Continue

Plan de continuidad del negocio

Latest products and innovations across Cisco Power your metro, core, and data center networks with Silicon One-based platforms built for the speed and scale of AI. Explore Cisco 8000 Series Cisco AI Defense safeguards the development and usage of AI applications so that enterprises can advance their AI initiatives with confidence. * Gartner®, Magic Quadrant™ for Digital Employee Experience Management Tools, Dan Wilson, Tom Cipolla, Stuart Downes, Autumn Stanish, Lina Al Dana, 26 Agosto 2024 **Gartner®, Magic Quadrant™ for Desktop as a Service, Stuart Downes, Eri Hariu, Mark Margevicius, Craig Fisler, Sunil Kumar, 16 de Septiembre de 2024GARTNER® es una marca comercial registrada y una marca de servicio de Gartner, Inc. y/o sus filiales en los EE. UU. y a nivel internacional, y MAGIC QUADRANT™ es una marca comercial registrada de Gartner, Inc. y/o sus filiales y se utilizan aquí con permiso. Todos los derechos reservados. Gartner® no respalda a ningún proveedor, producto o servicio descrito en sus publicaciones de investigación, y no aconseja a los usuarios de tecnología que seleccionen solo a los proveedores con las calificaciones más altas u otra designación. Las publicaciones de investigación de Gartner® consisten en las opiniones de la organización de investigación de Gartner y no deben interpretarse como declaraciones de hechos. Gartner® renuncia a todas las garantías, expresas o implícitas, con respecto a esta investigación, incluidas las garantías de comerciabilidad o idoneidad para un propósito en particular. AXA Car insurance is tailored to your needs. Get your car insurance quote. And if you've got more than one car registered at your home address, check out our MultiCar discount. With AXA Landlord Insurance, you get the core protection you need, including building insurance and property owners' liability cover. Our landlord insurance has you covered. If you rely on a van to keep your business running smoothly, you can tailor your insurance cover to suit your needs with AXA Van Insurance. Get your van insurance quote. Un plan de continuidad de negocio (PCN o BCP por Business Continuity Plan), también conocido como plan de continuidad operativa o plan de contingencia, es un conjunto de estrategias y acciones diseñadas para asegurar que una organización pueda continuar funcionando de manera efectiva y minimizar el impacto de eventos disruptivos o desastres que puedan afectar su operación normal. Los eventos que podrían requerir la activación de un PCN incluyen desastres naturales, como terremotos, inundaciones o huracanes, ciberataques, incendios, pandemias, interrupciones en la cadena de suministro, entre otros. ¿Qué es un plan de continuidad de negocio? El PCN debe ser un documento estructurado y completo que incluya una evaluación detallada de riesgos, un análisis de impacto en el negocio, una estrategia de respuesta, planes de recuperación y de comunicación, roles y responsabilidades del personal, así como mecanismos para revisar y mantener actualizado el plan en función de los cambios internos y externos que afecten a la organización. Su objetivo principal es permitir que la empresa se recupere rápidamente y siga operando, o al menos mantenga funciones críticas, en situaciones adversas o emergencias. Para ello debe enfocarse en identificar y evaluar los riesgos y amenazas que podrían afectar a la organización. Una vez realizado ese punto hay que desarrollar las estrategias necesarias para prevenir, mitigar y responder eficazmente a esos eventos. Importancia de contar con un plan de continuidad de negocio Un PCN bien diseñado puede ayudar a proteger la reputación de la empresa, minimizar pérdidas financieras, garantizar la seguridad de los empleados y mantener la confianza de los clientes, socios y otras partes interesadas. Es una herramienta esencial para la gestión de riesgos y la resiliencia empresarial. Cada organización debe adaptar su plan de continuidad a sus necesidades y características específicas, considerando los riesgos a los que está expuesta y las operaciones críticas que no pueden detenerse en ninguna circunstancia. Aunque en algunos sectores y países la existencia de un PCN puede ser un requisito legal o regulatorio para operar, razones como garantizar la continuidad de ingresos o proteger la cadena de suministro hacen que contar con un PCN sea de suma importancia para cualquier organización. Es fundamental que todas las partes interesadas, desde la alta dirección hasta los empleados, estén familiarizadas con el PCN y se realicen periódicamente pruebas y/o ejercicios para asegurar que el plan esté actualizado y sea efectivo en situaciones de crisis. De esta manera se minimiza el impacto de las interrupciones, ya que permite a la empresa anticiparse y prepararse para los eventos adversos, evitando pérdidas financieras significativas. Gracias a ello, la empresa demuestra su capacidad de respuesta y compromiso con sus clientes, proveedores y otras partes interesadas, lo que contribuye a mantener su reputación positiva. También asegura el bienestar de los empleados durante situaciones de emergencia, lo que crea un ambiente de trabajo seguro y protege al personal. Características de un plan de continuidad de negocio eficaz Si bien es imposible predecir todos los eventos que podrían afectar a una organización, para que un PCN sea eficaz y asegurar así el éxito y capacidad de respuesta ante situaciones de crisis de una organización debe de incluir: Una meticulosa evaluación de riesgos y sus análisis de impacto, para enfocar los esfuerzos en las áreas más vulnerables y priorizar las acciones necesarias. Esta evaluación debe de estar continuamente en revisión Un plan de respuesta a emergencias detallado que establezca los procedimientos específicos y claros para responder adecuadamente ante situaciones de crisis es crucial. Este plan debe incluir la activación de equipos de respuesta, la coordinación de esfuerzos y la toma de decisiones efectivas en momentos de emergencia. Un plan sólido para la recuperación de las operaciones y funciones esenciales del negocio después de una interrupción es fundamental. Debe definir las estrategias y los pasos a seguir para restablecer gradualmente las actividades y minimizar el tiempo de inactividad. ¿Qué fases se han de tener en cuenta al elaborar un plan de continuidad de negocio (PCN) Al elaborar un PCN, es importante seguir un enfoque estructurado y sistemático que abarque diversas fases para garantizar que el plan sea completo y efectivo. Evaluación de riesgos El PCN debe incluir una evaluación exhaustiva de los riesgos que pueden afectar a la organización, considerando tanto amenazas internas como externas. Hay que realizar un análisis detallado en el que se identifique las funciones y operaciones críticas para el negocio, así como los posibles impactos financieros y operativos en caso de interrupciones. Estos riesgos hay que priorizarlos para centrar los esfuerzos en aquellos más críticos y probables. Análisis de impacto Esta etapa es crucial para la creación del plan. Su objetivo principal es entender cómo afectaría al funcionamiento de la organización los diferentes escenarios encontrados en la fase anterior. Para ello lo primero es identificar cuáles son las funciones y procesos esenciales de la empresa, incluyendo todos los departamentos, y establecer para cada una de ellas el tiempo máximo de inactividad y analizar las dependencias entre las diferentes funciones y procesos. También es imprescindible cuantificar las pérdidas potenciales asociadas a la interrupción, como pueden ser, pérdidas de ingresos, costes adicionales, penalizaciones contractuales, ... Una vez identificado lo anterior, hay que desarrollar los escenarios específicos para ilustrar