INDICE

I.- INTRODUCCION 3

II.-JUSTIFICACION 3

III.- DESARROLLO DEL TEMA 4

1.- PLAN DE CONTINGENCIA 4

2.-OBJETIVOS DEL PLAN DE CONTINGENCIA 4

2.1.-OBJETIVOS GENERALES 4

2.2.-OBJETIVOS ESPECIFICOS 4

3.- DESARROLLO 6

3.1.-QUE ES UN PLAN DE CONTINGENCIA INFORMATICO 6

3.2.-PARA QUE SIRVE 6

3.3.-DONDE SE APLICA 7

3.4.-CUANDO SE APLICA 8

3.5.-COMPONENTES DE UN PLAN DE CONTINGENCIA INFORMÁTIC 9

3.6.-TIPOS DE PLAN DE CONTINGENCIA 10

3.7.-ETAPAS DEL PLAN DE CONTINGENCIA 13

IV.-MARCO TEORICO 18

V.- CONCLUSIONES 23

VI.-RECOMENDACIONES 24

VIII.- WEBGRAFIA 25

I.- INTRODUCCION

Todas las empresas u organizaciones, siempre van a estar expuestas a eventos inesperados que pueden interrumpir parcial o totalmente sus operaciones. Estos eventos pueden incluir desastres naturales, fallos tecnológicos, emergencias sanitarias, incendios, hackers, errores humanos, entre otros. Ante este tipo de riesgos, es indispensable contar con mecanismos eficaces que permitan responder de manera organizada, oportuna y eficaz para poder reducir estos riesgos.

Para poder reducir todos estos riesgos se debe crear un plan de contingencia, que es un conjunto de estrategias, procedimientos y recursos previamente establecidos que tienen como objetivo asegurar la continuidad de las operaciones esenciales de una empresa ante cualquier situación. Su propósito es reducir al mínimo el impacto de los incidentes, proteger los recursos humanos, tecnológicos y materiales.

La elaboración de este plan responde a la necesidad de estar preparados ante eventos que, aunque no se puedan prever completamente, pueden gestionarse con una planificación adecuada. A través de este plan, se definen roles, responsabilidades, recursos disponibles y acciones específicas que permitirán una respuesta rápida, coordinada y eficiente.

II.-JUSTIFICACION

Adquirir más conocimiento, investigando el concepto del plan de contingencia su origen, finalidad y estructura. Aprender la importancia de este tema y su funcionamiento como herramienta preventiva ante situaciones inesperadas. Identificar sus

componentes, sus etapas de elaboración, los riesgos y cómo podemos llegar aplicarlos en distintos ámbitos. Reforzar nuestro conocimiento para así poder lograr vencer la materia de auditoria en control de sistemas.

III.- DESARROLLO DEL TEMA

1.- PLAN DE CONTINGENCIA

2.-OBJETIVOS DEL PLAN DE CONTINGENCIA

2.1.-OBJETIVOS GENERALES

El objetivo general de un plan de contingencia informática es garantizar la continuidad de las operaciones de los sistemas de información críticos, minimizando el impacto de posibles incidentes y permitiendo una rápida recuperación. El plan debe asegurar que los servicios esenciales de la organización sigan funcionando, incluso en caso de una interrupción o falla en los sistemas informáticos.

Este objetivo se logra mediante la implementación de medidas de seguridad y recuperación de datos que permitan minimizar el impacto de una interrupción y restablecer los sistemas con la mayor rapidez posible.

2.2.-OBJETIVOS ESPECIFICOS

Los objetivos específicos de un plan de contingencia informática suelen incluir:

Definir la estructura organizacional para la gestión de la contingencia:

Identificar los roles y responsabilidades de cada persona o equipo involucrado en la respuesta a incidentes y la recuperación de sistemas.

Establecer procesos de recuperación:

Definir los pasos y procedimientos a seguir para restaurar los sistemas informáticos y los servicios de TI.

Coordinar la respuesta a incidentes:

Establecer mecanismos de comunicación y colaboración entre los diferentes equipos y partes interesadas involucradas en la gestión de la contingencia.

Identificar mecanismos de recuperación:

Determinar las herramientas, técnicas y recursos necesarios para la restauración de los sistemas informáticos.

