

Sustento del uso justo
de Materiales Protegidos
derechos de autor para
fines educativos



UCI

Universidad para la
Cooperación Internacional

UCI
Sustento del uso justo de materiales protegidos por
derechos de autor para fines educativos

El siguiente material ha sido reproducido, con fines estrictamente didácticos e ilustrativos de los temas en cuestión, se utilizan en el campus virtual de la Universidad para la Cooperación Internacional – UCI – para ser usados exclusivamente para la función docente y el estudio privado de los estudiantes pertenecientes a los programas académicos.

La UCI desea dejar constancia de su estricto respeto a las legislaciones relacionadas con la propiedad intelectual. Todo material digital disponible para un curso y sus estudiantes tiene fines educativos y de investigación. No media en el uso de estos materiales fines de lucro, se entiende como casos especiales para fines educativos a distancia y en lugares donde no atenta contra la normal explotación de la obra y no afecta los intereses legítimos de ningún actor.

La UCI hace un USO JUSTO del material, sustentado en las excepciones a las leyes de derechos de autor establecidas en las siguientes normativas:

- a- Legislación costarricense: Ley sobre Derechos de Autor y Derechos Conexos, No.6683 de 14 de octubre de 1982 - artículo 73, la Ley sobre Procedimientos de Observancia de los Derechos de Propiedad Intelectual, No. 8039 – artículo 58, permiten el copiado parcial de obras para la ilustración educativa.
- b- Legislación Mexicana; Ley Federal de Derechos de Autor; artículo 147.
- c- Legislación de Estados Unidos de América: En referencia al uso justo, menciona: "está consagrado en el artículo 106 de la ley de derecho de autor de los Estados Unidos (U.S.Copyright - Act) y establece un uso libre y gratuito de las obras para fines de crítica, comentarios y noticias, reportajes y docencia (lo que incluye la realización de copias para su uso en clase)."
- d- Legislación Canadiense: Ley de derechos de autor C-11– Referidos a Excepciones para Educación a Distancia.
- e- OMPI: En el marco de la legislación internacional, según la Organización Mundial de Propiedad Intelectual lo previsto por los tratados internacionales sobre esta materia. El artículo 10(2) del Convenio de Berna, permite a los países miembros establecer limitaciones o excepciones respecto a la posibilidad de utilizar lícitamente las obras literarias o artísticas a título de ilustración de la enseñanza, por medio de publicaciones, emisiones de radio o grabaciones sonoras o visuales.

Además y por indicación de la UCI, los estudiantes del campus virtual tienen el deber de cumplir con lo que establezca la legislación correspondiente en materia de derechos de autor, en su país de residencia.

Finalmente, reiteramos que en UCI no lucramos con las obras de terceros, somos estrictos con respecto al plagio, y no restringimos de ninguna manera el que nuestros estudiantes, académicos e investigadores accedan comercialmente o adquieran los documentos disponibles en el mercado editorial, sea directamente los documentos, o por medio de bases de datos científicas, pagando ellos mismos los costos asociados a dichos accesos.

Guía práctica para la

Continuidad de Negocio



Índice

Introducción.....	1
Capítulo 1: La continuidad de negocio a simple vista.....	2
Capítulo 2: Análisis de riesgo.....	4
Capítulo 3: Análisis de impacto de negocio.....	10
Capítulo 4: Gestión de prioridades.....	13
Capítulo 5: Recuperación ante desastres.....	16
Capítulo 6: RPO y RTO.....	18
Capítulo 7: Planeación para la continuidad de negocio.....	20
Capítulo 8: Gestión de la crisis.....	22
Capítulo 9: Ejecución de pruebas.....	26
Capítulo 10: ECM y la nube como parte del plan de continuidad de su negocio.....	30
Estas listo para ver una demostración de Laserfiche.....	32
Acerca de Laserfiche.....	33

Introducción

Una situación de emergencia puede presentarse en cualquier momento, ya sea un huracán que inunda sus instalaciones, una pandemia que fuerza a todos a trabajar desde casa, o un acto de ciberterrorismo que compromete los sistemas.

Es de suma importancia tener planes detallados para enfrentar estas situaciones para asegurarse de que su personal y su negocio pueda seguir con las operaciones. Es crítico para la supervivencia de su negocio reanudar actividades lo antes posible, aún si no se encuentra con operaciones al 100%. El hecho de tener un plan para mitigar los riesgos de eventos imprevistos es un fundamento básico de la gestión de contingencia y continuidad de negocios.