cómo los riesgos evaluados pueden afectar a las funciones críticas. Facilitando así la comprensión y planificación de las etapas siguientes. Documentación Con miras a las siguientes fases es importante realizar dos documentos clave: Informe de evaluación de riesgos y Perfiles de Funciones Críticas, donde se vinculen los riesgos con las funciones y los impactos. Estrategias de prevención y mitigación Esta etapa consiste en desarrollar medidas para reducir la probabilidad de que ocurran los eventos disruptivos y minimizar así su impacto negativo en nuestra organización. Se deben proporcionar procedimientos específicos y detallados para cada situación de crisis identificada, incluyendo pasos a seguir, roles y responsabilidades del personal y acciones a tomar. Se recomienda ser flexible en los procedimientos para así poder adaptarse a situaciones cambiantes. Plan de respuesta a emergencias El plan de respuesta es una parte integral de un PCN y se centra en las acciones específicas que se deben tomar cuando ocurre una interrupción. Incluyendo la activación de equipos de respuesta, las comunicaciones tanto internas como externas, la coordinación de esfuerzos y la toma de decisiones efectivas en momentos de emergencia. En esta fase se incluyen también la realización de simulacros periódicos para la evaluación del plan de respuesta y la mejora continua. Plan de recuperación El plan de recuperación se centra en las estrategias y procedimientos para restaurar las operaciones normales después de que una interrupción haya ocurrido. El primer paso es tener claros los objetivos de recuperación para establecer metas cuantificables en términos de tiempo, datos y funcionalidad. En él hay que definir las funciones críticas en función de su importancia, para así priorizar su recuperación en consecuencia. Para ello hay que enumerar los recursos necesarios para la recuperación, estableciendo prioridades según la criticidad, y desarrollar los procedimientos para la recuperación de cada función crítica, especificando como se realizará la restauración de los sistemas informáticos y la integridad de los datos, utilizando copias de seguridad o sistemas redundantes. También hay que definir los roles y las responsabilidades del personal encargado de la recuperación, establecer protocolos de comunicación y coordinación tanto para socios, como para clientes y proveedores, así como de información y formación para el personal. Al igual que en el plan de respuesta a emergencias, en el plan de recuperación también hay que realizar pruebas regulares para asegurarnos de que los procedimientos son efectivos y eficientes, por ello es importante documentar todas las acciones efectuadas durante el proceso de recuperación para la mejora continua. Al seguir estas fases, se logra un PCN sólido y completo que ayuda a la organización a estar preparada para enfrentar situaciones de crisis y mantener su funcionamiento en circunstancias adversas. Hoy en día, las empresas dependen más que nunca de los datos y la conectividad, lo que las hace más vulnerables a interrupciones inesperadas.La encuesta de PwC sobre crisis y resiliencia global de 2023 reveló que el 96 % de los líderes empresariales han experimentado interrupciones en los últimos dos años. Y lo que es aún más preocupante, el 76 % afirmó que su peor interrupción afectó gravemente a las operaciones.Y aquí está la cuestión: no hace falta un ciberataque masivo para causar el caos. A veces, basta con un solo archivo comprometido o una pequeña brecha de seguridad para desbaratar todo. Por eso, el Foro Económico Mundial clasifica los ciberataques y las violaciones de datos entre los 10 principales riesgos empresariales a nivel mundial.¿La clave para mantenerse a la vanguardia? Un plan de continuidad de negocio (BCP) sólido que mantenga a su equipo preparado, sus operaciones en funcionamiento, los activos de la empresa protegidos y las interrupciones bajo control.Profundicemos en lo que realmente significa la continuidad del negocio, por qué es esencial y cómo construir un plan que realmente funcione.Un plan de continuidad de negocio es un plan que ayuda a las empresas a seguir operativas durante interrupciones como ciberataques, fallos en la cadena de suministro o crisis financierasLas empresas utilizan los BCP para fallos informáticos, pandemias, recesiones económicas y ciberamenazasLa creación de un plan de continuidad de negocio implica identificar riesgos, planificar la recuperación, probar el plan y mantenerlo actualizadoLos ejemplos reales de continuidad empresarial muestran cómo empresas como Netflix y Ford gestionaron eficazmente las crisis mediante una planificación proactiva y la gestión de riesgosEl intervalo de funciones de ClickUp (y plantillas gratis, gratuitas), como Tareas, Paneles, Documentos, Brain y Automatizaciones, hacen que el BCP sea más ágil que nuncaUn plan de continuidad de negocio (BCP) es un manual que ayuda a las empresas a mantenerse en funcionamiento cuando se producen interrupciones inesperadas, como desastres naturales, fallos técnicos o errores humanos.Establece pasos claros para que las empresas sepan exactamente qué hacer en una crisis. Esto garantiza que las operaciones, los empleados y los socios sigan su curso con una interrupción mínima.Un plan de continuidad prepara a las organizaciones para riesgos como ciberataques, pandemias y cortes de energía o de TI. No hace falta decir que un plan bien definido es crucial para proteger la estabilidad, la reputación y el intento correcto a largo plazo de una empresa. ¿Sabías que...? Para la mayoría de las empresas medianas y grandes (más del 90 %), cada hora de inactividad cuesta más de 300 000 $. Esto supone un gran impacto en términos de productividad, confianza de los clientes, equipo de ventas e incluso sanciones por incumplimiento.Un plan de continuidad de negocio sólido necesita algunos elementos clave para ser eficaz:La pérdida de datos críticos puede paralizar las operaciones en un instante. Las copias de seguridad periódicas, tanto in situ como fuera de las instalaciones, mantienen la información segura y accesible. Configure copias de seguridad automatizadas, pruebe los pasos de recuperación y familiarice a su equipo con el proceso para evitar confusiones cuando sea necesario.En una crisis, todos deben conocer su rol. Asigne responsabilidades clave, mantenga actualizadas las listas de contactos y establezca una forma clara de transmitir la información. Disponga de múltiples canales de comunicación (correo electrónico, teléfono, apps de mensajería) para que no haya confusión cuando se necesiten decisiones rápidas.Las amenazas se presentan de muchas formas: desastres naturales, ciberataques, fallos del sistema y errores humanos. Identificar los puntos débiles a tiempo ayuda a reducir los daños antes de que se agraven. Un plan proactivo hoy puede ahorrar tiempo, dinero y frustración en el futuro.Un plan que no se pone a prueba no es más que papel mojado. Realice simulacros con regularidad, forme a su equipo y modifique las cosas a medida que su empresa evolucione. Los cambios tecnológicos, los cambios de personal y los nuevos riesgos surgen, por lo que mantener el plan actualizado significa que siempre va un paso por delante.