Planes de Continuidad y Contingencia

Aplicaciones GreyPhillips

El plan de continuidad y de contingencia tiene como finalidad los pasos a seguir por un eventual suceso o desastre, tal que permita recuperar o mantener la capacidad funcional de los sistemas.

Entiéndase por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al evento, habiéndose reemplazado o recuperado el máximo o la totalidad de los recursos e información".

Por tanto, se dice que el Plan de Contingencia es el encargado de sostener el modelo de planteado y de levantarlo cuando se vea afectado.

La recuperación de la información se basa en el uso de una política de copias de seguridad (Backups) adecuada y a tener soluciones alternas a contingencias previstas mediante análisis.

Alcance

La presente Política para la continuidad y contingencia contempla los lineamientos de los servicios, que se dicta en cumplimiento de las disposiciones vigentes en Lógica Digital del Oriente S.A, con el objeto de gestionar adecuadamente los sistemas informáticos y el ambiente tecnológico de la organización.

Debe ser conocida y cumplida por todo el personal sea cual fuere su nivel jerárquico, rol dentro de la organización o tercerización.

Términos y Definiciones

A los efectos de este documento se aplican las siguientes definiciones relacionadas para la gestión de la continuidad:

Continuidad: Un Plan de Continuidad está enfocado a asegurar la continuidad del negocio, cuando inesperadamente ocurre un incidente.

El objetivo del plan es permitir que no se detenga la productividad de la empresa e intentar que la situación que ha sucedido en ese momento tenga el menor impacto posible.

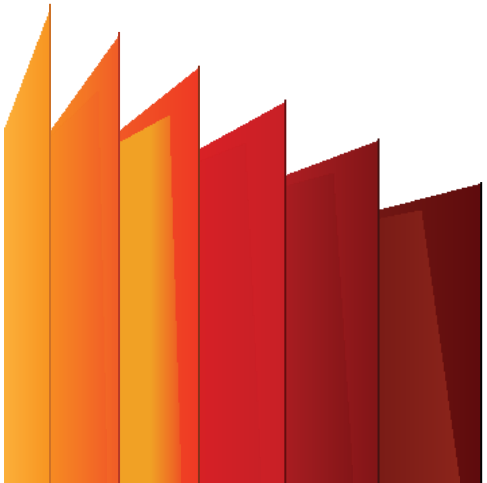
Contingencia: Un Plan de Contingencia consiste en minimizar el impacto financiero que puede causar un «incidente» inesperado en la compañía dentro del marco de los procedimientos habituales de la empresa, este plan trabaja para recuperar a la compañía de los imprevistos especiales que se puedan presentar, y que por su causa interrumpen el sistema de producción.

Objetivo General

Establecer bajo los protocolos de contingencia, una adecuada previsión de posibles eventos que se encuentre fuera de casos fortuitos o fuerza mayor.

Objetivos Específicos

- Determinar las políticas y procedimientos para respaldar las aplicaciones y datos.
- Planificar la reactivación de los servicios asociados a un evento, así como los procedimientos y sus funciones asociadas.
- Ejecutar permanentemente el mantenimiento y supervisión de los sistemas.
- Establecer una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un evento.



Plan de Continuidad y Contingencia

Generalidades

En esta sección indicaremos las acciones a tomar, los actores a involucrar, los recursos a emplear, procedimientos a seguir, etc. en un formato adecuado para su uso en situaciones críticas.

Se establecen 4 fases para la ejecución del plan de contingencia:

- Fase de Alerta
  - Notificación
  - Evaluación
  - Ejecución del Plan
- Fase de Transición
  - Procedimiento de agrupación de personas y equipos requeridos
  - Procedimiento de puesta en marcha del protocolo de recuperación
- Fase de Recuperación
  - Protocolo de restauración
  - Protocolo de gestión y soporte
- Fase de vuelta a la normalidad
  - Análisis de Impacto
  - Procedimiento de vuelta a la normalidad

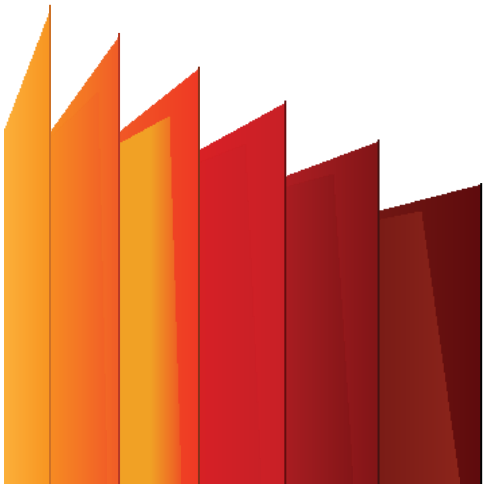
Plan de continuidad y contingencia de las áreas de servicio y almacenamiento de la información para la adecuada solución de casos:

Clase de incidente	Plan de Acción	Personas
Cambios en el personal	Capacitación continua y transferencia de conocimiento a las áreas relacionadas	• Encargado del departamento de Recursos Humanos • Encargado del Área relacionada
Interrupción del servicio de energía	**Infraestructura Local:** Activación de la planta eléctrica de respaldo para mantener los servidores y sistemas de telecomunicaciones activos. **Infraestructura Internacional:** Actualmente se cuenta con servicios redundantes de data center y control de caídas eléctricas en tiempo real.	• Encargado del Departamento Operativo
Interrupción de los servicios de telecomunicaciones	**Infraestructura Local:** Reporte técnico de la caída al proveedor de servicio local y asignación de responsable para el seguimiento del reporte y ejecución del SLA Corporativo relacionado **Infraestructura Internacional:** Actualmente se cuenta con servicios redundantes de data center y control de caídas de servicios de telecomunicaciones en tiempo real.	**Infraestructura Local:** • Encargado del Departamento Operativo **Infraestructura Internacional para casos que deban ser escalados:** • Gerente de TI
Incidentes por fallas o mal funcionamiento de sistemas o de dispositivos como servidores, routers, entre otros.	1. Evaluar la situación 2. Se determina que personas están relacionadas a los sistemas con mal funcionamiento 3. Se establece el plan de acción a seguir para resolver la situación en el menor tiempo posible 4. Se reasignan las prioridades 5. Se comunica a los clientes afectados a través de los canales preestablecidos de la situación en los casos de afectación directa 6. Se ejecutan el plan de acción 7. Se aplican las correcciones necesarias para normalizar la operación 8. Se evalúan las correcciones 9. Se notifica a los clientes afectados de la solución 10. Se establece un plan de acción para hacer correcciones necesarias que surjan como resultado del fallo	• Gerencia de TI • Encargado del Área relacionada • Gerencia de Operaciones • Equipo Técnico relacionado • Encargado de Servicio al Cliente • Encargado de Soporte Técnico
Incidentes por actividad maliciosa con el fin de desestabilizar o dañar un sistema informático, tales como: suplantación de identidad, Phishing, Negación de servicio (DoS, DDoS), Código malicioso (malware, troyanos, gusanos, inyección de código, virus, ransomware).	**Procedimiento:** 1. Evaluar la situación 2. Se determina que personas están relacionadas a los sistemas y/o servicios afectados 3. Se establece el plan de acción a seguir para resolver la situación en el menor tiempo posible 4. Se reasignan las prioridades 5. Se comunica a los clientes afectados a través de los canales preestablecidos de la situación en los casos de afectación directa 6. Se ejecutan el plan de acción 7. Se aplican las soluciones necesarias para normalizar la operación 8. Se evalúan las soluciones y su efectividad 9. Se notifica a los clientes afectados de la solución 10. Se establece un plan de acción para hacer correcciones necesarias que surjan como resultado del fallo **Prevención:** Actualmente se cuenta con las respectivas relaciones con los proveedores que ayuden a prevenir y mitigar el impacto de fallos potenciales de esta naturaleza, tales como Antivirus, Firewalls, Servicios de Ciber Seguridad	• Gerencia de TI • Encargado del Área relacionada • Gerencia de Operaciones • Equipo Técnico relacionado • Encargado de Servicio al Cliente • Encargado de Soporte Técnico
Incidentes por desastres naturales o ambientales, tales como:	**Infraestructura Local:**	Personal de todos los

Terremotos, inundaciones, huracanes, incendios.	• Se activa el protocolo para desocupar el edifico principal • Se asignan las labores a nivel de teletrabajo para dar continuidad de los servicios críticos • Se evalúa el alcance de la afectación para establecer cuales servicios locales pueden continuar sin interrupción. Infraestructura Internacional: Actualmente se cuenta con servicios redundantes de data center y control de caídas de servicios de telecomunicaciones en tiempo real.	departamentos

Asociado a los planes de contingencia se deben de considerar los eventos que se presenten según la naturaleza de estos, es decir, un servicio o un sistema puede fallar debido a otras circunstancias diferentes a los fallos propios del software o la infraestructura, que pueden ser clasificado de la siguiente manera:

Tipo	Descripción
Por Integridad	Datos incompletos, exactitud de los registros, por selección errónea de reportes de las aplicaciones usadas para la gestión de los servicios.
Por Relación	Información gestionada por otras aplicaciones relacionadas sobre las cuales no se tiene un adecuado control de calidad o de precisión de los datos.
Por Recursos	Cuando no existe una estructura tecnológica efectiva (hardware, software, redes, personas y procesos) para realizar el adecuado uso de los sistemas y la información derivada de estos.



Contención, Corrección y Recuperación

Generalidades

Actividades Post Incidente

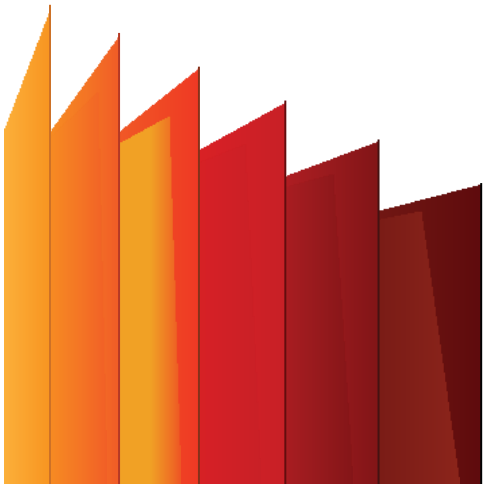
Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas, el establecimiento de medidas tecnológicas necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

Lecciones Aprendidas

Mantener un proceso de "lecciones aprendidas" después de un incidente o evento, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes.

Por tanto, parte de los planes de mejora en la continuidad de la información es mantener un adecuado registro de lecciones aprendidas que permitan conocer los siguientes aspectos:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente de la misma naturaleza.
- Acciones correctivas que pueden prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.



Políticas Corporativas
Junio 2023

www.greyphillips.com

Por mucho tiempo, la seguridad se ha equiparado a estar cerrado, pero cuando se trata de ecosistemas móviles esa transformación ha tenido que ir de plataformas aisladas a plataformas abiertas que fomenten la innovación y permitan la interoperabilidad dentro de un marco de seguridad y confianza. El esquema de seguridad de GreyPhillips está construido para proteger a los usuarios y a las organizaciones a mantener su información segura.

25 YEARS

GreyPhillips
Make IT happen