Capítulo 1

La continuidad de negocio a simple vista

Si desea tener un marco completo para la gestión de la continuidad de negocio, debe considerar incluir lo siguiente:



Análisis de riesgo

Este análisis debe incluir posibles riesgos a su negocio o procesos. Incluya todos los riesgos, entre ellos puede incluir sucesos como siniestros, tormentas de nieve, o hasta un conflicto militar. Si identifica un riesgo que puede impactar potencialmente las actividades del día al día, agréguelo a la lista.



Análisis de impacto de negocio (BIA, por sus siglas en inglés)

Este análisis debe incluir una lista de todos los factores que pueden impactar negativamente su negocio, como pérdida de ingresos, productividad, o hasta de la reputación del negocio. Se debe generar un análisis de impacto de negocio para cada proceso y sistema esencial de su negocio.



Plan de recuperación ante desastres (DRP, por sus siglas en inglés)

Este plan involucra principalmente al departamento de Informática y Tecnología para la planeación de recuperación ante desastres de datos, sistemas y aplicaciones. Se debe crear un plan de recuperación ante desastres para cada sistema y aplicación esencial de su negocio.



Plan de continuidad de negocio (BCP, por sus siglas en inglés)

Estos planes aseguran que el proceso de negocio puede continuar, aún si no se cuenta con el personal, los flujos de trabajo u otros recursos que tendría bajo circunstancias normales.



Estrategia para la gestión de crisis

Esta estrategia aborda principalmente el lado humano de la crisis. ¿Cómo puede garantizar la seguridad de su personal? ¿Quién coordina la comunicación con proveedores, clientes, partes asociadas, y los medios de comunicación ¿Qué información se compartirá?

Capítulo 2

Análisis de riesgo

Un análisis de riesgo es el estudio de las causas de posibles amenazas a su negocio y procesos, y cómo afrontarlos.

Por ejemplo, en caso de que una inundación dañe los registros de una institución financiera y no cuenten con sitios de respaldos (o si el sitio de respaldo también ha sido dañado) los problemas que se pueden generar por el incumplimiento normativo por la pérdida de estos registros pueden continuar por meses o hasta años después del desastre.

Cualquiera que sea el desastre, natural o provocado por el hombre, es importante identificar los riesgos y planear para situaciones en las que no tenga acceso a los datos, recursos o personal que generalmente utiliza en las operaciones diarias.

Según el sitio Business News Daily, estos son algunos de los errores más comunes que las empresas cometen al considerar la gestión de la continuidad de negocio:

No tomar en cuenta la pérdida de personal esencial ni considerar el estrés o trauma del personal de trabajo.

No compartir el plan de emergencia con el personal, ya sea laborando en la oficina o remotamente, o dejar el plan muy genérico, muy detallado o sin actualizar.

No abordar los problemas críticos de comunicación y problemas de relaciones públicas durante el período de recuperación del evento.

No definir un centro de operaciones de emergencia (EOC, por sus siglas en inglés) o centros de crisis, o no se tiene un plan para que los empleados puedan trabajar desde cada cuando el sitio físico de trabajo no esté disponible.

Pensar que ayuda externa o el seguro se encargará de todo.