¿La meta? Menos tiempo de inactividad, menos estrés y una empresa que se mantenga fuerte pase lo que pase. Consejo profesional: Cree una tarjeta de puntuación de Análisis de Impacto en el Negocio (BIA) para cada departamento antes de fijar su BCP. Hágalo de forma sencilla: valore cada función de la empresa en una escala del 1 al 5 en tres áreas: impacto en los ingresos, experiencia del cliente y dependencia operativa. Si una función obtiene una puntuación de 12 o más, es una operación crítica y debe tener la máxima prioridad cuando las cosas vayan mal.Cuando se produce una catástrofe, ¿cómo de preparada estaría su empresa? Cada crisis exige un plan de acción diferente, desde ciberataques hasta desastres naturales.Aquí hay cinco ejemplos reales de planes de continuidad de negocio que muestran cómo las empresas inteligentes manejan las crisis y los pasos clave para construir su propio plan de continuidad de negocio.Un plan de recuperación ante desastres de TI es un proyecto de estrategias, procedimientos y protocolos, incluidos aspectos de planificación de la capacidad de TI, diseñado para ayudar a las empresas a restaurar su infraestructura y operaciones de TI después de eventos disruptivos como ciberataques, fallos de hardware o errores humanos. Ejemplo real: Uno de los mejores ejemplos de continuidad empresarial, el BCP de Netflix, se puso a prueba durante la interrupción de AWS en 2011. En lugar de depender de un único punto de fallo, construyeron un sistema utilizando servicios sin estado, replicación de datos entre zonas y redundancia para mantener las operaciones en funcionamiento. ¡Es uno de los mejores ejemplos de plan de continuidad empresarial! Copia de seguridad y restauración: Realice copias de seguridad periódicas para poder restaurar rápidamente los datos cruciales cuando sea necesario Recuperación basada en la nube: confíe en los servicios en la nube para obtener opciones de recuperación flexibles y escalables Respuesta a incidentes: Disponga de un plan paso a paso para detectar, analizar y recuperar sus servicios críticos de los problemas (¡invierta en software de gestión de incidencias!) Redundancia: Duplique los sistemas para evitar fallos (no ponga todos los huevos en la misma cesta)Un plan de respuesta ante una pandemia ayuda a las empresas a mantener el seguimiento durante los brotes de enfermedades infecciosas. Se centra en mantener a los empleados seguros, compatibilidad con el teletrabajo, reforzar la cadena de suministro y mantener una comunicación fluida.Este ejemplo de plan de continuidad de negocio se desarrolla en tres fases:1️⃣ Antes de la pandemia: Esta es la fase de preparación. Usted planifica, prueba y ajusta su plan de continuidad de negocio para que todo esté listo. 2️⃣ Durante la pandemia: Es hora de poner el plan en acción, manteniendo las operaciones en funcionamiento con una interrupción mínima. 3️⃣ Después de la pandemia: Una vez que las cosas se calmen, revisará lo que funcionó, arreglará lo que no funcionó y hará que la empresa vuelva a funcionar a toda velocidad Ejemplo real: Cuando llegó la COVID-19, el plan de respuesta a la pandemia de Walmart se puso en marcha rápidamente. Protegieron a los empleados con bajas por enfermedad remuneradas, EPI y más, mientras mantenían las tiendas en funcionamiento con entregas sin contacto. Para mantener a los clientes seguros, redujeron el horario de las tiendas, aumentaron la desinfección e impusieron sitios de prueba de COVID-19 en los estacionamientos Coordinador de la pandemia: Designe un equipo específico y nombre a un jefe de equipo para supervisar la respuesta Políticas de teletrabajo: Configure sistemas de teletrabajo seguros para que los empleados puedan trabajar desde casa sin perder el ritmo Gestión de cuarentenas: Desarrollar protocolos para prohibiciones de viaje y cierres de fronterasUn plan de continuidad de la cadena de suministro es una estrategia que garantiza que la cadena de suministro de una empresa siga funcionando durante las interrupciones, como conflictos geopolíticos, ciberataques o fallos de los proveedores. Ayuda a las empresas a mitigar los riesgos, minimizar el tiempo de inactividad y mantener el flujo de bienes y servicios. Ejemplo del mundo real: Cuando el terremoto y el tsunami de Japón de 2011 golpearon, la cadena de suministro de Toyota sufrió un golpe significativo, pero su plan de continuidad los mantuvo en el juego. Se recuperaron más rápido que muchos competidores trabajando con proveedores de copia de seguridad, almacenando piezas críticas y correlacionando toda su cadena de suministro. ¡Hablemos de planificación organizativa! Identifique a los proveedores críticos: Haga una lista de todos los proveedores clave y evalúe sus niveles de riesgo (ubicación, estabilidad financiera, opciones alternativas) Diversificar los proveedores: Evitar la dependencia de un único proveedor o región mediante proveedores de copia de seguridad en diferentes ubicaciones Correlacione su cadena de suministro: Comprenda de dónde proviene cada pieza o material, incluidos los proveedores de nivel 2 y nivel 3 Almacenar inventario crítico: Mantener existencias de reserva de materiales esenciales para evitar la escasez durante las interrupciones Desarrollar planes logísticos de emergencia: Planificar rutas de envío y modos de transporte alternativos en caso de interrupcionesUn plan de gestión de crisis financieras ayuda a las empresas a afrontar recesiones económicas, escasez de liquidez y contratiempos financieros inesperados. Se centra en mantener el flujo de caja y asegurar una financiación alternativa para mantener las operaciones en funcionamiento. Algunas de sus acciones clave incluyen la identificación de riesgos financieros, la optimización de cuentas por cobrar y por pagar, la renegociación de contratos con proveedores y la priorización de gastos esenciales. Ejemplo real: Un gran ejemplo de un FCMP en acción es Ford durante la crisis financiera de 2008. Mientras que otros fabricantes de automóviles como GM y Chrysler necesitaron rescates gubernamentales, Ford había conseguido 23 500 millones de dólares en préstamos privados dos años antes. Esto les dio el colchón de efectivo para sobrevivir sin ayuda externa. Priorizar las operaciones críticas: Garantizar que la nómina, las cuentas por pagar/cobrar, el cumplimiento de las obligaciones fiscales y la gestión de ingresos no se vean interrumpidos Anticípese a los riesgos antes de que se produzcan: Identifique amenazas como la inestabilidad económica, los ciberataques y las multas reglamentarias. Utilice plantillas de planes de contingencia para correlacionar los riesgos y reforzar la resiliencia Protecciones técnicas seguras: Proteja los sistemas financieros basados en la nube, haga copias de seguridad de los datos críticos y proteja los activos clave, como las pólizas de seguro y los contratos con proveedores, de las ciberamenazasUn plan de respuesta ante incidentes de ciberseguridad es imprescindible, pero solo el 45 % de las empresas lo tienen. Ahora, la cuestión no es si se producirá un ataque, sino cómo estará preparado cuando lo haga.Es entonces cuando la gestión de riesgos de ciberseguridad, o respuesta a incidencias, se presenta como un enfoque estructurado para detectar, responder y recuperarse de las ciberamenazas. Garantiza que las funciones críticas de la empresa continúen con una interrupción mínima, incluso durante un ataque. Ejemplo real: Uno de los mayores avisos de alerta en ciberseguridad fue el ataque del ransomware WannaCry. Afectó al 34 % de los fideicomisos del Servicio Nacional de Salud (NHS) del Reino Unido, paralizando los sistemas. Identifique los activos clave: ¿Qué sistemas y datos críticos mantienen su empresa en funcionamiento? Protéjalos primero Realizar evaluaciones de riesgos: Evaluar periódicamente las vulnerabilidades y las brechas de seguridad mediante procesos como las pruebas de penetración Datos de copia de seguridad: Almacene copias de seguridad cifradas en ubicaciones seguras, como almacenamiento en la nube o unidades Probar el plan: Realizar simulacros de ciberseguridad para garantizar la preparación➡ Leer más: Plantillas de gestión del cambio gratis con ejemplos de planes Un plan de continuidad de negocio para la fabricación es un marco diseñado para garantizar que una empresa de fabricación pueda