Establecer plazos de recuperación:

Definir el tiempo máximo en el que se espera que los sistemas informáticos y los servicios de TI se puedan recuperar y volver a funcionar.

Además de los objetivos anteriores, un plan de contingencia informática también puede incluir objetivos específicos relacionados con la seguridad de la información, como la protección contra virus informáticos, ataques cibernéticos y la prevención de la pérdida de datos críticos.

Estos objetivos específicos de un plan de contingencia informática son fundamentales para garantizar la continuidad de las operaciones, minimizar el impacto de los incidentes y recuperar la funcionalidad de los sistemas de forma rápida y eficiente.

3.- DESARROLLO

3.1.-QUE ES UN PLAN DE CONTINGENCIA INFORMATICO

Un Plan de Contingencia Informática es un conjunto de estrategias y procedimientos diseñados para garantizar la disponibilidad, integridad y confidencialidad de los datos críticos y los sistemas de información de una organización.

Propone una serie de procedimientos alternativos al funcionamiento normal de una organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa. Estos planes lo que pretenden es garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad.

Los especialistas recomiendan planificar cuando aún no es necesario; es decir, antes de que sucedan los accidentes. Por otra parte, un plan debe ser dinámico y debe permitir incluir alternativas frente a nuevas incidencias que se pudiesen producir con el tiempo. Es por eso que un plan debe ser revisado y actualizado de forma periódica.

3.2.-PARA QUE SIRVE

La función principal de un plan de contingencia es proporcionar a la empresa una hoja de ruta estructurada para manejar situaciones de crisis. Sirve como un salvavidas organizativo, permitiendo respuestas rápidas y eficaces ante eventos que podrían comprometer la estabilidad de la empresa. Además, ayuda a minimizar la

interrupción del servicio, proteger la reputación de la empresa y reducir las pérdidas económicas asociadas con situaciones imprevistas.

Estos planes no solo responden a crisis inmediatas, sino que también fomentan una cultura organizacional al promover la conciencia y la preparación continua de todo el personal de la empresa. Actúa como un marco sólido que capacita a los equipos para gestionar eventos críticos de manera coordinada y efectiva.

3.3.-DONDE SE APLICA

Se aplica en todas las organizaciones de todos los tamaños y tipos: desde pequeñas empresas hasta grandes corporaciones, instituciones gubernamentales y organizaciones sin fines de lucro. Cualquier entidad que utilice tecnología para sus operaciones diarias necesita un plan de contingencia informática. Se pueden aplicar también en las siguientes situaciones:

Cualquier área que dependa de sistemas de información:

Desde el área de administración y finanzas hasta las áreas de producción, ventas y marketing. Un plan de contingencia debe abarcar todas las áreas y procesos que dependen de los sistemas informáticos.

En caso de cualquier evento que pueda causar interrupciones:

Esto incluye desastres naturales (incendios, terremotos, inundaciones), fallas de hardware o software, errores humanos, ciberataques y otras interrupciones imprevistas.

Para garantizar la continuidad del negocio:

El objetivo principal del plan de contingencia es permitir que la organización pueda seguir operando o reanudar sus operaciones lo más rápido posible después de un incidente.

En resumen, los planes de contingencia informática son esenciales para cualquier organización que dependa de la tecnología para sus operaciones, y se aplican en cualquier área o proceso que pueda verse afectado por una interrupción o incidente.

3.4.-CUANDO SE APLICA

Los planes de contingencia informática se aplican cuando ocurren eventos imprevistos que pueden interrumpir o afectar la operación de las tecnologías de información (TI). Estos eventos pueden ser

Desastres naturales:

Incendios, terremotos, inundaciones, etc., que pueden dañar o destruir equipos informáticos y la infraestructura de TI.

Fallos de hardware:

Daños o fallos en servidores, computadoras, redes u otros dispositivos que afectan el funcionamiento de la TI.

Errores humanos:

Errores en la configuración de sistemas, acceso no autorizado, borrado accidental de datos, etc.

Ciberataques:

Ataques maliciosos a la red, sistemas o datos que pueden comprometer la seguridad y disponibilidad de la TI.

Problemas de software:

Errores en el código, fallos de software, actualizaciones fallidas, etc., que pueden causar interrupciones o problemas de funcionamiento.

