Supplier Requirements: Business Continuity Management

Revised December 2019

Table of Contents

Click on the desired language above.

Supplier BCM Requirements – Translations

ENGLISH

Business Continuity Management

Definitions

“Business Continuity Management” or “BCM” means the holistic management of the process of identifying the organization’s business critical functions, evaluating risks and their impacts, and developing plans that enable organizational resiliency in the midst of Incidents.

“Disaster Recovery” or “DR” means the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization when impacted by an Incident. DR focuses on the IT or technology systems that support business functions, as opposed to Business Continuity, which involves planning for keeping all aspects of the business (e.g. operations, facilities, personnel, equipment, infrastructure, applications, etc.) functioning in the midst of an Incident.

“Incident” is a situation that is, or could lead to, a disruption, loss, emergency or crisis. An Incident could materially impair or halt operations of the Supplier.

Business Continuity Management Standard

CenturyLink requires its suppliers (each a “Supplier”) to comply with, at a minimum, the Business Continuity Management standards listed in Subsections a-k below (“BCM Standard”) to ensure Suppliers are able to continue to support CenturyLink when CenturyLink or the Supplier experiences an Incident. Supplier shall comply with this BCM Standard and must maintain a Business Continuity Management plan (“BCM Plan”) that outlines the Supplier’s processes for ensuring continuity of Supplier’s business in the event of an actual or threatened Incident during the period of time Supplier is providing products or services to CenturyLink. Supplier’s BCM Plan may include a Disaster Recovery plan and an Incident management plan. Upon CenturyLink’s request, Supplier must provide CenturyLink with a copy of its BCM Plan or meet with a CenturyLink BCM representative at a convenient time to review Supplier’s BCM Plan and any exercise or test results.

a) Supplier must conduct a business impact analysis and risk assessment to sequence its recovery and mitigate the impacts of potential threats and hazards.

b) Supplier must implement strategies to protect and fortify environments, facilities, networks, systems/applications and Supplier’s people.

c) Supplier must back up its data and systems/applications to an alternate location that is in a different geographic location dispersed from the primary location and routinely test the backups to confirm viability.

d) Supplier’s BCM Plan must include defined roles and responsibilities, activation triggers, a communication plan, recovery solutions and a sequence for recovering all of Supplier’s functions, facilities, networks, environments and systems/applications that are utilized to provide products and services to CenturyLink.

e) Supplier must review and update its BCM Plan whenever there are operational changes, but not less than once each calendar year.

f) Supplier must test/exercise its BCM Plan at least once each calendar year and share those results with CenturyLink during audit assessments.

g) Supplier must maintain and exercise its Incident management structure to ensure timely recovery from Incidents and provide prompt notifications to CenturyLink when the provisioning of the products and services could be interrupted.

h) Supplier must manage the resiliency of its third-party vendors and subcontractors to ensure they can continue to support Supplier when Supplier or its third-party vendors and subcontractors experience operational disruptions.

i) Supplier must immediately notify CenturyLink when any actual or anticipated Incident could cause a disruption in the delivery of its products or services to CenturyLink. Notifications should be sent to Supplier's CenturyLink point of contact.

j) Supplier will take the appropriate steps to immediately address any such Incident and will provide CenturyLink with a report stating the reason for the outage/disruption and indicate the measures being taken to prevent a reoccurrence.

k) Supplier must not make or permit any statements to be made concerning any Incident that expressly mention CenturyLink to any third-party without the written authorization of CenturyLink.

FRENCH

Gestion de la continuité des activités

Définitions

« Gestion de la continuité des activités » ou « GCA » désigne la gestion holistique du processus d'identification des fonctions critiques de l'organisation, l'évaluation des risques et de leurs répercussions, et l'élaboration de plans qui permettent à l'organisation de faire preuve de résilience en cas d'incident.