seguir operando durante y después de interrupciones, como desastres naturales, ciberataques, fallos en la cadena de suministro, averías en los equipos o escasez de mano de obra.En él se describen medidas preventivas, estrategias de respuesta ante emergencias y procedimientos de recuperación para minimizar el tiempo de inactividad y las pérdidas financieras, al tiempo que se mantiene la eficiencia de la producción. Ejemplo real: El ataque de ransomware de 2017 en EE. UU. golpeó con fuerza al gigante farmacéutico Merck & Co., paralizando las operaciones de fabricación, investigación y equipos de ventas. Los empleados perdieron el acceso al correo electrónico y 70 000 trabajadores se quedaron sin acceso a sus ordenadores. Conozca los procesos internos: Identifique los procesos y activos críticos (por ejemplo, maquinaria, cadenas de suministro, logística) Tenga una línea de comunicación directa: Desarrolle un plan claro de línea de comunicación para empleados, proveedores y partes interesadas Tener planes de seguridad: Implementar protocolos de seguridad y procedimientos de evacuación para emergencias in situ Mantener el cumplimiento: Garantizar el cumplimiento de las normativas de OSHA, medioambientales y del sector ClickUp Insight: Alrededor del 41 % de los profesionales prefieren la mensajería instantánea para la comunicación del equipo. Aunque ofrece intercambios rápidos y eficientes, los mensajes a menudo se distribuyen a través de múltiples canales, hilos o mensajes directos, lo que dificulta la recuperación de la información más adelante.Con una solución integrada como ClickUp Chat, sus hilos de chat se correlacionan con proyectos y tareas específicos, manteniendo sus conversaciones en contexto y fácilmente disponibles.Un plan de continuidad de negocio para la construcción ayuda a las empresas a estar preparadas, responder rápidamente y recuperarse sin problemas de las interrupciones sin que las operaciones o los ingresos se vean muy afectados.En la construcción, los contratiempos inesperados pueden desviar los proyectos, retrasar los cronogramas y provocar grandes pérdidas financieras. Si bien los desastres climáticos son un riesgo obvio, los problemas de la cadena de suministro y la escasez de mano de obra pueden ser igual de difíciles de manejar. Ejemplo real: Al-Thuwairat Construction Company se enfrentó a riesgos importantes, como las perturbaciones meteorológicas y los problemas de mano de obra, pero su mayor desafío fue la falta de un sistema claro para gestionar estos riesgos. Para solucionarlo, mejoraron la comunicación entre los departamentos e introdujeron un enfoque estructurado de evaluación de riesgos. Esto hizo que sus operaciones fueran más resistentes, ayudándoles a manejar las interrupciones sin descarrilar los proyectos. Planifique lo inesperado: Identifique riesgos como el mal tiempo, retrasos en la cadena de suministro o amenazas cibernéticas, y ponga en marcha planes de copia de seguridad para mantener los proyectos bajo seguimiento Tenga una estrategia de recuperación rápida: Establezca pasos claros para reubicar las operaciones, restaurar los datos y que los equipos vuelvan al trabajo lo antes posible Mantener a los equipos alineados: Asegúrese de que todos conozcan su rol durante las interrupciones con planes de respuesta bien ensayadosUn plan de continuidad de negocio para incidencias de seguridad física garantiza que esté preparado para manejar emergencias, proteger activos y volver a la normalidad rápidamente. Un buen plan cubre todo, desde la respuesta a emergencias hasta el cumplimiento y las evaluaciones de riesgos continuas para que su empresa se mantenga resiliente. Ejemplo real: Durante el huracán Katrina en 2005, los hospitales y las empresas de Nueva Orleans se enfrentaron a fallos masivos de seguridad física, con saqueos, cortes de electricidad y averías en las infraestructuras que empeoraron la situación. Aquellos que contaban con energía de copia de seguridad, planes de evacuación de emergencia y suministros almacenados lograron mantener en funcionamiento las operaciones limitadas. Alinearse con la recuperación de TI: Garantizar una integración perfecta con los planes de recuperación de desastres de TI para gestionar las interrupciones del sistema Manténgase en cumplimiento de la ley: Cumpla con las normativas de seguridad y los requisitos de (elaboración de) informes para evitar complicaciones legales Revise y mejore con regularidad: Evalúe continuamente los riesgos, actualice los protocolos y aplique las lecciones aprendidas de incidencias pasadas para estar preparadoUn corte de energía puede paralizar las operaciones de una empresa. Y lo que es peor, el corte puede prolongarse durante días. Con el plan de respuesta ante emergencias por corte de energía adecuado, puede mantener en funcionamiento las funciones críticas, minimizar las interrupciones y mantener la confianza de los clientes. Una estrategia bien preparada garantiza que su equipo sepa qué hay pendiente, qué recursos movilizar y cómo recuperarse rápidamente. Ejemplo real: Un corte de energía paralizó a Delta Air Lines en 2016, lo que obligó a cancelar miles de vuelos. En respuesta, la empresa invirtió en infraestructura de TI, construyó sistemas redundantes y mejoró los protocolos de comunicación para evitar interrupciones similares. Identificar funciones críticas: Determinar qué operaciones (sistemas informáticos, fabricación, servicio al cliente, etc.) son más vulnerables a los cortes de energía Soluciones de energía de copia de seguridad: invierta en generadores, sistemas SAI y fuentes de energía alternativas Plan de contingencia operativa: priorizar tareas, reasignar recursos y establecer flujos de trabajo para mantener la productividadUn plan sólido de gestión de crisis y retirada de productos es esencial para controlar emergencias como la contaminación de productos, problemas de seguridad o fallos en la cadena de suministro. Por ejemplo, si la FDA anuncia que un ingrediente de su producto no es seguro, es fundamental actuar con rapidez para proteger a los clientes, mantener la confianza y evitar problemas legales. Ejemplo real: Johnson & Johnson se enfrentó a una grave crisis en 1982 cuando sus cápsulas de Tylenol con cianuro provocaron varias muertes. La empresa retiró rápidamente 31 millones de botellas e introdujo envases a prueba de manipulaciones. Su rápida respuesta y transparencia restablecieron la confianza y llevaron a un intento correcto de relanzamiento del producto. Fortalecer el control de calidad: Realizar un análisis de la causa raíz para identificar lo que salió mal, reforzar los controles de seguridad y prevenir futuros contratiempos Comuníquese con confianza: Forme a un portavoz para que gestione con fluidez las preocupaciones de los medios de comunicación, los reguladores y los clientes Soporte a sus clientes: Organice sustituciones rápidas de productos o soluciones alternativas para mantener la confianza y minimizar las interrupcionesLas interrupciones inesperadas pueden afectarle en cualquier momento, pero un plan de continuidad de negocio sólido mantiene sus operaciones en funcionamiento sin problemas.A continuación, le indicamos cómo crear uno que proteja su empresa frente a lo inesperado Lo primero es lo primero: averigüe qué podría salir mal y cómo podría afectar gravemente a su empresa. Este paso le ayuda a identificar los riesgos, minimizar los daños y crear un plan para mantener las cosas en funcionamiento.Piense en amenazas potenciales como fallos del sistema, interrupciones en la cadena de suministro o ciberataques que podrían entorpecer sus operaciones. Establezca procesos empresariales transparentes para medir y gestionar estos riesgos, de modo que sepa lo que su empresa puede manejar y cuándo actuar. Consejo profesional: Identifique los riesgos potenciales y correlacione su impacto en plantillas de evaluación de riesgos predefinidas. Esto facilita la correlación de posibles amenazas, la colaboración con su equipo y mantener todo organizado en un solo lugarObtener plantilla gratis, gratuitaIdentifique y priorice los riesgos en función de su intensidad y probabilidad utilizando la plantilla de pizarra de evaluación de riesgos de ClickUpAverigüe qué partes de su empresa no pueden permitirse ralentizarse cuando una interrupción comienza a afectar a los clientes, los requisitos legales, las operaciones o incluso su reputación. Una vez que conozca los puntos de inflexión, puede elaborar un plan para minimizar los riesgos y recuperarse rápidamente.