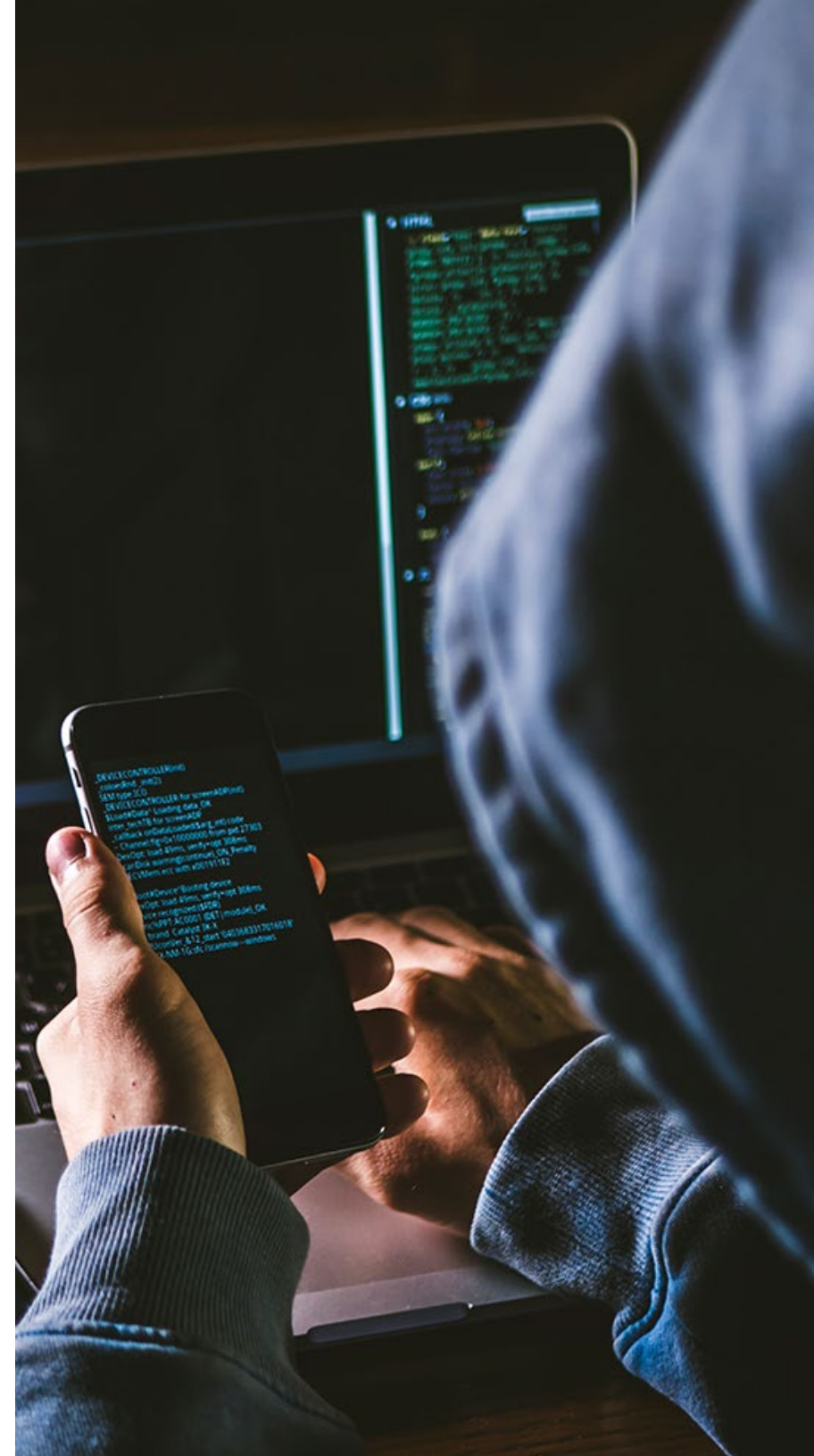
La mejor manera para prepararse para estos errores es convertirse en un experto en el arte de esperar lo inesperado. Existen muchos factores que pueden interrumpir el flujo de un negocio y por lo general se dividen en [cuatro categorías](#). Tenga en mente cada una de estas categorías al realizar su análisis de riesgo:

Situación 1: Pérdida del sistema y datos

Las empresas deben estar siempre al pendiente de los riesgos que pueden afectar sus sistemas, redes, y datos. Lamentablemente, las empresas no solo deben prepararse para enfrentar desastres naturales, sino que también deben estar preparados para delitos en la propiedad y fallas en la seguridad cibernética, dos riesgos significativos.

En el sector de la salud, un sector con muchas regulaciones, una falla en la seguridad cibernética puede significar miles de personas afectadas, numerosos medios de comunicación, y en el caso de ciertos países, rendimiento de cuentas ante entidades regulatorias. Si el caso se presenta en los EE. UU., se tiene que notificar al Departamento de Salud y Servicios Humanos inmediatamente. Al realizar su plan, tome en cuenta las regulaciones pertinentes a su industria.

Al considerar el respaldo de información, piense en grande. Algunas de las soluciones a considerar para asegurar que su información y sistemas pueden recuperarse con pérdidas mínima son múltiples centros de datos ubicados estratégicamente en diferentes regiones o una solución en la nube.





Situación 2: Pérdida del edificio

Los planes de contingencia y continuidad de negocio deben incluir situaciones como la pérdida total o parcial del edificio. Por ejemplo:

- Daños por incendios.
- Derrame de productos químicos que son un riesgo a la salud.
- El edificio se encuentra en un área activa donde se cometió un delito.
- Protestas (o en casos más extremos, motines) que impiden el ingreso al edificio y son un riesgo para la seguridad de sus empleados.

Los planes de recuperación de desastres deben incluir sitios alternos de trabajo. El plan ideal sería implementar un plan para trabajar desde casa ya que es una opción fácil para los empleados y rentable para el negocio y se cuentan con los recursos tecnológicos para empresas y consumidores. Cualquiera sea la opción que decida, en ambos casos será necesario que los empleados tengan la habilidad de acceder a las aplicaciones, sistemas y datos de manera remota y segura durante un evento de emergencia.

