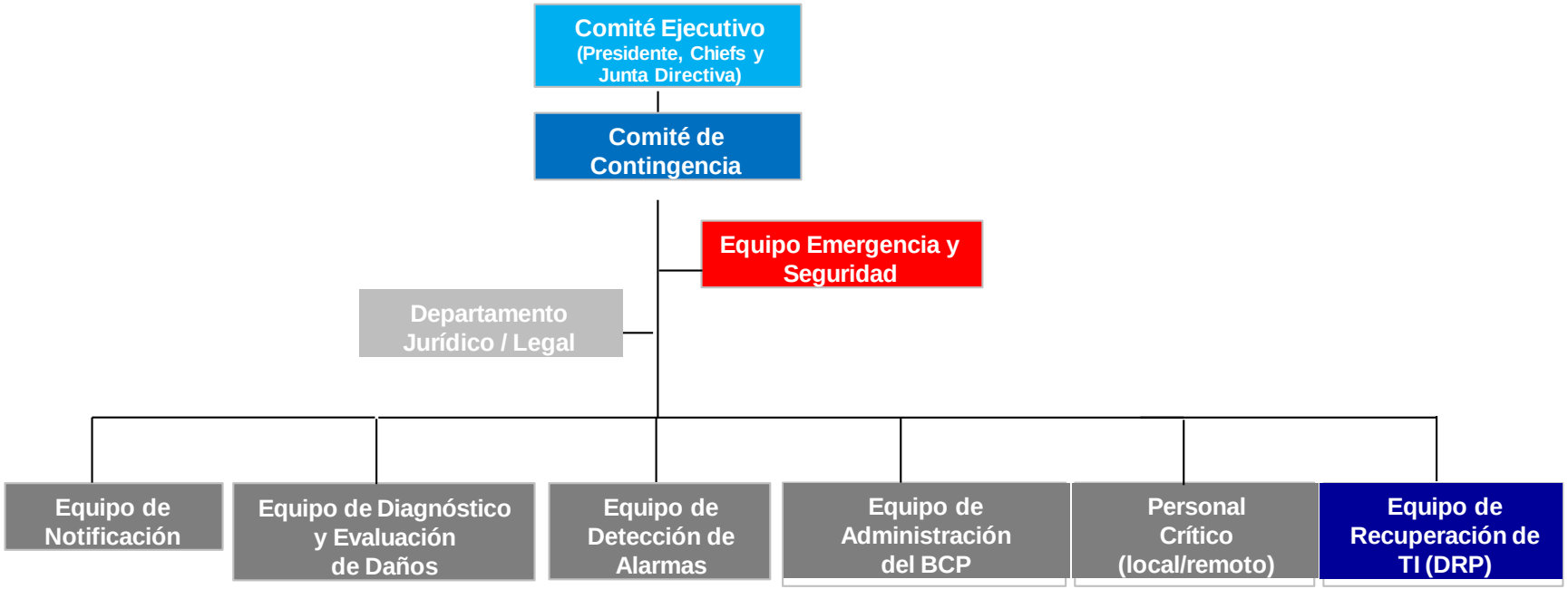
Cualquier documento físico o digital que sea necesario utilizar durante una situación de contingencia para poder operar.

Algunos ejemplos de registros vitales:

- Mapas, planos de planta física, etc.
- Originales de Facturas, contratos, registros de clientes.
- Archivos digitales con información crítica (Excel, Word, ppt, etc.)
- Documentos escaneados, certificados, permisos.
- Información respaldada en lugares de almacenamiento compartido.

RTO (Recovery Time Objective)
Periodo de tiempo dentro del cual los niveles mínimos de servicios, sistemas de soporte, aplicaciones o funciones deben de ser recuperados después de que ha ocurrido una disrupción.

RPO (Recovery Point Objective)
Punto en el tiempo en el cual los datos deben ser recuperados después de que una disrupción ha ocurrido. ¿Cuánta información estoy dispuesto a perder?