➡ Bonus: Cómo redactar un informe de incidencias en el trabajoUna vez que conozca los riesgos, cree un plan claro para manejar las interrupciones y mantener a todos informados.En resumen, incluye: Respuesta y gestión de emergencias: Actúe rápidamente para estabilizar la situación, proteger a las personas y tomar el control de los sistemas internos. Asigne roles, coordínese con el personal de respuesta a emergencias y asegúrese de que todos conozcan sus responsabilidades Estrategia de comunicación en caso de crisis: Tu equipo de continuidad de negocio debe decidir quién habla en público, qué canales utilizar y cómo priorizar las actualizaciones. Establece procedimientos de escalado para que los equipos sepan exactamente cómo manejar diferentes escenarios de crisisObtener plantilla gratis, gratuitaPlanifique fácilmente su estrategia de comunicación en caso de crisis utilizando la plantilla de plan de comunicación de ClickUp Recuperación y continuidad de la empresa: ¿Cómo se restauran las funciones críticas de la empresa después de una interrupción? Esquematice los procedimientos de recuperación, como la restauración de datos, la comunicación con clientes y proveedores clave, la implementación de planes de contingencia y el ajuste de soluciones temporales de trabajoIdentifique las funciones críticas, actúe con rapidez y vuelva a la normalidad con confianzaEsta fase final es la que garantiza que su BCP siga siendo relevante, eficaz y esté actualizado.Planifique auditorías y actualizaciones: Un plan de continuidad de negocio no es «lo pones y te olvidas». Revíselo, pruébelo y actualícelo regularmente para mantenerlo al día. Realice simulaciones, perfeccione estrategias y manténgase alineado con su política de continuidad de negocioFormación de los empleados: Tu equipo necesita saber exactamente qué hacer en una crisis. Organiza sesiones de formación, aclara los roles y refuerza la comunicación para que todos estén preparados cuando sea necesarioVersiones de prueba y simulaciones: No espere a que ocurra un desastre, practique antes de que sea real. Los simulacros ayudan a detectar puntos débiles, mejorar los tiempos de respuesta y garantizar que todo funcione sin interrupcionesCuando se trata de estar preparados y responder rápidamente, las herramientas adecuadas son las que marcan la diferencia.Aquí tiene algunos que ayudan a las empresas a gestionar los riesgos y la recuperación sin problemas:Sistema Fusion Framework: Ayuda a correlacionar las funciones críticas de la empresa y a automatizar la supervisión de riesgosRiskonnect: Centraliza la planificación de la continuidad del negocio con seguimiento de riesgos en tiempo real.Zerto: se centra en la recuperación de desastres de TI y la protección de datosLogicManager: Proporciona un enfoque estructurado para identificar riesgos y planificar respuestasPero, ¿y si necesita una solución más flexible y todo en uno para gestionarlo todo, sin complicaciones? Muchas herramientas se centran en un solo aspecto de la continuidad del negocio, dejándole haciendo malabarismos con múltiples plataformas. ¡Aquí es donde necesita ClickUp (la app, aplicación, Todo para el trabajo)!Une todo en un solo lugar, lo que facilita el seguimiento de los riesgos, la asignación de tareas y la coordinación de su equipo durante cualquier interrupción. Así es como funciona. Creación y edición de documentos en tiempo real con su equipo con ClickUp DocsLa gestión eficaz de riesgos y la planificación de respuestas dependen del acceso rápido a información crítica. Con ClickUp Docs , puede crear, almacenar y actualizar sus planes de continuidad de negocio, evaluaciones de riesgos y protocolos de respuesta en una ubicación central. Esto garantiza que todas las partes interesadas tengan la información más reciente al alcance de la mano, lo que permite una respuesta rápida y coordinada.Asigne elementos de acción, asigne el trabajo a los departamentos adecuados y realice seguimientos con las tareas de ClickUpUna vez que su plan esté en marcha, la claridad en la ejecución es clave. Las tareas de ClickUp ayudan a asignar y realizar un seguimiento de cada elemento de acción relacionado con la gestión de riesgos, los procedimientos de recuperación y las funciones críticas de la empresa. Establezca prioridades, plazos y dependencias para que su equipo sepa exactamente quién es responsable de qué, eliminando la confusión y permitiendo una acción rápida cuando más importa.Para mejorar aún más la eficiencia, utilice la guía de priorización de tareas de ClickUp para estructurar los flujos de trabajo y asegurarse de que las tareas más urgentes se aborden primero.Obtenga una vista de alto nivel de su BCP con los paneles de ClickUpDurante las fases de prueba y las crisis reales, puede estar al tanto de su plan de continuidad con los paneles de ClickUp, que proporcionan una instantánea en tiempo real del progreso. Ya sea que esté haciendo un seguimiento de la finalización de tareas, los tiempos de respuesta o los posibles retrasos, los paneles le brindan visibilidad instantánea de su plan de continuidad de negocios, lo que le ayuda a mantenerse organizado y alineado cuando cada segundo cuenta.A nadie le gusta crear documentos desde cero, sobre todo cuando implica una extensa entrada manual de datos e información repetitiva. En días como estos, las plantillas ya preparadas pueden ser su mejor aliado. Con la plantilla del plan de continuidad de negocio de ClickUp, el trabajo preliminar ya está hecho, solo le queda rellenar los detalles.Obtener plantilla gratis, gratuitaEvalúe los riesgos, complete las estrategias de recuperación y las soluciones con la plantilla de plan de continuidad de negocio de ClickUpPor eso le encantará esta plantilla:Fácil seguimiento del progreso: Los estados personalizados como «Completada», «En curso» y «Pendiente» le ayudan a ver al instante en qué punto se encuentran las tareas*información organizada: Los campos personalizados como «Categoría del plan Business» y «Detalles» le permiten almacenar y visualizar información crítica sin esfuerzoVarias vistas prácticas: Elija entre cuatro vistas diferentes (Prioridades, Tablero, Lista y Guía de inicio) para mantener sus datos organizados y fácilmente accesiblesClickUp ha supuesto un cambio radical para nuestro equipo, ¡la ayuda que nos proporcionaron durante nuestra incorporación fue increíble! Nos ha ahorrado innumerables horas de tiempo, nos ha proporcionado los datos para asignar nuestros recursos de manera más eficaz y ha mantenido nuestros proyectos en un cronograma mientras mantenía a nuestros clientes informados.ClickUp ha supuesto un cambio radical para nuestro equipo, ¡la compatibilidad que nos proporcionaron durante nuestra incorporación fue increíble! Nos ha ahorrado innumerables horas de tiempo, nos ha proporcionado los datos para asignar nuestros recursos de manera más efectiva y ha mantenido nuestros proyectos en un cronograma mientras mantenía a nuestros clientes informados.ClickUp ha supuesto un cambio radical para nuestro equipo, ¡la ayuda que nos