Situación 3: Pérdida de recursos tecnológicos

En este ámbito de rápida evolución tecnológica, muchas organizaciones dependen de aplicaciones externas para sus diferentes departamentos como contabilidad, informática, mercadotecnia digital y recursos humanos. El plan de contingencia y continuidad de negocio debe considerar las situaciones en las que estas aplicaciones externas pueden disolverse o dejar de prestar servicios esenciales. Las empresas deben tener preparada una lista alternativa de proveedores y tener un plan de contingencia en caso de ser necesario migrar la información para minimizar su dependencia en un solo proveedor.





Situación 4: Pérdida de recursos humanos

La pérdida de personal crítico impacta de manera significativa cualquier negocio, especialmente si no existen reemplazos o no tienen la capacitación para realizar otras responsabilidades esenciales. Se recomienda que las empresas capaciten a su personal para que puedan apoyar en otras responsabilidades y desempeñar procesos críticos en una situación de emergencia.

Al momento de estar elaborando su plan de gestión de la continuidad de negocio, debe tomar en cuenta cada aspecto que pueda afectar su negocio. Esto puede ser problemático al momento de considerar los sucesos del "cisne negro", que son eventos sorpresivos. Por ejemplo, no se sabe si un terremoto va a causar un tsunami o una epidemia en un país pueda convertirse en una pandemia que afecta todo el mundo. Lo mejor que puede hacer, y lo que debe hacer, es considerar los escenarios que se mencionan anteriormente y utilizarlos de la mejor manera para planear todos los escenarios que pueden afectar su negocio en caso de un desastre, sin importar su origen. Enfóquese en lo que puede controlar y podrá prepararse para los eventos inesperados que no puede controlar.

Capítulo 3

Análisis de impacto de negocio

Una vez que haya identificado los riesgos a su negocio, es tiempo de realizar un análisis de impacto o BIA por sus siglas en inglés. Esto implica:

Identificar los procesos afectados por ciertos eventos.

Identificar el tipo de pérdida (financiera, de productividad, de reputación).

Cuantificar las pérdidas potenciales.

Establecer un objetivo de punto de recuperación (RPO, por sus siglas en inglés) que especifique la cantidad máxima tolerable de pérdida de datos en caso de un fallo o desastre.

Establecer un objetivo de tiempo de recuperación (RTO, por sus siglas en inglés) que especifique la máxima cantidad de tiempo tolerable que un sistema o procesos puede estar inactivo después de un fallo o desastre.

Ejemplo: Comercio en línea

Su sitio de comercio en línea recientemente ha sido víctima de un ataque de denegación de servicios (DDos, por sus siglas en inglés). ¿Qué tipo de pérdidas puede esperar mientras trabaja en recuperar el sistema?

Tipos de pérdida



Financiera

Pérdida de ingresos de clientes que tenían órdenes pero que la información de la orden no fue respaldada, y de aquellos clientes que podrían haber realizado órdenes, pero no podían acceder al sitio.



Reputación

Clientes insatisfechos al no poder ordenar artículos o al no recibirlos debido a que su orden fue parte de la pérdida de información.

Cuantificación del impacto



RPO

La información de las compras debe respaldarse inmediatamente, especialmente si hay intercambio de dinero. Si la información actual de la compra no se encuentra al día, esto podría causar una interrupción significativa en el negocio.

RTO



En una situación ideal, le gustaría recuperar el sistema en unos segundos; sin embargo, si el sitio no se puede acceder por más de 15 minutos, el negocio puede tener una pérdida financiera significativa.