Comité Ejecutivo
(Presidente, Chiefs y Junta Directiva)
Comité de Contingencia
Equipo Emergencia y Seguridad
Departamento Jurídico / Legal
Equipo de Notificación
Equipo de Diagnóstico y Evaluación de Daños
Equipo de Detección de Alarmas
Equipo de Administración del BCP
Personal Crítico (local/remoto)
Equipo de Recuperación de TI (DRP)

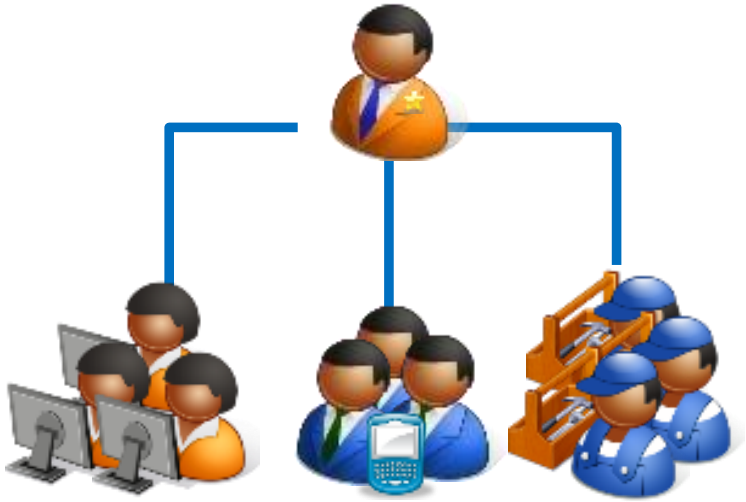
- Ubicación física alternativa, diferente a la principal, en donde se va a establecer la estrategia de recuperación de una empresa, pudiendo ser un Centro Alterno para TI y/o de Operación.

- Punto de reunión del Comité de Contingencia o Comité de Manejo de Crisis que es el grupo Líder del manejo de las contingencias. Estará ubicado en un lugar distinto al Centro de Operación principal siguiendo prácticas y estándares de distribución de personal en situaciones de contingencia.

- Oficinas y espacios de trabajo para el personal crítico y los equipos de contingencia que serán habilitados en situaciones de contingencia de la empresa.

Los Comités, Equipos de Contingencia y personal crítico serán los encargados de la operación de la empresa en una situación de Contingencia y operarán en muchos casos desde los Centros Alternos.

Tomando en cuenta la estructura organizacional, principales localidades de operación y de líneas de negocio, así como, las características de la plataforma tecnológica, se deberán identificar los comités, equipos o grupos de trabajo que interactuarían en las diferentes fases de una contingencia.



Existen diferentes tipos de Centros Alternos o sedes de recuperación, según el tipo de estrategia a implementar y el alcance definido por la empresa dentro de la planificación de la continuidad.

Algunos de estos sitios son:

- ✓ Centro Alterno de Operación
- ✓ **Centro Alterno de Procesamiento o de TI (DATA CENTER ALTERNO)**
- ✓ Emergency Operation Center / War Room
- ✓ Work space areas
- ✓ Remote Work

Se define como el Centro de Operación Alterno en donde se ejecutará la operación de la empresa durante la situación de contingencia, que inhabilite la operación en su sede principal. Son oficinas de trabajo equipadas para operar una empresa, con lo mínimo necesario en una situación de contingencia.

Se define como el Centro de Procesamiento Alterno Tecnológico en donde se encontrará una replica de los aplicativos y servicios de TI más críticos para la empresa, a ser utilizados en caso de una contingencia.

¿Qué son las Work Space Area?

Es un área de trabajo alterna equipadas para el personal crítico identificado por la empresa, en donde laboraran de forma presencial durante una situación de Contingencia.