proporcionaron durante la incorporación fue increíble! Nos ha ahorrado innumerables horas de tiempo, nos ha proporcionado los datos para asignar nuestros recursos de manera más eficaz y ha mantenido nuestros proyectos en un cronograma mientras mantenía a nuestros clientes informados.ClickUp ha supuesto un cambio radical para nuestro equipo, ¡la ayuda que nos proporcionaron durante la incorporación fue increíble! Nos ha ahorrado innumerables horas de tiempo, nos ha proporcionado los datos para asignar nuestros recursos de forma más eficaz y ha mantenido nuestros proyectos en un cronograma mientras mantenía a nuestros clientes informados.ClickUp ha supuesto un cambio radical para nuestro equipo, ¡la compatibilidad que nos proporcionaron durante nuestra incorporación fue increíble! Nos ha ahorrado innumerables horas de tiempo, nos ha proporcionado los datos para asignar nuestros recursos de manera más efectiva y ha mantenido nuestros proyectos en un cronograma mientras mantenía a nuestros clientes informados.En una crisis, la comunicación instantánea no es negociable. Necesita que sus equipos y departamentos trabajen juntos de inmediato sin tener que cambiar entre múltiples apps, aplicaciones o buscar información. Por eso ClickUp Chat es un cambio de juego.Mantenga las conversaciones en marcha en tiempos de crisis con ClickUp ChatPermite a todos discutir los planes de recuperación y las estrategias de mitigación en un solo lugar, manteniendo la comunicación abierta y rápida cuando más se necesita. Incluso puedes asignar tareas directamente desde el chat, convirtiendo las discusiones en acciones al instante.Pero eso es solo el principio. Con ClickUp Brain (el asistente de IA de ClickUp) directamente en el chat, puede encontrar rápidamente las actualizaciones más relevantes o los documentos críticos sin tener que rebuscar.Resuma, cree o busque tareas con ClickUp Brain integrado directamente en ClickUp ChatY cuando se trata de convertir estos planes en realidad, Automatizaciones de ClickUp es el camino a seguir. ¿Quiere que un documento o tarea de recuperación crucial llegue a la persona adecuada en el momento en que se le asigne? Configure un comando personalizado rápido y ClickUp se encargará del resto.Asigne automáticamente elementos de acción, prioridades de tareas y actualizaciones de estado con las automatizaciones de ClickUpSi no quieres crear comandos manualmente, no te preocupes, solo tienes que pedirle a ClickUp Brain con una simple indicación. Se encargará de la configuración de la automatización por ti en segundos. Menos trabajo, más acción.➡ Leer más: El mejor software de gestión de riesgos corporativosSi hay algo que hemos aprendido, es que la incertidumbre no se trata de «si», sino de «cuándo». Las interrupciones sucederán, ya sea un ciberataque, una ruptura en la cadena de suministro o un cambio inesperado en el mercado.La verdadera pregunta es: ¿estará preparada su empresa?Un BCP ofrece a la organización la mejor oportunidad de afrontar correctamente una situación de desastre al proporcionar instrucciones ya preparadas.Pero seamos realistas: un BCP no es eficaz si está enterrado en una carpeta olvidada, nunca se actualiza o es demasiado complejo para que los equipos lo sigan.Con las diversas funciones y plantillas personalizables de ClickUp, la planificación de la continuidad del negocio se vuelve más sencilla, más organizada y mucho menos desalentadora.¡Regístrese hoy mismo en ClickUp! El objetivo de la gestión de riesgos no es eliminar todos los riesgos, sino reducir efectivamente su probabilidad e impacto. Una forma de hacerlo es a través de la planificación de la continuidad empresarial.Tener un plan de continuidad empresarial puede ayudar a su organización a seguir operando en alguna capacidad durante un desastre.A continuación, obtenga respuestas directas sobre qué incluye un plan de continuidad empresarial, por qué es importante y cómo redactar uno. También encontrará una plantilla de continuidad empresarial para simplificar el proceso.Un plan de continuidad empresarial es un documento que contiene un conjunto predeterminado de procedimientos que describen cómo una organización mantendrá sus operaciones comerciales durante y después de una interrupción significativa.Esta interrupción puede ser causada por una amplia gama de amenazas, incluidas desastres naturales, fallos técnicos y ciberataques.¿Qué es la gestión de la continuidad empresarial?Un plan de continuidad empresarial es una parte de la gestión de la continuidad empresarial (BCM). La BCM incluye la evaluación de riesgos, la planificación de respuestas, la recuperación y el mantenimiento a largo plazo de las políticas y procedimientos desarrollados, probados y utilizados cuando ocurre una crisis.El objetivo principal de la planificación de la continuidad empresarial es identificar las preparaciones y acciones de recuperación que pueden ayudar a una organización a reanudar operaciones y servicios lo más rápido posible durante y después de una crisis.Por ejemplo, la mayoría de las operaciones comerciales dependen en gran medida de la tecnología y los sistemas automatizados, y la interrupción de estos sistemas, incluso por unas pocas horas, puede causar problemas graves. Considere una interrupción de Zoom. Esto puede afectar las reuniones con colegas, clientes y prospectos, así como proyectos y acuerdos importantes. Una empresa con un plan de continuidad empresarial que haya identificado una herramienta de sustitución para las reuniones de video podrá recuperarse más rápido que una empresa sin uno.Para asegurar que su negocio funcione lo más suavemente posible incluso cuando se enfrente a fallos del sistema, ciberataques, desastres naturales y otras interrupciones importantes, debe haber una conciencia de las posibles crisis que podrían impactar los sistemas críticos, herramientas y habilidades de su organización y un plan para manejarlas.La planificación de la continuidad empresarial también es importante para obtener y mantener el cumplimiento con algunos estándares de privacidad y seguridad, incluido SOC 2®. Veamos este otro motivo para crear un BCP y mantenerlo actualizado.Cumplimiento de SOC 2: Requisitos, Proceso de Auditoría y Beneficios para el Crecimiento EmpresarialRead MoreUn plan de continuidad empresarial es parte de la documentación que un auditor de SOC 2 probablemente revisará, junto con sus sistemas y controles de seguridad, para determinar su nivel de cumplimiento con los Criterios de Servicios de Confianza (TSC) que ha seleccionado. Este plan es especialmente importante si incluye Disponibilidad como TSC en su auditoría de SOC 2.Los controles de Disponibilidad en SOC 2 se centran en minimizar el tiempo de inactividad. Por lo tanto, la evaluación de riesgos es esencial.Un auditor de SOC 2 probablemente revisará si su empresa ha identificado y pensado en formas de mitigar las amenazas ambientales que podrían afectar la disponibilidad del sistema, como huracanes, tornados e incendios forestales. El mismo proceso debe aplicarse a las amenazas “provocadas por el hombre”, como el robo y los ciberataques.Un auditor de SOC 2 también probablemente revisará si su plan de continuidad empresarial puede aplicarse a eventos imprevistos que podrían afectar la disponibilidad y capacidad de su sistema, como una pandemia global.Es probable que un auditor también revise si has probado tu Plan de Continuidad de Negocio (BCP) en el último año (al menos).La planificación de la continuidad del negocio debe ser un esfuerzo de arriba hacia abajo. Es decir, debe contar con el apoyo y la participación voluntaria de un director o gerente senior de la empresa. Aunque actuarán como el patrocinador ejecutivo, se debe nombrar a otra persona como el coordinador del BCP. Dependiendo del tamaño de