Falla de servicios de terceros:

Interrupciones en la conexión a internet, proveedores de servicios de nube, etc., que pueden afectar la operación de la TI.

3.5.-COMPONENTES DE UN PLAN DE CONTINGENCIA INFORMÁTICO

Evaluación de Riesgos:

Identificar y evaluar los riesgos potenciales que podrían afectar la infraestructura y los sistemas de información.

Estrategias y Procedimientos:

Desarrollar las estrategias y procedimientos para prevenir, mitigar y responder a los riesgos identificados.

Organización y Responsabilidades:

Definir la estructura organizativa y las responsabilidades de cada persona o equipo en caso de emergencia.

Comunicación:

Establecer los canales de comunicación para informar a los usuarios y a las partes interesadas sobre la situación.

Pruebas y Actualización:

Realizar pruebas periódicas del plan de contingencia y actualizarlo según sea necesario.

Ejemplos de Actividades de un Plan de Contingencia:

Realizar copias de seguridad de los datos y sistemas de forma regular.

Mantenimiento de equipos de respaldo.

Capacitación del personal en temas de seguridad informática y gestión de emergencias.

Restauración de sistemas después de una falla o desastre.

Mantenimiento de un ambiente seguro y protegido para los sistemas y datos.

3.6.-TIPOS DE PLAN DE CONTINGENCIA

3.6.1.-Plan de respaldo

Este tipo de plan se centra en la protección y recuperación de datos esenciales para la operación. Incluye estrategias para la copia de seguridad de información crítica, la implementación de sistemas de redundancia y la salvaguarda de activos digitales. En el mundo digital actual, donde la información es un activo clave, el plan de respaldo se convierte en un componente esencial para salvaguardar la actividad empresarial y sus datos.

3.6.2.-Plan de emergencia

El plan de emergencia se orienta hacia la seguridad y el bienestar de las personas dentro y fuera de la organización. Define protocolos para evacuaciones, primeros auxilios, comunicación de emergencia y coordinación con servicios de respuesta externos. Su enfoque principal es garantizar la seguridad física de los empleados y colaboradores en situaciones críticas o de peligro.

3.6.3.-Plan de recuperación

Cuando una crisis impacta las operaciones, el plan de recuperación entra en juego. Se centra en la restauración de las funciones y servicios clave de la empresa después de un incidente. Incluye la asignación de roles y responsabilidades específicas, la evaluación de daños y la implementación de estrategias para la recuperación operativa. Este plan es crucial para minimizar el tiempo de inactividad y acelerar la vuelta a la normalidad.

3.7.- DEFICIENCIAS DE UN PLAN DE CONTINGENCIA INFORMATICO

Un plan de contingencia informática deficiente puede resultar en pérdidas significativas, interrupción de operaciones, y daño reputacional. Las deficiencias comunes incluyen falta de compromiso de la dirección, falta de integración entre diferentes programas, no tener en cuenta todos los posibles riesgos y vulnerabilidades, no involucrar a la dirección en la planificación, y no realizar pruebas y simulaciones regulares.

Deficiencias comunes de un plan de contingencia informático:

Falta de compromiso de la dirección:

Si la dirección no está comprometida con la importancia del plan, es menos probable que se implemente adecuadamente y se mantenga actualizado

Falta de integración:

Los programas y herramientas de un plan de contingencia deben funcionar juntos de manera eficiente. Si no están integrados, pueden surgir problemas de comunicación, datos duplicados, y retrasos en la recuperación.

Análisis incompleto de riesgos:

Un plan de contingencia debe identificar todos los riesgos y vulnerabilidades que puedan afectar a los sistemas y datos. Si no se realiza un análisis exhaustivo, se puede dejar de lado una amenaza crítica.

Falta de capacitación y pruebas:

El personal que participará en la recuperación de la información debe estar capacitado y debe realizarse pruebas periódicas para asegurar que el plan funcione como se espera, según OBS Business School.

No involucrar a la dirección:

La dirección debe ser parte del proceso de planificación y debe apoyar la implementación del plan.

No realizar pruebas y simulaciones:

Las pruebas y simulaciones regulares son esenciales para identificar las debilidades del plan y garantizar que funcione correctamente en caso de una emergencia.

No tener en cuenta las vulnerabilidades:

Las vulnerabilidades informáticas cambian constantemente, por lo que el plan debe estar actualizado con las últimas amenazas y medidas de seguridad.