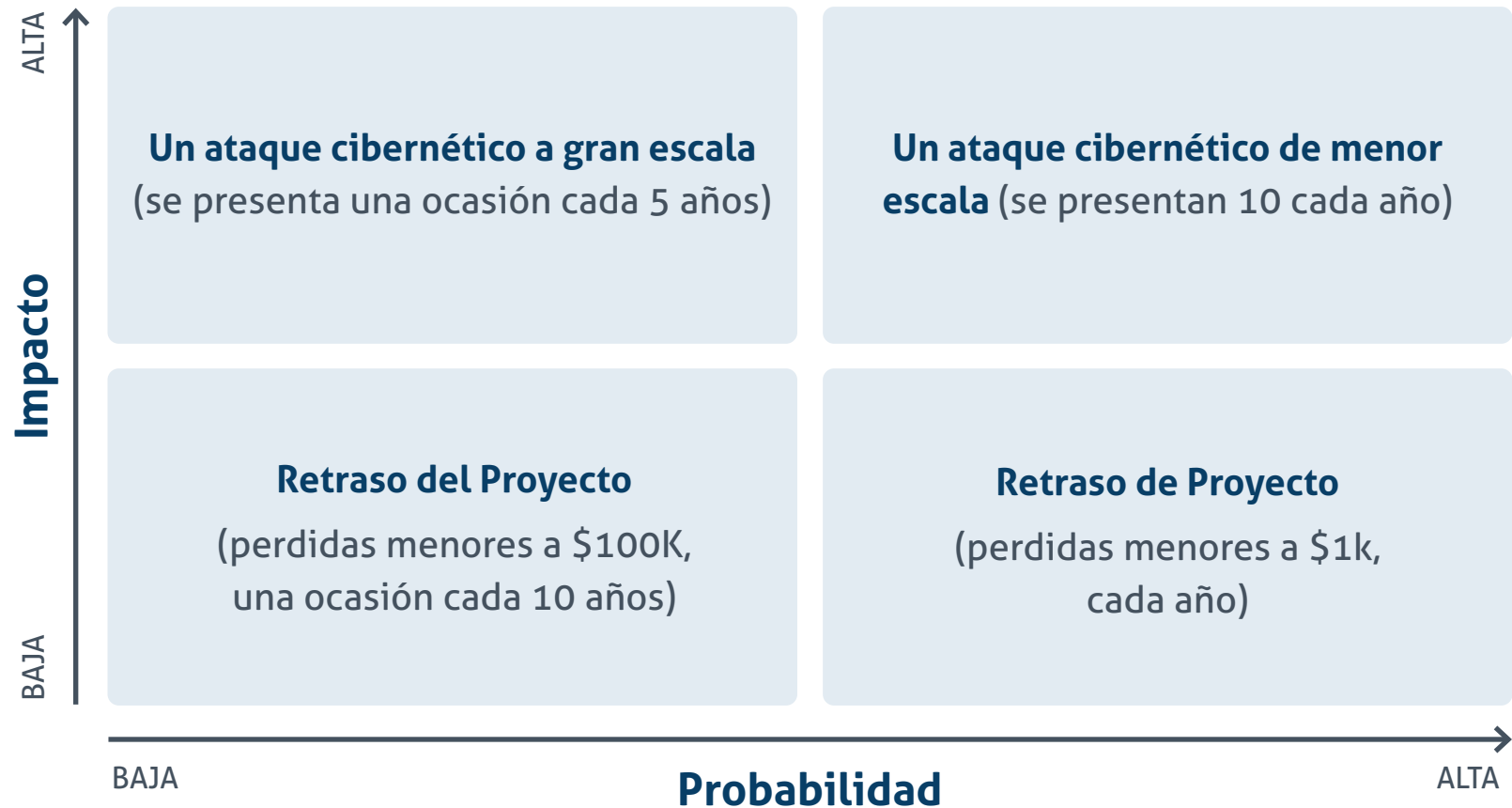
Nivel de la pérdida

Si no se cumplen con los valores de objetivo de punto de recuperación y objetivo de tiempo de recuperación (RPO y RTO), el negocio podría perder más de un valor estimado de un USD\$1 millón en ingresos, y podría tardar hasta un año para recuperar el nivel de reputación que tenía.

Capítulo 4

Gestión de prioridades

Si busca la perfección y se enfoca en los pequeños detalles, entonces su negocio puede estar en serios problemas. Una manera en la que puede priorizar apropiadamente dentro de su estrategia de gestión de continuidad de negocio es crear un gráfico, como el que se muestra abajo, [difundido por la asociación en el gobierno las Tecnologías de la Información, ISACA](#).



El gráfico muestra cuatro diferentes categorías en las que un negocio puede ser impactado:

Bajo impacto/baja probabilidad:

Para la mayoría de las empresas, es inevitable tener retrasos en ciertos proyectos, en algunos casos. Aún con la posibilidad de pérdida de ingresos, es poco frecuente, y su tolerancia para estas pérdidas puede ser alta.

Alto impacto/baja probabilidad:

Un ataque cibernético a gran escala que tiene efectos devastadores en su negocio. Aunque poco probable, asegúrese de que su negocio esté preparado para este tipo de evento.

Bajo impacto/alta probabilidad:

Retrasos en proyectos pueden tener bajo impacto, pero si son frecuentes pueden acumularse con el tiempo hasta ser una pérdida considerable.

Alto impacto/alta probabilidad:

Los ataques cibernéticos de menor escala que pueden en sí tener efectos devastadores a su negocio y tiene la probabilidad de ser más frecuentes. Aumente su infraestructura de informática y tecnología para protegerse de estos ataques.