« Reprise après sinistre » ou « RAS » désigne le processus, les politiques et les procédures liés à la préparation de la reprise du maintien de l'infrastructure technologique vitale pour une organisation touchée par un incident. RAS met l'accent sur les systèmes informatiques ou les systèmes technologiques qui soutiennent les fonctions opérationnelles, par opposition à la continuité des activités, qui implique la planification pour maintenir tous les aspects du fonctionnement opérationnel (par exemple, opérations, installations, personnel, équipement, infrastructure, applications, etc.) au beau milieu de l'incident.

Un « incident » est une situation qui cause ou pourrait causer une perturbation, une perte, une urgence ou une crise. Un incident pourrait nuire gravement aux activités du fournisseur, voire les interrompre.

Norme de gestion de la continuité des activités

CenturyLink exige de ses fournisseurs (chacun un « fournisseur ») qu'ils se conforment, au minimum, aux normes de gestion de la continuité des opérations énumérées dans les sous-sections a à k ci-dessous (« norme GCA ») pour que les fournisseurs soient capables de continuer à soutenir CenturyLink quand un incident survient chez CenturyLink ou le fournisseur. Le fournisseur doit se conformer à la présente norme GCA et doit maintenir un plan de gestion de la continuité des activités (le « plan GCA ») qui décrit les processus du fournisseur pour assurer la continuité de ses activités en cas d'incident réel ou de menace au cours de la période pendant laquelle le fournisseur fournit des produits ou des services à CenturyLink. Le plan GCA du fournisseur peut comprendre un plan de reprise après sinistre et un plan de gestion des incidents. À la demande de CenturyLink, le fournisseur doit fournir à CenturyLink une copie de son plan GCA ou rencontrer un représentant de CenturyLink GCA à un moment opportun pour examiner le plan GCA du fournisseur et tout exercice ou résultat de test.

a) Le fournisseur doit effectuer une analyse des répercussions sur les activités et une évaluation des risques afin de séquencer son rétablissement et d'atténuer les répercussions des menaces et des dangers potentiels.

b) Le fournisseur doit mettre en œuvre des stratégies pour protéger et renforcer les environnements, les installations, les réseaux, les systèmes/applications et son personnel.

c) Le fournisseur doit sauvegarder ses données et ses systèmes/applications dans un autre emplacement géographiquement éloigné du site principal et tester régulièrement les sauvegardes pour confirmer leur viabilité.

d) Le plan GCA du fournisseur doit inclure les rôles et responsabilités définis, les déclencheurs d'activation, un plan de communication, des solutions de récupération et une séquence pour récupérer toutes les fonctions, installations, réseaux, environnements et systèmes/applications du fournisseur qui sont utilisés pour fournir des produits et services à CenturyLink.

e) Le fournisseur doit examiner et mettre à jour son plan GCA chaque fois qu'il y a des changements opérationnels, mais au moins une fois par année civile.

f) Le fournisseur doit tester/exercer son plan GCA au moins une fois par année civile et partager ces résultats avec CenturyLink lors des évaluations de vérification.

g) Le fournisseur doit maintenir et exercer sa structure de gestion des incidents afin d'assurer une résolution rapide des incidents et fournir des notifications rapides à CenturyLink lorsque l'approvisionnement des produits et services pourrait être interrompu.

h) Le fournisseur doit gérer la résilience de ses fournisseurs tiers et sous-traitants pour s'assurer qu'ils peuvent continuer à le soutenir lorsque lui-même ou ses fournisseurs tiers et sous-traitants subissent des perturbations opérationnelles.

i) Le fournisseur doit aviser immédiatement CenturyLink lorsqu'un incident avéré ou anticipé est susceptible de causer une interruption dans la livraison de ses produits ou services à CenturyLink. Les notifications doivent être envoyées au point de contact CenturyLink du fournisseur.

j) Le fournisseur prendra les mesures appropriées pour faire face immédiatement à un tel incident et fournira à CenturyLink un rapport indiquant la raison de la panne/interruption et indiquant les mesures prises pour éviter qu'elle ne se reproduise.

k) Le fournisseur ne doit pas faire ou permettre que des déclarations concernant un incident quelconque mentionnent expressément CenturyLink à un tiers sans l'autorisation écrite de CenturyLink.

GERMAN

Business Continuity Management

Definitionen

„Business Continuity Management“ oder „BCM“ bezeichnet das ganzheitliche Management des Prozesses zur Identifizierung der geschäftskritischen Funktionen des Unternehmens, zur Bewertung der Risiken und ihrer Auswirkungen sowie zur Entwicklung von Plänen, die die Ausfallsicherheit des Unternehmens inmitten von Störfällen gewährleisten und so die geschäftliche Kontinuität gewährleisten.

„Desaster Recovery“ oder „DR“ bezeichnet den Prozess, die Richtlinien und Verfahren, die im Zusammenhang mit der Vorbereitung auf die Wiederherstellung oder Weiterführung der technologischen Infrastruktur stehen, die für Unternehmen von entscheidender Bedeutung ist, wenn sie von einem Störfall betroffen sind. DR konzentriert sich auf die IT- oder Technologiesysteme, die die Geschäftsfunktionen unterstützen, im Gegensatz zu Business Continuity, bei der u. a. geplant wird, wie alle Aspekte des Geschäfts (z. B. operativer Betrieb, Anlagen, Personal, Ausrüstung, Infrastruktur, Anwendungen usw.) während eines Störfalls weiterhin funktionieren.

„Störfall“ beschreibt eine Situation, die eine Störung, einen Verlust, einen Notfall oder eine Krise darstellt oder dazu führen könnte. Ein Störfall könnte den Betrieb des Lieferanten erheblich beeinträchtigen oder unterbrechen.

Business Continuity Management-Standard

Von seinen Lieferanten (jeweils ein „Lieferant“) verlangt CenturyLink, dass sie mindestens die in den folgenden Abschnitten a bis k des aufgeführten Standards des Business Continuity Management („BCM-Standard“) einhalten, um sicherzustellen, dass Lieferanten CenturyLink weiterhin unterstützen können, falls CenturyLink oder der Lieferant von einem Störfall betroffen ist. Der Lieferant muss diesen BCM-Standard einhalten und einen Business Continuity Management-Plan („BCM-Plan“) vorhalten, der die Prozesse des Lieferanten beschreibt, mit dem die Kontinuität des Geschäfts des Lieferanten im Falle eines tatsächlichen oder drohenden Störfalls während des Zeitraums, in dem der Lieferant Produkte oder Dienstleistungen an CenturyLink bereitstellt, sicherzustellen. Der BCM-Plan des Lieferanten kann einen „Desaster Recovery“-Plan und einen Plan für den Umgang mit Störfällen enthalten. Auf Anfrage von CenturyLink muss der Lieferant CenturyLink eine Kopie seines BCM-Plans zur Verfügung stellen oder sich zu einem geeigneten Zeitpunkt mit einem BCM-Vertreter von CenturyLink treffen, um den BCM-Plan des Lieferanten sowie etwaige Übungs- oder Testergebnisse zu überprüfen.

a) Der Lieferant muss eine Analyse der Auswirkungen auf den Geschäftsbetrieb und eine Risikobewertung durchführen, um die zeitliche Abfolge der Wiederherstellung darzustellen und die Auswirkungen potenzieller Bedrohungen und Gefahren zu mindern.

b) Der Lieferant muss Strategien zum Schutz und zur Stärkung von Umgebungen, Anlagen, Netzwerken, Systemen/Anwendungen und seiner Mitarbeiter implementieren.

c) Der Lieferant muss seine Daten und Systeme/Anwendungen an einem anderen Speicherort sichern, der sich an einem anderen geografischen Ort befindet als der primäre Speicherort, und die Datensicherungen regelmäßig testen, um die Funktionsfähigkeit zu garantieren.

d) Der BCM-Plan des Lieferanten muss definierte Rollen und Verantwortlichkeiten, auslösende Faktoren für den Plan, einen Kommunikationsplan, Wiederherstellungslösungen und eine zeitliche Abfolge für die Wiederherstellung aller Funktionen, Anlagen, Netzwerke, Umgebungen und Systeme/Anwendungen des Lieferanten enthalten, die zur Bereitstellung von Produkten und Dienstleistungen an CenturyLink verwendet werden.