No tener un plan de respaldo y recuperación:

El plan debe incluir un plan de respaldo de datos y un plan de recuperación en caso de que los sistemas fallen.

No tener un sitio de recuperación alterno:

En caso de que la infraestructura principal se dañe, se debe tener un sitio de recuperación alterno para poder seguir operando.

No tener un plan de comunicación:

El plan debe incluir un plan de comunicación para informar a los usuarios y stakeholders sobre la situación y los pasos a seguir.

3.7.-ETAPAS DEL PLAN DE CONTINGENCIA

Existen 3 etapas y son las siguientes:

3.7.1.-ANTES: FASE DE PLANIFICACIÓN Y PREVENCIÓN

Esta es la etapa más importante. Aquí se sientan las bases para estar preparado ante cualquier evento inesperado.

1. Identificación de riesgos

Se analizan todos los posibles eventos negativos que pueden afectar las operaciones: fallas tecnológicas, incendios, inundaciones, crisis sanitarias, errores humanos, etc.

Se clasifican según:

Probabilidad de ocurrencia (baja, media, alta).

Impacto potencial (leve, moderado, crítico).

2. Evaluación de impactos

Se analizan los efectos que cada riesgo puede tener sobre:

Personas (empleados, clientes).

Infraestructura.

Tecnología.

Información/confidencialidad.

Continuidad del negocio.

3. Definición de recursos críticos

Se determinan los activos y procesos más importantes para la organización. Ejemplos: servidores, personal clave, software, redes, comunicaciones, insumos, etc.

4. Diseño del plan de contingencia

Se crean procedimientos de respuesta específicos para cada tipo de incidente.

Se asignan responsabilidades (quién hace qué).

Se establecen canales y protocolos de comunicación internos y externos.

5. Capacitación y simulacros

Se entrena al personal en su rol dentro del plan.

Se hacen pruebas periódicas (simulacros, ensayos técnicos, pruebas de restauración de datos, etc.).

3.7.2.-DURANTE: FASE DE RESPUESTA

Es cuando ocurre el incidente. Aquí se ejecuta el plan según lo previsto para minimizar el impacto.

1.- Activación del plan

Un responsable o comité toma la decisión de activar el plan de contingencia.

Se declara el nivel de emergencia (leve, moderada, crítica).

Se convoca al equipo designado.

2. Ejecución inmediata de medidas

Aplicación de protocolos definidos: apagar servidores, evacuar edificios, migrar datos, contener amenazas, etc.

Tareas clave:

Protección de vidas y bienes.

Contención del incidente.

Continuidad de servicios críticos.

3. Comunicación interna y externa

Notificación clara y rápida a todo el personal afectado.

Comunicación con clientes, proveedores, medios, si es necesario.

Usar canales oficiales: emails, altavoces, redes sociales, etc.

4. Monitoreo y toma de decisiones

Se supervisa la evolución del incidente en tiempo real.

Se hacen ajustes en la estrategia si es necesario.

Se documenta todo lo que ocurre.

3.7.3.-DESPUÉS: FASE DE RECUPERACIÓN Y MEJORA

Una vez que se controla la situación, se trabaja para volver a la normalidad y aprender de la experiencia.

1. Evaluación de daños

Se revisa el impacto real del evento.

Evaluación técnica, financiera, operativa y humana.

2. Restauración de operaciones

Recuperación de sistemas y servicios afectados.

Reinstalación de servidores, recuperación de datos, reparación de daños físicos, etc.

Retorno progresivo a la normalidad operativa.

3. Informe post-evento

Se elabora un informe detallado con:

Qué pasó.

Cómo se respondió.

Qué funcionó y qué no.

Recomendaciones.

4. Lecciones aprendida

Se hace una reunión de retroalimentación con todo el equipo.

Se identifican errores o brechas en el plan.

Se recopilan sugerencias de mejora.

5. Actualización del plan

Se hacen los ajustes necesarios para que el plan sea más robusto y eficaz.

Se actualiza documentación, roles y procedimientos

IV.-MARCO TEORICO

4.1. Contingencia en el ámbito informático

Una contingencia, en el contexto de las tecnologías de la información, se refiere a cualquier situación inesperada que pueda interrumpir el funcionamiento normal de los sistemas informáticos o servicios TI de una organización. Estas contingencias pueden derivarse de fallas técnicas, ciberataques, errores humanos, desastres naturales o incidentes físicos como incendios o cortes eléctricos.

El plan de contingencia informática tiene como finalidad garantizar la continuidad de los servicios digitales y proteger los activos de información ante cualquier interrupción.

4.2. Impacto de las contingencias informáticas

El impacto de una interrupción en los sistemas informáticos puede ser grave, especialmente en organizaciones cuya operatividad depende de sistemas digitales. Entre los efectos más comunes se encuentran:

Pérdida de datos críticos.

Caída de servicios esenciales.

Deterioro de la imagen institucional.

Pérdidas económicas y legales.

Interrupciones en la comunicación y toma de decisiones.

Según la norma **ISO 27031**, el impacto debe medirse en función del tiempo máximo tolerable de inactividad (RTO) y la cantidad de datos que se puede perder sin consecuencias graves (RPO).

4.3.- Servicios TI y continuidad operativa

Los servicios de tecnologías de la información (TI) son pilares fundamentales para las organizaciones actuales. Incluyen correo electrónico, servidores, bases de datos, almacenamiento en la nube, software empresarial, redes y soporte técnico. La continuidad de estos servicios es esencial.

4.4.-Identificación de riesgos

La identificación de riesgos es el primer paso en la gestión de la continuidad operativa. Consiste en reconocer todos los eventos, internos o externos, que pueden afectar el funcionamiento normal de la organización.

Según la norma **ISO 31000**, el riesgo se define como el “efecto de la incertidumbre sobre los objetivos”.

4.5.-. Probabilidad de ocurrencia

Una vez identificados los riesgos, se evalúa su **probabilidad de ocurrencia** y su impacto potencial. Esto permite priorizarlos y establecer estrategias de mitigación. Los riesgos se clasifican comúnmente en matrices de riesgo con dos dimensiones:

Probabilidad: Baja, media o alta (¿qué tan probable es que ocurra?).

Impacto: Bajo, medio o alto (¿qué tan grave sería si ocurre?).

Por ejemplo, un fallo del servidor principal podría tener una alta probabilidad si no se realizan mantenimientos, y un impacto crítico si afecta ventas o servicios al cliente.

4.6.-Recursos críticos

Los recursos críticos son aquellos elementos sin los cuales la organización no podría operar con normalidad. Pueden ser tangibles (equipos, servidores, sistemas informáticos) o intangibles (datos, personal especializado, procesos clave).

Identificarlos es clave para definir qué se debe proteger y recuperar con prioridad durante una contingencia. Algunos ejemplos:

- Infraestructura tecnológica (redes, servidores, energía).

- Software de gestión empresarial (ERP, CRM).

- Base de datos de clientes.

- Personal técnico clave.

- Comunicaciones internas y externas.

La protección y respaldo de estos recursos es fundamental dentro del plan de contingencia.

4.7.- Fase post-evento

La fase post-evento es la etapa de recuperación y evaluación tras una contingencia. Aquí se desarrollan acciones para restablecer operaciones, revisar la respuesta dada y mejorar el plan para el futuro.

4.8.- Incidente

Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En este contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático.

4.9.- Plan de Prevención

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan.

El plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

4.10.- Plan de Ejecución

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones

descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

4.11.- Plan de Recuperación

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

4.12.- Plan de Pruebas

Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

4.1.3.-Eventos críticos

Es un incidente o situaciones puede tener un impacto significativo o negativo en una organización, sus operaciones, su reputación o su capacidad para funcionar de manera efectiva.

4.1.5.-Crisis

Es una situación que requiere una respuesta inmediata y efectiva para minimizar el impacto negativo en una organización. Es conjunto de problemas graves y complejos que afectan la industria del software, como la dificultad en desarrollar software de calidad a tiempo y dentro del presupuesto, así como la falta de profesionales cualificados.

4.1.6.-Ciberataques

Es un intento de acceso no autorizado a sistemas informáticos o redes para robar, modificar o destruir datos, o para causar interrupciones. Estos ataques pueden tener como objetivo a individuos, organizaciones o incluso gobiernos.