Capítulo 5

Recuperación ante desastres

La recuperación ante desastres por lo general se centra en tener planes detallados de cómo recuperar sus sistemas, datos y aplicaciones. Al realizar una auditoría interna, o si emplea a un tercero, su plan debe incluir lo siguiente:



Su ubicación geográfica



El giro de su negocio

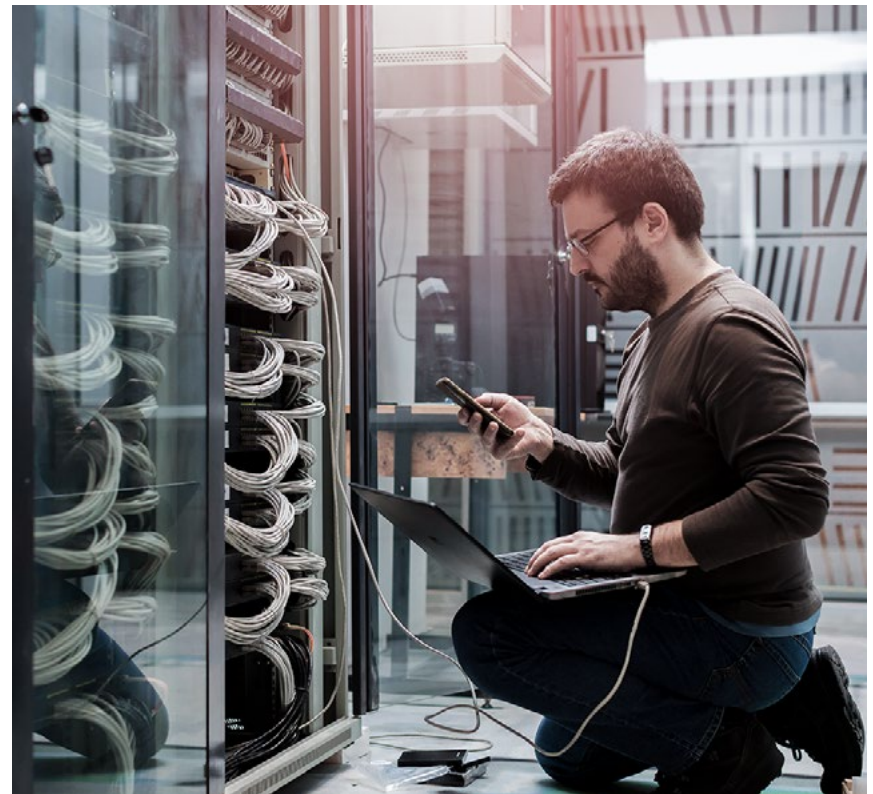


Cualquier marco legal o regulatorio

Ejemplo: Finanzas

Digamos que tiene una agencia financiera ubicada en Los Ángeles. El sector financiero implica múltiples marcos de cumplimiento normativo que requieren que se mantengan registros de maneras muy específicas. Además, como la agencia está en Los Ángeles, tiene el riesgo de desastre naturales por los terremotos.

Dado estas circunstancias, debe asegurarse de que sus centros de datos estén respaldados (para evitar multas si el centro de datos sufre daños o destrucción) y también debe considerar la opción de que los centros de respaldos estén ubicados en otro lugar (por ejemplo, un centro de respaldo de datos en Wyoming, puede ser menos susceptible a terremotos).



Capítulo 6

RPO y RTO

Los valores de RPO y RTO debe delinearse en su Análisis de riesgos de negocio y se deben describir los pasos para lograrlos en su plan.

Cualquier estrategia toma un tiempo promedio de implementación, así que es importante que considere las estrategias que estén dentro de los parámetros de RPO y RTO.

Como se muestra en el gráfico a continuación, mantener varias de sus instancias de servicio operando (clúster activo-activo) es una de las estrategias más rápidas, ya que, si una instancia de su servicio falla, la otra está ya activa. La medida más lenta sería tener un sistema que pueda activar manualmente como respaldo (también conocido como espera pasiva)

En términos de RPO, la duplicación en tiempo real de su información (una funcionalidad común que se incluye actualmente con las soluciones en la nube) puede restaurar sus datos de hasta segundos atrás, mientras una copia de un momento específico (snapshot) puede no estar al día y no llenar los requisitos para su RPO.



Capítulo 7

Planeación para la continuidad de negocio

Una parte esencial de la planeación para un plan de continuidad de negocio, es los pasos a seguir para continuar con un proceso de negocio específico en el evento de una falla o interrupción. Los planes de continuidad de negocio pueden y deben incluir pasos a seguir en casos de interrupciones en todos los niveles, desde un fallo en su plataforma de automatización de mercadotecnia, a situaciones dónde el edificio es inaccesible.

Ejemplo: Contabilidad

El pago de nómina a tiempo a los empleados es un proceso crítico de cualquier negocio. ¿Cuáles son los pasos a seguir en el caso de que el departamento de contabilidad no pueda acceder al sistema electrónico de contabilidad? Su plan de continuidad de negocio debe detallar el proceso:

- Obtener la información de la nómina del año pasado.
- Confirmar con la gerencia cualquier cambio en la nómina desde el último período.
- Expida la nómina basada en estos números; esto puede incluir generar los cheques.
- Trabaje con el banco para facilitar la transferencia automática de la nómina hasta que el sistema esté en línea nuevamente.