la organización, también puede ser necesario nombrar un equipo de planificación que represente todas las áreas principales de operaciones para asistir al coordinador del BCP.Este coordinador y/o equipo deben ser debidamente anunciados y capacitados para llevar a cabo una serie de responsabilidades, incluyendo descubrir las debilidades de tu empresa y hacer planes para mitigarlas, probar esos planes para asegurarse de que sean efectivos para diferentes tipos de crisis y actualizarlos a medida que surjan nuevas amenazas.Existen varios planes de contingencia y continuidad que pueden ayudar a minimizar el impacto de eventos catastróficos. Veamos a continuación los tres planes más comunes y cómo se diferencian entre sí.Plan de continuidad del negocio vs plan de recuperación ante desastresLa principal diferencia entre un plan de continuidad del negocio y un plan de recuperación ante desastres es que un BCP proporciona procedimientos para mantener las operaciones comerciales mientras se recupera de una interrupción significativa, mientras que un DRP proporciona procedimientos para recuperar las operaciones de los sistemas de información después de una interrupción significativa del sistema, como una falla importante de software o un desastre natural, reubicándolos en una ubicación alternativa.Muchas organizaciones eligen combinar sus planes de continuidad del negocio y de recuperación ante desastres en un solo documento. Sin embargo, algunas optan por crearlos como documentos independientes.Plan de continuidad del negocio vs respuesta a incidentesLa principal diferencia entre un plan de continuidad del negocio y un plan de respuesta a incidentes es que un BCP proporciona procedimientos para mantener las operaciones comerciales mientras se recupera de una interrupción significativa, mientras que un IRP proporciona procedimientos para mitigar y corregir un sistema después de un incidente de seguridad, como un virus o un troyano.Un plan de IRP debe detallar un proceso de recuperación para cuando ocurran incidentes de seguridad.Este es otro documento crucial que un auditor de SOC 2 probablemente revisará para determinar tu nivel de cumplimiento con el TSC que has seleccionado.Un plan de continuidad del negocio típicamente incluye lo siguiente:Servicios, procesos y recursos críticos para la misión: Todo BCP debe incluir una lista de servicios, procesos y recursos críticos para la misión. Estos deben recuperarse primero cuando ocurre un evento de BCP para minimizar el tiempo de inactividad.Consideraciones para ubicaciones alternativas: Durante un evento significativo del Plan de Continuidad del Negocio (BCP), una organización puede necesitar utilizar centros de datos de respaldo, sitios de respaldo para operaciones, ubicaciones remotas u otras ubicaciones alternativas. Estos típicamente se documentan en el BCP junto con consideraciones como la accesibilidad de estos sitios alternativos, alternativas de transporte a estos sitios, la cantidad de personal necesario para realizar actividades críticas en estos sitios y otros recursos que serán necesarios.Relaciones con proveedores: Las organizaciones pueden categorizar a los proveedores en niveles de riesgo y evaluar el riesgo en sus planes de BCP.Servicios de telecomunicaciones y consideraciones tecnológicas: Las organizaciones suelen detallar estrategias para mantener operaciones durante interrupciones en las comunicaciones en su BCP. Esto puede incluir el uso de múltiples proveedores de telecomunicaciones, líneas telefónicas secundarias, tecnología en la nube, líneas telefónicas temporales, unidades móviles de telecomunicaciones y Wi-Fi para el personal sin energía, así como servicios móviles de respaldo con diferentes operadores.Planes de comunicación: Las organizaciones típicamente establecen planes de comunicación con personal, clientes y otras terceras partes externas, incluidos reguladores, intercambios y oficiales de emergencia, en su BCP.Consideraciones de regulación y cumplimiento: Las organizaciones suelen incluir requisitos regulatorios en sus BCP y deben actualizarlos regularmente para incluir cualquier nuevo requisito.Métodos de revisión y prueba: Las organizaciones deben incluir cómo se revisa y prueba su BCP y con qué frecuencia. Por ejemplo, pueden realizar pruebas completas del BCP al menos una vez al año o antes si se realizan cambios significativos. También pueden realizar capacitaciones para empleados o requerir que los empleados revisen su BCP anualmente para asegurar que todo el personal esté familiarizado con el plan y sus responsabilidades.Objetivos de recuperación: Un BCP típicamente incluye objetivos clave de recuperación que ayudan a las organizaciones a planificar cuán rápido necesitan recuperar datos y sistemas para minimizar interrupciones y mantener operaciones sin problemas durante eventos inesperados. Estos se definen a continuación: - RPO (Objetivo de Punto de Recuperación): RPO establece el límite de cuánto pérdida de datos puede tolerar un negocio después de una interrupción. Define el punto en el tiempo más reciente aceptable para recuperar datos, minimizando pérdidas potenciales.- RTO (Objetivo de Tiempo de Recuperación): RTO es el tiempo máximo de inactividad aceptable para sistemas o procesos. Indica con qué rapidez un negocio necesita recuperarse y reanudar operaciones normales después de una interrupción.Este ejemplo de plan de continuidad del negocio de Santa Cruz Health está diseñado para que diferentes instalaciones lo personalicen para asegurar que se tomen medidas para preparar y pre-positionar recursos para asegurar la continuidad de los servicios y procesos críticos para la misión en caso de un evento que interrumpa las operaciones normales y afecte las operaciones esenciales de la instalación. Está dividido en varias secciones, incluyendo:General: Describe el propósito del BCP, como se mencionó anteriormente.Activación: Describe brevemente cuándo se debe activar el plan.Descripción general: Describe brevemente qué es el plan, cómo se desarrolló, qué pasos se necesitan tomar para asegurar su efectividad y qué está incluido.Requisitos de continuidad: Enumera los servicios críticos para la misión de la instalación, procesos, equipos y suministros, aplicaciones de TI, registros y personal de continuidad del negocio.Acciones de continuidad y recuperación: Enumera procedimientos después de la ocurrencia de diferentes eventos de BCP, incluyendo pérdida de energía, pérdida de HVAC y reubicación de servicios departamentales a una ubicación alternativa.Ahora es el momento de comenzar a formular y desarrollar su plan de continuidad de negocios. Para guiarle a través del proceso, hemos desglosado el proceso en seis pasos clave. También hemos proporcionado una plantilla a continuación para ayudarle a comenzar.1. Identifique y evalúe sus riesgos.La primera gran tarea de escribir un BCP es identificar los riesgos o amenazas en su entorno y determinar cómo podrían impactar sus operaciones. Por ejemplo, algunas amenazas ambientales pueden causar daños físicos a su edificio. Otros tipos de amenazas pueden afectar a su personal y sus familias. Los riesgos que son más amenazantes para sus operaciones deben ser priorizados.2. Identifique los elementos críticos de su organización.La siguiente gran tarea es identificar las herramientas, sistemas y habilidades que son esenciales para sus operaciones y qué tan críticos son para su recuperación. Puede iniciar la lluvia de ideas planteando la pregunta, ¿cómo logramos nuestros objetivos?Por ejemplo, digamos que uno de sus servicios críticos es la recaudación de fondos. En ese caso, un activo crítico podrían ser las tarjetas de promesa. El proveedor que imprime sus tarjetas de promesa también se consideraría crítico.Al identificar estos sistemas, herramientas y habilidades, también querrá determinar qué recursos serían necesarios para restaurarlos y, por lo tanto, reanudar los servicios y procesos críticos en los que participan. Ejemplos de requisitos de recursos son instalaciones, personal, equipo, software, archivos de datos, componentes del sistema y registros vitales.Esto ayudará a determinar los niveles de prioridad para secuenciar las actividades de recuperación. En otras palabras, ¿qué debe ser restaurado primero para volver al trabajo lo más rápido posible durante y después de una crisis?3. Identifique formas de mitigar riesgos.Ahora que comprende los riesgos y elementos críticos únicos de su organización, está listo para crear un plan de acción.Comience identificando estrategias que eliminarán los riesgos que identificó en el paso 1 por completo. Si eso no es posible, identifique estrategias que disminuirán su impacto. Por ejemplo, es imposible eliminar completamente la amenaza de amenazas ambientales como tormentas de nieve. En su lugar, puede crear un procedimiento para que sus empleados y contratistas trabajen de forma remota si una tormenta de nieve imposibilita o dificulta llegar a la oficina. Esto requerirá que todos los empleados y contratistas tengan los suministros y equipos adecuados y reciban las mismas comunicaciones.Estas estrategias de mitigación están diseñadas para eliminar o disminuir el impacto de una amenaza antes de una crisis y, por lo tanto, deben ser implementadas lo más rápido posible.4. Identifique formas de prepararse y recuperarse de la pérdida de cualquier elemento crítico.Dado que es imposible eliminar todas las amenazas que enfrenta su organización, su próximo paso es identificar tantas estrategias como sea posible para lidiar con la pérdida de cada elemento crítico identificado en el paso 2.Por ejemplo, instalar sistemas de protección como un sistema de seguridad, sistema de alarma contra incendios y software antivirus, todos pueden considerarse estrategias para prepararse y recuperarse de la pérdida de elementos críticos causados por robos, vandalismo, peligros ambientales, ciberataques y otras amenazas.El objetivo es inventar tantas estrategias de preparación como sea posible para estar mejor preparado y recuperarse de la pérdida de activos críticos durante y después de una crisis.Durante la etapa de revisión o prueba, puede eliminar cualquier estrategia que sea demasiado lenta o costosa.5. Prepárese para cómo responderá después de una crisis.Ahora que los planes y estrategias están en marcha, puede tomar medidas para mejorar la eficiencia y la calidad de la respuesta de su organización ante una crisis y ayudarle a volver al trabajo lo más rápido posible.Considere crear un equipo de recuperación que pueda evaluar sus pérdidas e iniciar acciones de recuperación después de una crisis. Los roles y responsabilidades de este equipo pueden estar documentados en su BCP.6. Actualice y pruebe su plan de continuidad del negocio.Su plan de continuidad del negocio es un documento vivo. Debe actualizarse para reflejar los riesgos y necesidades cambiantes de su negocio. Ya sea que esté integrando un nuevo software que de repente se bloquea o incorporando a un nuevo miembro del equipo de gestión, su BCP debe reflejar estos cambios.Si no hay cambios importantes que afecten a su negocio, aún debe probar su plan de continuidad del negocio una vez al año como mínimo. Esta es una práctica recomendada y un requisito de cumplimiento. Puede usar una variedad de métodos de prueba, incluidos ejercicios de mesa y pruebas de simulación.Probar y mantener la documentación actualizada como esta es una parte importante del cumplimiento continuo.Qué es el cumplimiento continuo + Cómo lograrloRead MoreUse esta plantilla para comenzar a identificar los riesgos, elementos críticos, acciones de mitigación y estrategias de preparación que conformarán los componentes básicos de su plan de continuidad del negocio.¿Cuáles son los beneficios de un plan de continuidad del negocio?La implementación y el mantenimiento de un plan de continuidad del negocio efectivo ofrece una variedad de beneficios, que incluyen:costos reducidos y menor impacto en el rendimiento del negocio cuando ocurre una interrupciónun enfoque coherente en toda la organización para responder y recuperarse de una interrupción significativagarantía para clientes, proveedores, reguladores y otras partes interesadas de que la organización tiene sistemas y procesos en su lugar para la continuidad del negociomejora del rendimiento empresarial y la resiliencia organizativauna mejor comprensión del negocio, sus problemas críticos y áreas de vulnerabilidad¿Cuáles son los 5 componentes de un plan de continuidad del negocio?Si bien cada plan de continuidad del negocio es único, cinco componentes clave son:Riesgos y su impacto potencial en el negocio y la probabilidad de que ocurranServicios, procesos y recursos críticos para la misiónAcciones de mitigación de riesgosEstrategias de preparación para prepararse y recuperarse de la pérdida de cualquier elemento críticoCapacitación, pruebas y mantenimiento del plan¿Cuáles son las 4 P’s de la continuidad del negocio?Las cuatro P de la continuidad del negocio son personas, procesos, instalaciones y proveedores. A continuación se definen cada una de ellas:Personas: Esto incluye a tus empleados y clientes.Procesos: Esto incluye la tecnología y los procesos que utiliza tu negocio para mantener todo en funcionamiento.Instalaciones: Esto incluye los edificios y espacios desde los cuales opera tu negocio.Proveedores: Esto incluye socios, vendedores y suministradores de los que tu negocio depende para obtener recursos.¿Cuál es un ejemplo real de continuidad del negocio?Un ejemplo real de continuidad del negocio es la respuesta a la crisis del agua en Ciudad del Cabo, que comenzó en 2015. Durante un período de sequía severa, Ciudad del Cabo implementó varias estrategias de respuesta y recuperación que evitaron la catástrofe de quedarse sin agua —también conocida como “Día Cero”. Esto incluyó la introducción de metodologías innovadoras de reducción de presión para frenar las pérdidas de agua, una reducción sostenida en el uso del agua y programas efectivos de comunicación y concienciación pública para evitar el “Día Cero”. ¿Cómo escribo un plan de BCM?A continuación, un proceso paso a paso para escribir un plan de BCM:Identificar y evaluar riesgos (puedes usar las 4 P's)Identificar productos, servicios o funciones críticos para la misiónEvaluar el impacto potencial de los riesgos y las interrupciones en los elementos críticosEnumerar acciones para mitigar estos riesgosEnumerar estrategias para prepararse y recuperarse de la pérdida de cualquier elemento críticoMantener, revisar y actualizar continuamente el plan de continuidad del negocio¿Por qué fallan los planes de continuidad del negocio?Los planes de continuidad del negocio fallan por varias razones, siendo la más común la falta de compromiso de la alta dirección. Otras razones son que no se asigna a alguien para tomar responsabilidad de la planificación de la continuidad del negocio, o que el plan no se prueba y actualiza regularmente para mantenerse al día con los cambios que afectan al negocio.Usa la confianza para acelerar el crecimientoSolicitar una demo

- security plus exam questions
- practical gifts christmas
- testing cerebellar function
- free masters degree online
- mokoluxu
- how do you unblock on instagram

- bucket ball cool math games
- rinelayu
- eulogy examples grandma
- kokabu
- examples of analytical essays
- http://dikiro.info/UserFiles/File/susexofodof-sugojifekev.pdf
- http://vietjadetravel.com/upload/files/gikokegozajin.pdf
- http://lchwh.com/v15/Upload/file/20255161054551598.pdf
- yacupo
- how to open google doc in excel
- puxu