4.1.7.- Incidentes

Es un evento no deseado o inesperado que interrumpe el funcionamiento normal de un sistema de información o que compromete la seguridad de la información. Puede incluir accesos no autorizados, uso no autorizado de datos, fallos en la operación de la red, sistemas o recursos informáticos, o violaciones de políticas de seguridad.

V.- CONCLUSIONES

Un plan de contingencia es fundamental para garantizar la continuidad de las operaciones y poder minimizar el impacto de posibles incidentes o desastres que afecten a los sistemas informáticos. Este tipo de plan permite establecer protocolos claros para poder actuar antes, durante y después de una emergencia minimizando los daños. Asimismo, definir roles claros, realizar simulacros periódicos y mantener el plan actualizado garantiza su efectividad frente a amenazas emergentes. Este trabajo demuestra la importancia de que los futuros profesionales en áreas como auditoría, contabilidad, administración y finanzas conozcan a fondo estos procedimientos, ya que la tecnología es parte esencial de la operación y la toma de decisiones estratégicas de cualquier organización. Contar con un plan sólido y funcional no solo protege los activos informáticos, sino que también preserva la reputación, la confianza de los clientes y la viabilidad del negocio en el largo plazo.

VI.-RECOMENDACIONES

Para poder desarrollar un plan de contingencia efectivo debemos seguir las siguientes recomendaciones:

Identificar los posibles riesgos o amenazas

Designar personas responsables de implementar y mantener el plan de contingencia

Realizar pruebas regulares del plan de contingencia

Actualizarlo periódicamente para reflejar cambios

Capacitar al personal

Incluir procedimientos de respaldo y recuperación de datos

Establecer canales de comunicación claros y efectivos

Capacitación constante del personal involucrado.

Inversión en infraestructura de respaldo.

Adopción de políticas de seguridad cibernética proactivas.

Integración de este plan con el plan general de continuidad del negocio

VIII.- WEBGRAFIA

https://www.nalandaglobal.com/blog/que-es-el-plan-de-contingencia-de-una-empresa/

https://adservice.me/es/adservice/adnews/planes-de-contingencias-informaticas#:~:text=%C2%BFQu%C3%A9%20es%20un%20Plan%20de,de%20informaci%C3%B3n%20de%20una%20organizaci%C3%B3n.

https://www.senara.go.cr/acerca_del_senara/direcciones/gestion_informatica/Plan%20de%20Contingencia%20Informatico%20y%20Recuperacion%20de%20Servicios%20de%20Tecnologia%20de%20la%20Informacion%20y%20Comunicaciones.pdf

https://asana.com/es/resources/contingency-plan?utm_source=.com

https://iris.paho.org/handle/10665.2/57791?utm_source=.com

https://www.ifrc.org/es/nuestro-trabajo/desastres-clima-y-crisis/preparacion-para-desastres/planificacion-contingencias?utm_source=.com

https://pmbc.es/plan-de-contingencia-que-es-y-como-se-elabora/?utm_source=.com

https://recursos-humanos.org/productividad/plan-de-contingencia/?utm_source=com

https://iso.cat/es/iso-22301-plan-de-continuidad-del-negocio/?utm_source=com

https://www.isotools.us/2019/06/04/elementos-del-plan-de-contingencia-segun-iso-22301/?utm_source=c

https://www.senara.go.cr/acerca_del_senara/direcciones/gestion_informatica/Plan%20de%20Contingencia%20Informatico%20y%20Recuperacion%20de%20Servicios%20de%20Tecnologia%20de%20la%20Informacion%20y%20Comunicaciones.pdf

https://www.sixsenseadvisors.com/wp/el-plan-de-contingencia-informatico-y-recuperacion-de-servicios-de-tecnologias-de-la-informacion-y-comunicaciones-tic/

https://es.wikipedia.org/wiki/Plan_de_contingencias

https://liderazgo.space/plan-de-contingencia/

https://www.ibm.com/think/topics/disaster-recovery-plan

https://www.unisdr.org/campaign/resilientcities/uploads/city/attachments/4220-10814.pdf

https://www.unifikas.com/es/noticias/plan-de-contingencia-lo-que-debes-conocer

https://www.cynthus.com.mx/elementos-plan-contingencia-gestion-riesgos/#:~:text=El%20primer%20paso%20para%20elaborar,naturales%20o%20los%20ataques%20cibern%C3%A9ticos.