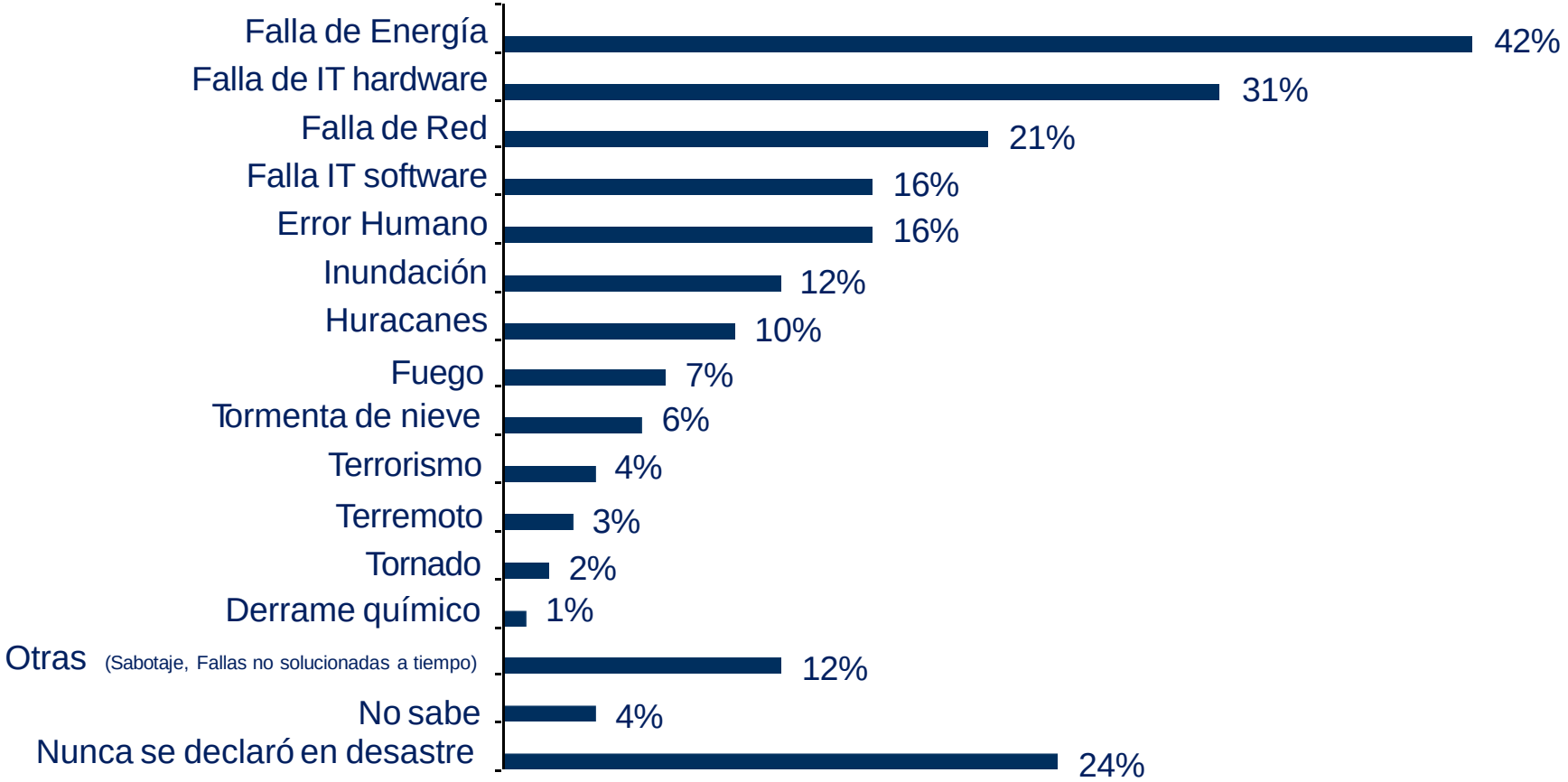
Donde utilizan herramientas que integra a la perfección todos los elementos esenciales del trabajo en equipo, como correo electrónico, chat, llamadas de voz y vídeo, documentos compartidos, gestión de tareas, consola de administración o herramientas de seguridad para que los usuarios puedan conectarse, crear y colaborar de forma fácil y fiable, estén donde estén.

También llamado EMERGENCY OPERATION CENTER (EOC) se define como el área de trabajo Alternativa donde podrá operar el Comité de Manejo de Crisis o Comité de Contingencia en conjunto con el Comité Ejecutivo, de ser el caso, equipadas para operar en situación de contingencia.

ESTANDARES DRII / BCI/ISO

SITUACIÓN ACTUAL

"Cuales son las causas que originaron la situación de riesgo más significativa o que ocasionó mayor tiempo de interrupción en las empresas"



Fuente: DRJ

Solo cuatro de cada 10 CIO tiene un plan de continuidad de negocio

Noticias & Análisis marzo 23, 2022 Maricela Ochoa

En materia de ciberseguridad, los principales riesgos que ven para sus compañías son las filtraciones de datos (47%), el malware y el ransomware (39%). Además, hay tres prioridades para los tomadores de decisiones en áreas IT: la continuidad del negocio, la resiliencia y la eliminación de riesgos.

https://www.itmastersmag.com/noticias-analisis/plan-de-continuidad-de-negocio-informe-logicalis/

Introducción

- Sobre el Riesgo País: **“vemos cómo las economías que se encuentran en escenarios inestables están en la cola de la clasificación, siendo Venezuela el de mayor riesgo con unos 3.204 puntos.” (EL AGRO, 2016)**
- “Mayoría de empresas peruanas no están preparadas para enfrentar riesgos en su negocio.”
- “Las empresas enfrentan a diario todo tipo de riesgos que pueden afectar de manera grave su funcionamiento.”
- “Según la casuística, por lo menos una vez al año toda empresa es afectada por un desastre”

  (ECONOMÍA, 2016)

Elaborado por (EL AGRO, 2016). Fuente: JP Morgan

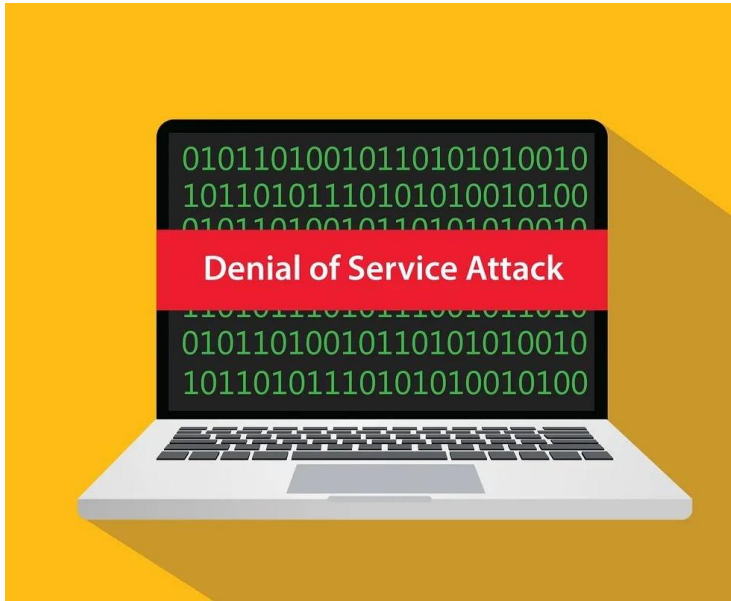
¿ Qué podría suceder ?

- Desastres de gran impacto
- Pequeños incidentes

¿ Por qué se requiere gestionar la Continuidad ?

Casos de desastres contra la continuidad

- Sitios WEB atacados mediante Denial of Service
- Situación terremoto de Armenia
- Atentados terroristas
- Desórdenes públicos que impiden el acceso a las instalaciones
- Centros de cómputo fuera de servicio



ESTANDARES DRII / BCI/ ISO

PILARES FUNDAMENTALES

BCP - DRP

Análisis de Impacto

- Cuantifica las pérdidas
- Establece tiempos de recuperación de procesos / sistemas críticos
- Prioriza los procesos críticos
- Establece los recursos y personal crítico

Análisis de Riesgo

- Establece escenarios contingentes
- Muestra riesgos y vulnerabilidades
- Analiza la utilización efectiva de controles
- Ofrece recomendaciones de mejora

Estrategia de Recuperación

- Provee información para la selección de una estrategia de respaldo alternativa
- Muestra la arquitectura necesaria para dar continuidad a los procesos críticos de la empresa

Plan de Contingencia

- Presenta los procedimientos necesarios a ser implementados en situaciones de contingencia
- Establece la Gobernabilidad del Plan
- Maneja las crisis
- Políticas de Continuidad

Plan de Mantenimiento y Pruebas / Plan de Capacitación y Concientización

Práctica

Caso de Estudio: Telefónica del Perú

- Ataque RANSOMWARE. (XATAKA, 2017)
- Envío de 5 millones de correos electrónicos por hora para difundir un malware llamado *WCry*, *WannaCry*, *WanaCrypt0r*, *WannaCrypt* o *Wana Decrypt0r*.
- Los empleados de Telefónica en Perú han recibido la orden de apagar sus computadoras y no conectarse a las redes inalámbricas de internet de la compañía desde sus celulares.
- "Sobre la incidencia en ciberseguridad ocurrida en España, informamos que nuestros servicios no se han visto afectados en el Perú, pero podríamos tener algunos inconvenientes en atención al cliente por desplegar los mecanismos preventivos correspondientes."(EL COMERCIO, 2017)

Fuente: El Comercio - WEB®

Pregunta de Estudio

- ¿Qué aspectos de la Continuidad del Negocio de la empresa, se vieron comprometidos ante esta amenaza?

ESTANDARES DRII / BCI

CONCLUSIONES

- La Continuidad de Negocio es una **estrategia para recuperar la operación crítica de una empresa en situaciones de contingencia.**

- El activo más importante para las empresas son las **personas.**

- Dentro del proceso de planificación deben identificarse los **riesgos, los impactos, los procesos y recursos críticos y los objetivos y puntos de recuperación.**

- El principal objetivo es **Salvaguardar la vida de las personas**.

- La **Capacitación y Concientización** son fundamentales.

- La estrategia debe **Mantenerse** en el tiempo y debe ser **Probada**
  - periódicamente.