e) Der Lieferant muss seinen BCM-Plan überprüfen und aktualisieren, wenn operative Änderungen eintreten, mindestens jedoch einmal pro Kalenderjahr.

f) Der Lieferant muss seinen BCM-Plan mindestens einmal pro Kalenderjahr testen/ausüben und die Ergebnisse dieser Ausführung im Verlauf von Audit-Bewertungen an CenturyLink weitergeben.

g) Der Lieferant muss seine Struktur für den Umgang mit Störfällen beibehalten und ausüben, um eine rechtzeitige Wiederherstellung nach Störfällen sicherzustellen und CenturyLink umgehend zu benachrichtigen, wenn die Bereitstellung der Produkte und Dienstleistungen unterbrochen werden könnte.

h) Der Lieferant muss die Ausfallsicherheit seiner Drittanbieter und Subunternehmer verwalten, um sicherzustellen, dass sie den Lieferanten weiterhin unterstützen können, wenn bei dem Lieferanten oder seinen Drittanbietern und Subunternehmern operative Störungen auftreten.

i) Der Lieferant muss CenturyLink unverzüglich benachrichtigen, wenn ein tatsächlicher oder zu erwartender Störfall die Lieferung seiner Produkte oder Dienstleistungen an CenturyLink stören könnte. Benachrichtigungen sollten an die CenturyLink-Kontaktstelle des Lieferanten gesendet werden.

j) Der Lieferant ergreift die geeigneten Maßnahmen, um einen solchen Störfall unverzüglich zu beheben, und übermittelt CenturyLink einen Bericht, in dem der Grund für den Ausfall/die Störung und die Maßnahmen angegeben sind, die ergriffen werden, um ein erneutes Auftreten zu verhindern.

k) Der Lieferant darf ohne schriftliche Zustimmung von CenturyLink keine Aussagen zu Vorfällen machen oder genehmigen, in denen CenturyLink ausdrücklich gegenüber Dritten erwähnt wird.

ITALIAN

Gestione della continuità operativa

Definizioni

"Gestione della continuità operativa" o "BCM" (Business Continuity Management) indica la gestione olistica relativa al processo di identificazione delle funzioni aziendali fondamentali dell'organizzazione, la valutazione dei rischi e dei loro impatti e lo sviluppo di piani che consentano la resilienza organizzativa in mezzo degli incidenti.

"Disaster Recovery" o "DR" indica il processo, le politiche e le procedure relative alla preparazione per il ripristino o la prosecuzione dell'operatività dell'infrastruttura tecnologica che sono vitali quando un'organizzazione subisce un Incidente. La DR si concentra sui sistemi IT o tecnologici a supporto delle funzioni aziendali, in contrapposizione alla Continuità operativa, che prevede la pianificazione finalizzata a preservare il funzionamento di tutti gli aspetti dell'azienda (ad es., operazioni, strutture, personale, attrezzature, infrastruttura, applicazioni, ecc.) nel mezzo di un Incidente.

L'"Incidente" è una situazione che è, o potrebbe risultare in, un'interruzione, perdita, emergenza o crisi. Un Incidente potrebbe compromettere materialmente o interrompere le operazioni del Fornitore.

Standard di gestione della continuità operativa

CenturyLink richiede ai propri fornitori (definiti in prosieguo individualmente come "Fornitore") di conformarsi, come minimo, agli Standard di gestione della continuità operativa elencati nelle Sottosezioni a-k seguenti ("Standard BCM") per garantire che i fornitori siano in grado di continuare a supportare CenturyLink quando CenturyLink o il Fornitore subiscono un Incidente. Il Fornitore è tenuto a conformarsi agli Standard BCM e a disporre di un Piano di gestione della continuità operativa ("Piano BCM") che descriva i processi del Fornitore al fine di garantire la continuità delle attività del Fornitore in caso di Incidente effettivo o minacciato durante l'arco di tempo in cui il Fornitore fornisce i prodotti o servizi a CenturyLink. Il piano BCM del Fornitore può includere un piano di Disaster Recovery e un piano di Gestione degli incidenti. Su richiesta di CenturyLink, il Fornitore deve fornire a CenturyLink una copia del proprio Piano BCM o incontrarsi al momento opportuno con un rappresentante del BCM di CenturyLink per esaminare il Piano BCM del Fornitore e qualsiasi risultato dell'esame o del test.

a) Il Fornitore deve condurre un'analisi dell'impatto aziendale e una valutazione dei rischi per sequenziarne il ripristino e mitigare gli impatti di potenziali minacce e pericoli.

b) Il Fornitore deve attuare strategie per proteggere e rafforzare ambienti, strutture, reti, sistemi/applicazioni e il personale del Fornitore.

c) Il Fornitore deve eseguire il backup dei propri dati e sistemi/applicazioni in una posizione alternativa ubicata in una diversa posizione geografica dispersa dalla posizione principale e testare regolarmente i backup per confermare la fattibilità.

d) Il Piano BCM del fornitore deve includere ruoli e responsabilità definiti, trigger di attivazione, un piano di comunicazione, soluzioni di rispristino e una sequenza per il rispristino di tutte le funzioni, strutture, reti, ambienti e sistemi/applicazioni del Fornitore utilizzati per fornire i prodotti e servizi a CenturyLink.

e) Il Fornitore deve esaminare e aggiornare il proprio Piano BCM ogni volta che si verificano cambiamenti operativi, ma non meno di una volta ogni anno solare.

f) Il Fornitore deve testare/esaminare il proprio Piano BCM almeno una volta ogni anno solare e comunicare i risultati dei test e degli esami a CenturyLink durante le valutazioni dell'audit.

g) Il Fornitore deve gestire ed esercitare la propria Struttura di gestione degli Incidenti per garantire il tempestivo ripristino dagli Incidenti e fornire tempestive notifiche a CenturyLink qualora la fornitura dei prodotti e servizi venga interrotta.

h) Il Fornitore deve gestire la resilienza dei propri fornitori e subappaltatori terzi per garantire che possano continuare a supportare il Fornitore quando il Fornitore o i suoi fornitori e subappaltatori terzi subiscono interruzioni operative.

i) Il Fornitore deve informare immediatamente CenturyLink nel caso in cui qualsiasi Incidente effettivo o previsto possa causare un'interruzione nella consegna dei propri prodotti o servizi a CenturyLink. Le notifiche devono essere inviate al punto di contatto CenturyLink del Fornitore.

j) Il Fornitore adotterà le misure appropriate per affrontare immediatamente qualsiasi Incidente di questo tipo e fornirà a CenturyLink un rapporto in cui dichiarerà il motivo dell'inattività/interruzione e indicherà le misure adottate per prevenire che si ripetano.

k) Il Fornitore non deve rilasciare né consentire che vengano rilasciate dichiarazioni relative a Incidenti che facciano espressamente menzione di CenturyLink a terzi senza l'autorizzazione scritta di CenturyLink.

PORTUGUESE

Gestão da Continuidade dos Negócios

Definições

“Gestão da Continuidade dos Negócios” ou “GCN” significa a gestão holística do processo de identificação das funções críticas dos negócios da organização, avaliação dos riscos e seus impactos, além do desenvolvimento de planos que permitam resiliência organizacional em meio a Incidentes.

“Recuperação de Desastre” ou “RD” significa o processo, políticas e procedimentos relacionados à preparação para a recuperação ou continuação da infraestrutura de tecnologia que são vitais para uma organização quando impactada por um Incidente. A RD concentra-se nos sistemas de TI ou tecnologia que suportam as funções de negócios, ao contrário da Continuidade dos Negócios, que envolve o planejamento para manter todos os aspectos dos negócios (por exemplo, operações, instalações, pessoal, equipamento, infraestrutura, aplicativos, etc.) funcionando em meio a um Incidente.

“Incidente” é uma situação que é ou pode levar a uma interrupção, perda, emergência ou crise. Um Incidente pode prejudicar ou interromper significativamente as operações do Fornecedor.

Norma de Gestão da Continuidade dos Negócios

A CenturyLink exige que seus fornecedores (individualmente, “Fornecedor”) cumpram, no mínimo, as normas de Gestão da Continuidade dos Negócios listadas nas Subseções a-k abaixo (“Norma de GCN”) para garantir que possam continuar a apoiar a CenturyLink quando esta ou o Fornecedor enfrentam um Incidente. O Fornecedor deve cumprir esta Norma de GCN e deve manter um plano de Gestão da Continuidade dos Negócios (“Plano de GCN”) que descreve os processos do Fornecedor para garantir a continuidade de seus negócios caso um Incidente ocorra ou ameace ocorrer durante o período em que fornece produtos ou serviços à CenturyLink. O Plano de GCN do Fornecedor pode incluir um plano de Recuperação de Desastres e um plano de gestão de Incidentes. Mediante solicitação da CenturyLink, o Fornecedor deve providenciar-lhe uma cópia do seu Plano de GCN ou reunir-se com um representante de GCN da CenturyLink em um horário conveniente para revisar o Plano de GCN do Fornecedor e qualquer resultado de exercício ou teste.

a) O Fornecedor deve realizar uma análise de impacto nos negócios e avaliação de riscos para sequenciar sua recuperação e mitigar os impactos de ameaças e perigos em potencial.

b) O Fornecedor deve implementar estratégias para proteger e fortalecer seus ambientes, instalações, redes, sistemas/aplicativos e funcionários.

c) O Fornecedor deve fazer backup de seus dados e sistemas/aplicativos em um local alternativo que esteja em uma região geográfica diferente, de forma dispersa do local principal e testar regularmente os backups para confirmar a viabilidade.

d) O Plano de GCN do Fornecedor deve incluir competências e responsabilidades definidas, gatilhos de ativação, um plano de comunicação, soluções de recuperação e uma sequência para recuperar todas as suas funções, instalações, redes, ambientes e sistemas/aplicativos que são utilizados para fornecer produtos e serviços à CenturyLink.

e) O Fornecedor deve revisar e atualizar seu Plano de GCN sempre que houver mudanças operacionais, mas não menos que uma vez a cada ano civil.

f) O Fornecedor deve testar/exercitar seu Plano de GCN pelo menos uma vez a cada ano civil e compartilhar esses resultados com a CenturyLink durante as avaliações de auditoria.

g) O Fornecedor deve manter e exercitar sua estrutura de gestão de Incidentes para garantir a recuperação em tempo hábil após Incidentes e fornecer notificações rápidas à CenturyLink quando o fornecimento dos produtos e serviços puder ser interrompido.

h) O Fornecedor deve gerenciar a resiliência de seus terceiros e subcontratados para garantir que possam continuar a dar-lhe suporte quando o Fornecedor ou os terceiros e subcontratados sofrerem interrupções operacionais.

i) O Fornecedor deve notificar imediatamente a CenturyLink quando qualquer Incidente real ou antecipado puder causar interrupção na entrega de seus produtos ou serviços à CenturyLink. As notificações devem ser enviadas ao ponto de contato da CenturyLink do Fornecedor.

j) O Fornecedor tomará as medidas apropriadas para resolver imediatamente qualquer Incidente desse tipo e fornecerá à CenturyLink um relatório informando o motivo da indisponibilidade/interrupção e indicará as medidas que estão sendo tomadas para evitar uma reincidência.

k) O Fornecedor não deve fazer ou permitir que sejam feitas declarações sobre qualquer Incidente que mencione expressamente a CenturyLink a terceiros sem a autorização por escrito da CenturyLink.

SPANISH

Gestión de continuidad del negocio

Definiciones

“Gestión de continuidad del negocio” o “BCM” (por sus siglas en inglés) se refiere a la gestión integral del proceso de identificar las funciones empresariales fundamentales de la organización, evaluar los riesgos y sus efectos y desarrollar planes que permitan la resiliencia de la organización en caso de Incidentes.

“Recuperación ante desastres” o “DR” (por sus siglas en inglés) se refiere al proceso, las políticas y los procedimientos que se relacionan con la preparación para la recuperación o continuación de la infraestructura tecnológica y que son esenciales para una organización afectada por un Incidente. La DR se enfoca en los sistemas de TI o tecnológicos que respaldan las funciones empresariales, a diferencia de la Continuidad del negocio, que implica planificar para mantener en funcionamiento todos los aspectos del negocio (por ejemplo, operaciones, instalaciones, personal, equipos, infraestructura, aplicaciones, etc.) en medio de un Incidente.

Un “Incidente” es una situación que es, o podría conducir a, una interrupción, pérdida, emergencia o crisis. Un Incidente podría perjudicar sustancialmente o detener las operaciones del Proveedor.

Estándar de Gestión de continuidad del negocio

CenturyLink requiere que sus proveedores (cada “Proveedor”) cumplan, como mínimo, con los estándares de Gestión de continuidad del negocio enumerados a continuación en las subsecciones a-k (“Estándar de BCM”) para garantizar que puedan continuar respaldando a CenturyLink cuando este o el Proveedor experimente un Incidente. El Proveedor deberá cumplir con este Estándar de BCM y deberá contar con un plan de Gestión de continuidad del negocio (“Plan de BCM”) que describa sus procesos para garantizar la continuidad de su negocio en caso de un Incidente real o inminente durante el período de tiempo en que proporciona productos o servicios a CenturyLink. El Plan de BCM del Proveedor puede incluir un plan de Recuperación ante desastres y un plan de gestión de Incidentes. A solicitud de CenturyLink, el Proveedor debe proporcionarle una copia de su Plan de BCM o reunirse con un representante de BCM de CenturyLink cuando sea conveniente para revisar su Plan de BCM y los resultados de desempeño o prueba.

a) El Proveedor debe realizar un análisis de impacto empresarial y una evaluación de riesgos para secuenciar su recuperación y mitigar los efectos de posibles amenazas y peligros.

b) El Proveedor debe implementar estrategias para proteger y fortalecer los entornos, las instalaciones, las redes, los sistemas/aplicaciones y a su gente.

c) El proveedor debe crear una copia de seguridad de sus datos y sistemas/aplicaciones en un lugar alternativo que se encuentre en una ubicación geográfica diferente, separada de la ubicación principal, y probar rutinariamente las copias de seguridad para confirmar su viabilidad.

d) El Plan de BCM del Proveedor debe incluir funciones y responsabilidades definidas, disparadores de activación, un plan de comunicación, soluciones de recuperación y una secuencia para recuperar todas sus funciones, instalaciones, redes, entornos y sistemas/aplicaciones que se utilizan para proporcionar productos y servicios a CenturyLink.

e) El Proveedor debe revisar y actualizar su Plan de BCM siempre que haya cambios operativos, pero no menos de una vez por año calendario.

f) El Proveedor debe probar/desempeñar su Plan de BCM al menos una vez por año calendario y compartir esos resultados con CenturyLink durante las evaluaciones de auditoría.

g) El Proveedor debe mantener y desempeñar su estructura de gestión de Incidentes para garantizar una oportuna recuperación de los Incidentes y notificar rápidamente a CenturyLink cuando el suministro de productos y servicios podría interrumpirse.

h) El Proveedor debe gestionar la resiliencia de sus distribuidores y subcontratistas externos para garantizar que puedan continuar respaldándolo cuando este o sus distribuidores y subcontratistas externos experimenten interrupciones operativas.

i) El Proveedor debe notificar de inmediato a CenturyLink cuando un Incidente real o previsto podría interrumpir la entrega de sus productos o servicios a CenturyLink. Las notificaciones deben enviarse al punto de contacto de CenturyLink del Proveedor.

j) El Proveedor tomará las medidas adecuadas para abordar de inmediato cualquier Incidente de este tipo y proporcionará a CenturyLink un informe que indique el motivo de la falla/interrupción e indicará las medidas que se están tomando para evitar que vuelva a ocurrir.

k) El Proveedor no debe realizar ni permitir que se realice ninguna declaración sobre un Incidente que mencione expresamente a CenturyLink a un tercero sin la autorización por escrito de CenturyLink.