Si el proceso solo se verá interrumpido por un corto tiempo, ¿es necesario escribir manualmente los cheques? La decisión final queda a la discreción de las necesidades de su negocio, pero puede ser buena idea tener un RTO para cuando sea necesario hacer la transición a un proceso manual.

Capítulo 8

Gestión de la crisis

La gestión de la crisis consiste principalmente en realizar decisiones ejecutivas, aquellas que de manera tranquila aseguran el comando y control sobre el caos que permea durante una crisis. Esto involucra manejar la seguridad y bienestar de los empleados, al mismo tiempo que desarrollar la estrategia de comunicación interna y externa de la empresa. Su estrategia de gestión de crisis puede incluir lo siguiente:

Crear un equipo de gestión de crisis para tomar y reforzar las decisiones durante la crisis.

Tener una guía que el equipo pueda utilizar para asegurarse que están cubriendo todas las necesidades.

Desarrollar una estrategia de relaciones públicas y comunicación interna.

Estudio de caso: Derrame de petróleo de BP

En el 2010, British Petroleum enfrentó una crisis de gran escala, después de que una explosión en una de sus plataformas de petróleo dejó 11 muertos y causó uno de los derrames de petróleo más grandes en el Golfo de México. Durante este evento desastroso el CEO de BP, Tony Hayward, comentó "solo quiero mi vida de regreso", mientras 3 millones de litros se derramaban en el Golfo por las costas de Luisiana. Este comentario parecía ignorar las dificultades de la población en Luisiana y la trágica muerte de sus empleados. Estos comentarios, al igual que los intentos continuos de minimizar la seriedad del accidente y los impactos ambientales que causaría, tenía a los críticos furiosos y también enfurecieron a un ex empleado de BP que le grito al televisor cuando escuchó el comentario del CEO.

La reputación de la empresa todavía no se recupera del todo, a pesar de los años; sin embargo, la empresa tomó medidas para controlar la crisis, aunque un poco tarde. Primero, reclutó a Glenn DaGian, el ex empleado que había gritado al televisor y originario de Luisiana, un detalle sumamente importante para asegurarle a los residentes de Luisiana que BP estaba trabajando en resolver el problema. Escoger a alguien que entendía la cultura local de las comunidades afectadas, ayudó a la empresa tener un mejor entendimiento del impacto social del desastre.



Para mejorar la estrategia de comunicación, remplazaron a Tony Hayward con un originario de Mississippi, Bob Dudley. Rápidamente la empresa inició una campaña en las redes sociales para comunicarse directamente con el público, no para disculparse como el CEO anterior lo había hecho, si no para proveer actualizaciones y dar un poco de contexto sobre cómo estaban controlando la situación de la mejor manera posible. Esto también abría un espacio para que el público en general plasmara sus frustraciones. Steve Marino, asesor para BP que impulsó los esfuerzos de la campaña publicitaria en las redes sociales, explica que las plataformas sociales "permitieron que el público sintiera que BP los escuchaba, y de hecho BP sí escuchaba".

Es claro que BP no tenía una guía o estrategia de gestión formal para este tipo de emergencia; sin embargo, sus errores iniciales y las lecciones que aprendieron de ellos muestran la importancia de tener una estrategia para encontrar al personal adecuado que comparta el mensaje apropiado durante una crisis para gestionarla eficientemente.

Capítulo 9

Ejecución de pruebas

Para saber si el plan que se ha creado es el adecuado necesita realizar pruebas. Es necesario probar los planes especialmente aquellos que tienen un alto impacto en su negocio. El objetivo de las pruebas debe ser:

Verificar que su plan de continuidad de negocio es el apropiado.

Evaluar el desempeño del personal en este tipo de situación.

Evaluar la coordinación entre los equipos de trabajo y terceros.

Determinar el desempeño y capacidad de los sitios de respaldo en una simulación del evento.

Ejemplo: Pandemia Global

En caso de que se presente una nueva enfermedad, altamente contagiosa que se propaga rápidamente, tal vez sea necesario cerrar sus oficinas para prevenir infecciones o tal vez tenga que cerrar las oficinas por recomendación del gobierno para evitar la propagación. En tales casos, facilitar que sus empleados trabajen desde casa puede ayudar con las operaciones. Para realizar pruebas de esta estrategia, podría tener a sus empleados trabajar desde casa por un día para evaluar el plan en base a sus objetivos:

Verifique que el plan de continuidad de negocio sea el apropiado:

¿El tener al personal laborando desde casa mantiene las operaciones?

Mida el desempeño en este tipo de situación

¿El personal tiene los recursos necesarios para llevar a cabo sus tareas esenciales?

Evalúe la coordinación de equipos de trabajo y terceros:

¿El personal tiene las herramientas necesarias para comunicarse y tener juntas? ¿Podrá tener una comunicación efectiva con proveedores, clientes, o los medios de comunicación?

Determine el desempeño y capacidad de los sitios de respaldo en una simulación del evento:

¿Logra los objetivos de RPO y RTO en caso de la interrupción de sus aplicaciones, servicios y datos?

Además de las pruebas y auditorías que conduzca internamente, se recomienda o será necesario tener sus planes auditados por terceros. Existen estándares regulatorios a los cuales su negocio tal vez necesite adherirse como el estándar ISO 22301, FPNA 1600, y ISACA CISA Dominio 2 Gobierno y gestión de las Tecnologías de la Información (TI). El objetivo de estas auditoria es:

Comprender la conexión entre el plan de continuidad de negocio y los objetivos del negocio.

Determinar si el plan de continuidad de negocio es satisfactorio y está actualizado.

Revisar los planes de ejecución de pruebas para verificar la efectividad del plan de continuidad de negocio propuesto.

Visitar o evaluar los sitios de almacenamiento fuera del sitio o en la nube.

Evaluar la habilidad de respuesta afectiva del personal al evento de emergencia.

Concluir con las pruebas del plan no significa que ha terminado con el proceso. Desarrollar y realizar pruebas a los planes de contingencia y continuidad de negocio son procesos repetitivos, siempre están evolucionando y existe la posibilidad de revisar su estrategia.

Capítulo 10

ECM y la nube como parte del plan de continuidad de su negocio

Las empresas que gestionan su contenido en la nube tienen una gran ventaja en caso de desastres. Con la gestión de contenido empresarial (ECM), software diseñado para gestionar digitalmente contenido y procesos en una organización, las empresas pueden continuar con sus operaciones en las condiciones más extenuantes. Tener la certeza de que sus empleados pueden acceder a su trabajo desde cualquier lugar y en cualquier momento es mucho más que solo una conveniencia, puede ser de vital importancia para las empresas en tiempos de incertidumbre.

Contar con un sistema de ECM como parte su plan de continuidad de negocio es una opción para que usted pueda rápidamente reaccionar ante desastres o fallos al:

- **Habilitar un lugar de trabajo digital con la tecnología de la nube**, lo que permite que los empleados puedan acceder a la información y procesos necesarios para llevar a cabo sus tareas y asegurar que el negocio continúe con sus operaciones.
- **Proveer funcionalidades de control de versión o edición colaborativa de documentos** para que puedan trabajar en las versiones actualizadas de los documentos.
- **Ofrecer servicios en línea a clientes, usuarios, y proveedores** para que ellos tengan toda la información necesaria, sin la necesidad que tener un lugar físico abierto.
- **Automatizar procesos esenciales que aseguran la estandarización, consistencia y continuidad** para proveer tranquilidad a los empleados de que los procesos pueden seguir corriendo sin problemas.

¿Está listo para ver en acción la gestión de contenido electrónico de Laserfiche?

Visite nuestra página de testimonios o solicite una demostración para conocer más sobre cómo la gestión de contenido electrónico puede ayudarle a tener visibilidad en el desempeño de su negocio, al mismo tiempo que le permite atender a sus clientes cuando más lo necesitan.

**Solicite una
demostración**

**Vea casos de
nuestros clientes**



Acerca de Laserfiche

Laserfiche es el proveedor global líder de gestión inteligente de contenido y automatización de procesos comerciales. Mediante poderosos flujos de trabajo, formularios electrónicos, gestión de documentos y analítica, la plataforma Laserfiche elimina los procesos manuales y automatiza las tareas repetitivas, acelerando la forma en que se hacen los negocios.

Laserfiche fue pionera en el concepto de oficina sin papel con la administración de contenido empresarial desde hace más de 30 años. Hoy, Laserfiche está innovando con la nube, el aprendizaje automático y la inteligencia artificial para permitir a las organizaciones en más de 80 países transformarse en negocios digitales. Clientes en todas las industrias, incluyendo gobierno, educación, servicios financieros y manufactura, usan Laserfiche para aumentar la productividad, escalar sus negocios y ofrecer experiencias digitales de primer nivel.

Los empleados de Laserfiche en oficinas de todo el mundo están comprometidos con la visión de la compañía de empoderar a los clientes e inspirar a las personas a re-imaginar la manera en que la tecnología puede transformar vidas.

Conozca más sobre Laserfiche:

