International Glossary for Resiliency

Glosario en español

Maintained by DRI International

For questions about this document, contact Chloe Demrovsky at **cdemrovsky@drii.org**. For more information, visit **www.drii.org**.

Legal Disclaimer

These materials are presented solely for informational purposes. DRI International, its officers, directors, staff, licensees, affiliates and volunteers (“DRI International”) are not offering it as legal or other professional services advice. While best efforts have been used in preparing these materials, DRI International makes no representations or warranties of any kind and assumes no liabilities of any kind with respect to the accuracy or completeness of the contents and specifically disclaims any implied warranties of merchantability or fitness of use for a particular purpose. DRI International shall not be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages caused, or alleged to have been caused, directly or indirectly, by the information contained herein. Every organization is different and the definitions contained herein may not be suitable for your situation. You should seek the services of a competent professional before beginning any improvement program.

Committee Members

Permanent Committee Members

Chair
Bobby Williams, MBCP, Fidelity

Coordinator
Chloe Demrovsky, CBCV, DRI International

Al Berman, MBCP, DRI International
Drew Buchanan, CBCP, Bowhead Systems Management, LLC
John Franchy, CBCP, United States Department of Defense
Dean Gallup, CBCP, Booz Allen Hamilton
James Price, MBCP, 3J Contingency Planning Services
Gary Villeneuve, MBCP, CBCLA, DRI International
Mark Wilson, MBCP, CSC
Brian Zawada, MBCP, Avalution Consulting

Spanish Language Committee Members

Chair
Manuel Violante, MBCP, Mexico

Manuel Guillen, ABCP, Costa Rica
Patricia Oliver, ABCP, Mexico
Hector Miguel Opazo, CBCP, Chile

Advisory Members
Agustín Lopez, CBCP, Spain
Oscar Campos Solano, CBCP, Costa Rica
Ana Terrada, CBCP, Puerto Rico

Contributing Committee Members

Carol Chia, CBCP, DRI Malaysia
Rod Crowder, CBCP, DRI Australia
Mohammed al Jenaibi, CBCP, Executive Council, United Arab Emirates
Jason Low, SPRING Singapore
Zainal Abidin Maarif, Central Bank of Malaysia
Winston Poon, CBCP, CBCA, DRI Singapore
Harley Lemons, MBCP, United States Department of Defense
Kelley Okolita, MBCP, Regence Blue Cross Blue Shield

Assistant Coordinators

Ingrid Covaci, New York University
Andrew Frame, New York University
Scott Reutter, New York University

Introduction

Notes from the Coordinator:

Clear communication is an essential part of what we do, yet we all have had experiences in which the same terms are used to describe different situations. For example, which term do you use to describe a fire? Is it an emergency, an incident, an event, a disaster, or all of the above? Sometimes the discrepancies are subtle, sometimes not. In everyday situations, ambiguity can be comical, confusing, or at worst, annoying. In a crisis situation, unclear definitions can be dangerous.

As the oldest and largest organization of its kind, DRI International is an industry thought leader, and our certified professionals and the greater continuity community look to us for guidance. When we were asked to offer a DRI glossary, we took on the challenge. The first question we posed was quite simple: What can we create to best serve the industry? As a nonprofit organization, service is our mission. In answering that question, we soon realized that the industry already has many glossaries and terms. These various documents offer much insight and are already widely used in various parts of the world. Rather than add to the abundant number of existing glossaries, we felt that DRI should act as an arbiter of existing definitions. For this reason, the DRI glossary does not create new definitions. Instead, we selected and presented the best-in-class definitions already in use in the English language.

The process had to be international, inclusive, and apolitical, so we established a volunteer committee of industry leaders to review and vote on the terms and definitions that would ultimately appear in this document. What you see here is the result of nearly two years of effort to build the beginnings of a standard set of terms.. We expect that this will be a living document, subject to revisions and changes. We are eager for your input, as well as the participation of representatives from each of the source documents, as we work to achieve our goal of uniformity in the industry.

I would like to thank everyone who contributed to this tremendous undertaking including the tireless committee members, reviewers, assistant coordinators, and DRI staff. Most of all, I cannot thank Bobby Williams enough for stepping forward when called upon during a meeting of DRI's Professional Development Committee to offer his services as chairperson. I am honored to have worked on this project with such an incredible group of people, and I look forward to working with many more of you as the DRI Glossary evolves along with the industry it serves.

Thanks,
Chloe Demrovsky

Notes from the Chair:

There are times in our lives when a simple question takes on a very complex life of its own. This document was such an undertaking for me. I was asked if I would lead a committee to develop a compilation of glossary terms for DRI International. I thought, “How hard could that be?” Harder than I thought, but also infinitely more rewarding.

You are now reading the result of our undertaking. A document (not a monster!) that we created and are hopeful will have a life of its own for many years to come.

The goal of our committee was to gather as many laws, standards, regulations, organizational best practice guides, and industry periodicals containing definitions relating to business continuity (BC), disaster recovery (DR), or risk management (RM). We took the terms contained in those documents and compiled a glossary of preferred definitions for use by our industry as a definitive source of terminology.

The first task (gathering the resource documents) proved to be pretty straightforward. We compiled a total of 23 documents. These 23 documents contained 2189 unique terms and a total of 2730 terms. The multiple definitions of terms proved to be the real challenge of this project. The committee took several ballots to eliminate some terms that we felt really weren’t specific to BC, DR, or RM. This stage of the process netted 479 unique terms from a total of 876 occurrences in 22 reference documents.

The next task was the most daunting: selecting the best definition across multiple resource documents. After many ballot iterations, negotiations, and gnashing of teeth, we feel that we have succeeded in compiling the most comprehensive glossary of BC, DR, and RM terms in our industry.

But just like a continuity plan, the work is never really done. This document is only the beginning! The long range vision for the glossary is to continue to refine and enhance it. I want to thank the committee members for their efforts on this project. I would also like to thank Chloe Demrovsky, our DRI coordinator. It has been a privilege to be a part of this committee.

Thanks,
Bobby Williams

A

Acción correctiva	Acción para eliminar la causa de una no conformidad y prevenir la recurrencia.
Aceptación del riesgo	Decisión de la gerencia que consiste en no tomar acción alguna para mitigar el impacto de un riesgo particular.
Acreditación	Declaración formal de un organismo acreditador o autorizado que valida la condición de una persona, organización o sistema de información y su facultad para desempeñar determinada actividad o cargo.
Activación	La implementación de procedimientos, actividades y planes de continuidad del negocio en respuesta a un incidente, emergencia, evento o crisis.
Activo	Cualquier componente que tenga valor para la organización. Nota del editor del BCI: Esto puede incluir activos físicos tales como instalaciones, maquinaria y equipos, o bien recursos humanos, propiedad intelectual, imagen interna y externa y reputación. (BCI)
Acuerdo de ayuda mutua	Convenio formalizado entre dos o más entidades para prestar asistencia a las partes del acuerdo.
Acuerdo de Basilea (Basilea III)	Convenio de las instituciones financieras internacionales sobre la evaluación financiera de riesgos y la relación entre capital y riesgo.
Acuerdo de nivel de servicio (SLA por sus siglas en inglés)	Convenio formal entre un proveedor de servicios y su cliente (sean estos internos o externos), que abarca la naturaleza, calidad, disponibilidad, alcance y respuesta del proveedor de servicios. El SLA debe cubrir las situaciones del día a día, así como situaciones de desastre, según vaya cambiando la necesidad del servicio.
Acuerdo recíproco	Convenio entre dos organizaciones (o dos grupos internos de la organización) con equipos/ambientes similares, que permite a cada uno recuperarse en la localidad del otro.
Administración de aplicaciones	Función responsable de administrar las aplicaciones a lo largo de su ciclo de vida. (ITIL)
Administrador del plan de continuidad del negocio	Persona responsable de la documentación, mantenimiento y distribución del plan.
Alcance	Límite que aplica a un proceso, procedimiento, certificación, contrato, etc. y que detalla las especificaciones y responsabilidades de todas las partes para la elaboración de un producto, la entrega de un servicio, un proyecto o cualquier otra actividad en la que debamos realizar una inversión o gasto.
Alerta	Notificación de una situación que podría derivar en una interrupción. Generalmente incluye lineamientos para que el personal se prepare ante una posible activación de los planes.
Almacén de registros vitales	Ubicación a una distancia segura de las instalaciones primarias, en la que se almacenan los datos críticos (computarizados o en papel) y desde la cual se pueden recuperar para su utilización en las instalaciones alternas.

Almacenamiento externo	Cualquier lugar localizado a una distancia significativa del sitio primario donde los registros duplicados y vitales (copias impresas o electrónicas y/o equipos) pueden almacenarse para su uso durante la recuperación.
Alta disponibilidad	Protocolo de diseño de un sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado.
Amenaza	Situación o condición natural u ocasionada por el hombre que puede causar una interrupción de las operaciones o servicios de una organización.
Amenazas ocasionadas por el hombre	Causas de una posible interrupción en las operaciones como resultado de acciones realizadas por el hombre identificadas en la evaluación de riesgos, por ejemplo, empleados inconformes, terrorismo, chantaje, protestas laborales, huelgas, disturbios sociales, etc.
Análisis costo-beneficio	Proceso (después del BIA y la evaluación de riesgos) que facilita, a nivel financiero, las diferentes opciones estratégicas para la gestión de la continuidad y que compara el costo de cada opción con la suma ahorrada.
Análisis de brechas	Proceso comparativo que identifica la diferencia entre el resultado real y el deseado.
Análisis de brechas de seguridad / Monitoreo de amenazas	Proceso de recopilación de información sobre seguridad con el objetivo de identificar posibles violaciones de seguridad de las instalaciones, la operación o los sistemas.
Análisis de causa raíz (RCA por sus siglas en inglés)	Proceso que identifica la causa raíz de un incidente o problema. Generalmente se refiere a fallas de infraestructura de TI.
Análisis de impacto al negocio (BIA por sus siglas en inglés)	Proceso de evaluación de las operaciones y del efecto que una interrupción tendría en ellas. Incluye no sólo el análisis de impacto al negocio, que es la identificación de los activos, funciones, procesos y recursos críticos, sino también la evaluación de los posibles daños o pérdidas que pudieran afectar a la organización como resultado de una interrupción o un cambio en el negocio. Este análisis identifica: a) cómo se va a manifestar la pérdida o daño b) cómo aumenta el grado de daño o pérdida en función del tiempo transcurrido después del incidente c) los servicios y recursos mínimos (humanos, físicos y financieros) necesarios para restablecer los procesos de negocio y seguir operando en un nivel mínimo aceptable d) el tiempo y el nivel en el cual las actividades, funciones y servicios de la organización deben ser recuperados
Análisis de riesgos	Proceso de cuantificación de las amenazas a una organización y la probabilidad de que se materialicen.
Apetito de riesgo	El apetito es el nivel de riesgo que la empresa está dispuesta a aceptar, tolerar o estar expuesta en cualquier punto en el tiempo. Su tolerancia será la desviación respecto a ese nivel de riesgo. La capacidad será el nivel máximo de riesgo que una organización puede soportar en la consecución de sus objetivos.
Aplicación	Software que realiza una función específica y que se puede ejecutar sin que el usuario cuente con privilegios de administrador del sistema.

Árbol de llamadas	Documento que describe gráficamente las responsabilidades y el orden en que deben producirse las llamadas a los diferentes niveles de la organización, así como a los clientes y proveedores y otros contactos clave en caso que se produzca una emergencia, catástrofe o situación de indisponibilidad grave. En la actualidad, los árboles de llamadas pueden generarse y activarse a través de un software especializado.
Área alterna de trabajo	Ambiente preparado para la recuperación, con los elementos críticos requeridos por una estación de trabajo (por ejemplo, escritorio, teléfono, hardware, software, comunicaciones, entre otros). (DRJ)
Arquitectura	Estructura de un sistema o un servicio de TI que incluye las relaciones de sus componentes y el ambiente en el que se encuentran. También incluye los estándares y los lineamientos que rigen el diseño y la evolución del sistema.
Ataque cibernético	Intromisión al entorno informático de una organización a través del espacio cibernético con el fin de interrumpir, desactivar, destruir o controlar malintencionadamente un entorno informático o de infraestructura, destruir la integridad de los datos o robar información.
Auditor	Persona con competencias para llevar a cabo una auditoría.
Auditoría	Revisión sistemática para determinar si las actividades y sus resultados cumplen con los planes existentes y si estos se aplican eficazmente y son adecuados para cumplir con la política y los objetivos de la organización. Una auditoría puede ser: a.- Interna: llevada a cabo por el personal de la propia organización b.- Externa: llevada a cabo por un tercero especializado. En continuidad del negocio, se puede realizar con el objetivo de validar que el plan cumple con las mejores prácticas o para obtener una certificación
Auditoría interna	Ver Auditoría
Autenticación	Proceso de verificación de la identidad u otros atributos asumidos por una entidad (usuario, proceso o dispositivo) o bien la verificación del origen y la integridad de los datos. A menudo es un prerrequisito para permitir el acceso a los recursos en un sistema de información.
Autorización	Privilegio otorgado a un usuario para acceder a un programa o realizar un proceso.

B

Benchmarking	Proceso para la rigurosa medición del desempeño respecto a las mejores compañías en su ramo, así como el uso del análisis para conocer y alcanzar el nivel del líder. Búsqueda de las mejores prácticas que conducen a un desempeño superior.
Brigada de Emergencia	Término utilizado en algunos países de América Latina. Ver Equipo de Respuesta a Emergencias

C

Cadena de suministros	Serie de procesos vinculados desde la adquisición de materia prima hasta la entrega de productos o servicios al usuario final a través de los medios de transporte. Incluye proveedores, vendedores, plantas de producción, proveedores de logística, centros internos de distribución, distribuidores, mayoristas y otras entidades orientadas al usuario final.
Capacidad	Propiedad de un individuo, organización o comunidad relacionada con las fortalezas, atributos y recursos disponibles para desempeñar una determinada tarea o cometido. La evaluación de la capacidad es un término que designa el proceso por el cual se compara la capacidad de un grupo contra los objetivos deseados, identificando así brechas que requieren una acción futura.
Capacitación/Entrenamiento	Proceso por el cual se enseñan habilidades y conocimientos orientados a la realización de una actividad específica de manera competente o calificada. Mientras que la concientización está generalmente dirigida a todo el personal, la capacitación está dirigida al personal con funciones y responsabilidades específicas.
Cartera de aplicaciones	Base de datos o documento estructurado que se usa para gestionar las aplicaciones en su ciclo de vida. Contiene atributos clave para todas las aplicaciones. Algunas veces se implementa como parte de la cartera de servicios o del sistema de gestión de la configuración.
Categorías de riesgo	Tipos de riesgo similares son agrupados bajo un título clave, también conocido como "categorías de riesgo". Estas categorías incluyen reputación, estrategia, financieros, inversiones, infraestructura operativa, negocio, cumplimiento regulatorio, subcontratación, personas, tecnología y conocimientos.
Causa raíz	Causa original de un incidente o problema.
Centro de comando de incidentes	Ubicación cercana al lugar en el que se produjo el evento desde la cual se monitorean y controlan las actividades de respuesta a la emergencia.
Centro de operaciones de emergencia o COE (EOC por sus siglas en inglés)	Ubicación física o virtual desde la cual se gestiona la crisis y se toman decisiones estratégicas orientadas a la continuidad y recuperación de operaciones. El centro de comando de incidentes le reporta al COE.
Checklist	a. Herramienta para recordar o validar que las tareas se han completado y los recursos están disponibles y para informar sobre el estatus de la recuperación. b. Lista de elementos (nombres, tareas, etc.) que deben ser verificados.
Ciclo de vida de la gestión de la continuidad del negocio	Conjunto de actividades que cubren todos los aspectos y fases del programa de gestión de continuidad del negocio.
Cold Site	Ubicación alterna que cuenta con la infraestructura necesaria para la operación de un centro de cómputo, pero no dispone de ningún hardware de computadora, equipos de telecomunicaciones, líneas de comunicación, etc. preinstalados. Estos deben ser adquiridos o instalados en el momento de producirse el desastre. También puede ser utilizado como sitio alterno para recuperar las funciones del negocio.

Comité directivo de continuidad del negocio	Grupo directivo responsable de dar dirección, asesoría y guía y aprobar los recursos financieros y materiales necesarios del programa de continuidad. En tiempos de crisis, se convierte en el comité de manejo de crisis.
Concientización en continuidad del negocio	Proceso orientado a que las personas se familiaricen con las responsabilidades y los conceptos relacionados con la continuidad del negocio a través de la observación o de la práctica, propiciando de esta manera cambios de conducta.
Confidencialidad	Propiedad por la cual se permite el acceso a la información únicamente a personas previamente autorizadas.
Continuidad	Capacidad estratégica y táctica de una organización, previamente aprobada por la administración, para planificar y responder a las condiciones, situaciones y eventos con el fin de continuar las operaciones a un nivel aceptable predefinido. ASIS Nota del Editor: La continuidad, tal como se utiliza en la presente Norma, es el término más general para la continuidad operativa y comercial para garantizar la capacidad de una organización y seguir operando fuera de las condiciones normales de funcionamiento. Se aplica no sólo a las empresas de lucro sino a organizaciones de cualquier naturaleza tales como organizaciones no gubernamentales, de interés público y organizaciones gubernamentales. (ASIS)
Continuidad del negocio	Capacidad de una organización para continuar con la entrega de sus productos o servicios después de una interrupción a un nivel predefinido aceptable.
Control	Medios de gestión de riesgos, como políticas, procedimientos, directrices, prácticas o estructuras organizacionales, que pueden ser de carácter administrativo, técnico, de gestión o legal. (ISACA)
Controles de seguridad	Procedimientos de gestión, operativos y técnicos, implementados para un sistema de información con el fin de proteger la confidencialidad, integridad y disponibilidad del sistema y su información. En español, el término se puede utilizar además en relación con la seguridad física y la protección de las personas.
Coordinador de continuidad del negocio	Persona responsable de planificar, desarrollar, implementar, difundir y gestionar el programa de continuidad del negocio.
Coordinador departamental de continuidad	Miembro que actúa como enlace y que es responsable del plan de continuidad de su departamento.
Crisis	Evento crítico que, si no se maneja de manera adecuada, podría afectar drásticamente la rentabilidad, reputación o capacidad operativa de una organización, o bien, un suceso o percepción de amenaza a las operaciones, al personal, los accionistas, las partes interesadas, la marca, la reputación y la confianza o los objetivos estratégicos o de negocio de una organización.
Criterios de riesgo	Términos de referencia contra los cuales se evalúa la importancia de un riesgo.

Cronograma de recuperación del negocio	Secuencia o representación gráfica en función del tiempo, de un conjunto de actividades a implementar tras una interrupción. Puede variar de minutos a semanas, dependiendo de los requisitos de recuperación y de la metodología.

D

Debido cuidado	Uno de los requisitos del gobierno corporativo relacionado con el cuidado de los activos de la organización; un deber que incumbe a los directivos de una organización.
Declaración	Anuncio formal por parte del personal previamente autorizado de que se prevé o se ha producido un desastre o una interrupción grave con el consecuente despliegue de acciones de mitigación predeterminadas (por ejemplo, desplazamiento a una ubicación alterna).
Degradación de servicio	Estrategia de recuperación que consiste en que los servicios TI se proporcionen con un menor nivel de servicio o tiempo de respuesta.
Delegación de autoridad	Cesión de funciones de mando a otras personas de niveles subordinados.
Denegación de servicio (DoS por sus siglas en inglés)	Ataque a un sistema de computadoras o a una red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
Departamento/Área/Función del negocio	Conjunto de actividades que se desarrolla para cumplir con los requisitos específicos de una organización. Algunos ejemplos son: Contabilidad, Finanzas, Recursos Humanos, TI, etc.
Dependencia	Relación o interacción de una actividad o proceso con respecto a otro.
Desastre	Acontecimiento catastrófico repentino (previsto o imprevisto) que causa daños o pérdidas inaceptables.
Detonante	Suceso que causa la activación de una respuesta.
Disponibilidad	Característica que permite que los datos estén accesibles de acuerdo a los niveles de servicio acordados.
Distribución automática de llamadas (ACD por sus siglas en inglés)	Redireccionamiento de llamadas telefónicas entrantes a la persona adecuada en el menor tiempo posible con el apoyo de la tecnología. También se conoce como distribución automatizada de llamadas.
Documento	Información y su medio de soporte (papel, dispositivos magnéticos, ópticos o electrónicos o de imagen).
***Downtime*/Tiempo de inactividad**	Período en el que un servicio o sistema no está operando como resultado de una interrupción.
***Downtime* aceptable**	Tiempo máximo sin operaciones que una organización está dispuesta a tolerar, desde el momento de la interrupción hasta la restauración.

E

Ejercicio	En su definición original en inglés, los ejercicios están orientados a las personas y las pruebas a los componentes físicos (sistemas, equipos, etc.). En América Latina se usa indistintamente la palabra "prueba" para ambos conceptos.
Emergencia	1. Situación inesperada que puede derivar en lesiones o muerte, daño a la propiedad o interrupción de la operación normal de una organización. 2. Suceso imprevisto y repentino que requiere de una acción inmediata.
Emergencia nacional	Situación que supone una amenaza a gran escala al bienestar de la población civil o a la protección de una o varias comunidades y de la cual se tiene que hacer cargo el sector público.
Equipo de continuidad del negocio	Grupo de personas responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución de los planes de continuidad de la organización.
Equipo de gestión de incidentes (IMT por sus siglas en inglés)	Grupo de personas capacitadas responsables del desarrollo y la implementación, a través de la toma de decisiones, del plan de respuesta a incidentes.
Equipo de manejo de crisis (CMT por sus siglas en inglés)	Grupo directivo responsable de la toma de decisiones estratégicas relacionadas con la continuidad y la recuperación tras una interrupción y de la gestión de la comunicación interna y externa, teniendo siempre en cuenta la imagen de la organización. Es el único equipo autorizado para activar los planes y todos los equipos que son activados en un incidente deben reportarle. En operación normal se denomina Comité directivo de continuidad del negocio y en operación de contingencia se denomina Equipo de manejo de crisis.
Equipo de recuperación del negocio	Grupo de personas del área de TI responsables del desarrollo, implementación, pruebas, mantenimiento y ejecución del plan de recuperación de desastres.
Equipo de respuesta a emergencias (ERT por sus siglas en inglés) / Brigada de emergencia	Grupo de personas que generalmente integran la brigada de emergencia y han sido entrenadas para proporcionar asistencia inmediata en una emergencia.
Escalación	Proceso por el cual la información relacionada con un evento es comunicada al nivel superior a través de la cadena de mando de una organización con la finalidad de involucrar a los niveles de decisión adecuados.
Escenario	Diseño de una serie de condiciones ficticias, pero probables, con base en un análisis de riesgos previo, que podrían generar una interrupción, alteración o pérdida relacionada con algún aspecto de las operaciones de una organización y que se utiliza en el desarrollo de una prueba de continuidad o recuperación. Generalmente, el diseño del escenario es responsabilidad del coordinador de continuidad del negocio.

Estrategia de continuidad del negocio	Curso de acción definido previamente (y aprobado por el comité directivo) con el fin de proteger la viabilidad de la empresa y reanudar sus actividades críticas en los plazos establecidos. Las estrategias seleccionadas deben cubrir los RTOs identificados en el BIA.
Estrategias de recuperación	Curso de acción definido previamente (y aprobado por el comité directivo) con el fin de asegurar la reanudación de los servicios y los sistemas críticos de TI (con base en los RTOs identificados en el BIA).
Evacuación	Proceso de desalojo de personas para alejarlas de áreas peligrosas en una ubicación, de forma organizada, supervisada y por fases, generalmente coordinado por brigadistas.
Evaluación	Inspección y análisis para verificar el cumplimiento de un estándar o un conjunto de lineamientos, por ejemplo, la validez de los registros o el cumplimiento de las metas de eficiencia y efectividad. (ITIL)
Evaluación de daños	Proceso de estimación o determinación de los efectos de un incidente sobre las personas, el medio ambiente, los activos y la operación de una organización.
Evaluación de vulnerabilidades	Revisión sistemática de un sistema de información o producto para determinar la suficiencia de las medidas de seguridad, identificar deficiencias de seguridad, proporcionar datos para predecir la eficacia de las medidas de seguridad propuestas y confirmar que tales medidas son idóneas después de la implementación. (CNSSI-4009)
Evaluación y control de riesgos	Proceso para identificar los riesgos de una organización, evaluar las funciones esenciales necesarias para continuar las operaciones del negocio, definir los controles necesarios para reducir la exposición de la organización y evaluar el costo de dichos controles. Con frecuencia implica una evaluación de la probabilidad de ocurrencia de un evento en particular.
Evento/Incidente	Suceso que origina una interrupción o que posee el potencial para generar una interrupción.
Evidencia de auditoría	Serie de documentos, archivos u otros elementos de información que se examinan durante una auditoría y que muestran cómo se maneja la operación de una organización.

F

Failover	Capacidad de cambiar automáticamente (generalmente sin intervención humana o advertencia) a un sistema de información redundante debido al fallo o terminación anormal del sistema activo.
Falla	Pérdida de la habilidad para operar de acuerdo a las especificaciones establecidas o para entregar el resultado esperado. El término "falla" puede ser utilizado cuando nos referimos a servicios de TI, procesos, actividades, elementos de configuración, etc. Una falla a menudo causa un incidente.
Funciones críticas	Actividades esenciales ejecutadas por las organizaciones, especialmente después de una interrupción de sus actividades normales.

G

Gerente de tecnologías de información (CIO por sus siglas en inglés)	Persona responsable de: a. Proporcionar asesoramiento y otro tipo de asistencia para el gerente de la organización y para otros miembros de la alta dirección de la organización, con el objetivo de asegurar que los sistemas de información son adquiridos y los recursos de información son gestionados de modo consistente con las leyes, órdenes ejecutivas, directivas, políticas, reglamentos y las prioridades establecidas por el gerente; b. Desarrollar, mantener y facilitar la implementación de una arquitectura de sistemas de información integrada y sólida para la organización; y c. Promover el efectivo y eficaz diseño y operación de los principales procesos de gestión de recursos de información de la organización, incluyendo las mejoras en los procesos de trabajo de la misma. (CNSSI-4009)
Gestión de activos	Función responsable de dar seguimiento e informar del valor de los activos financieros en todo su ciclo de vida. Forma parte de los servicios de activos y del proceso de gestión de la configuración. (ITIL)
Gestión de continuidad del negocio (BCM por sus siglas en inglés)	Proceso holístico que tiene como función identificar las posibles amenazas a la organización y los impactos resultantes si estas amenazas se materializaran, y que proporciona un marco para incrementar la resiliencia organizacional y, como consecuencia, la capacidad de una respuesta efectiva que proteja los intereses de las partes interesadas clave, la reputación, la marca y las actividades que generan valor.
Gestión de desastres/emergencias	1. Un proceso continuo de prevención, mitigación, estar preparado, de respuesta. 2. Mantener la continuidad durante la emergencia y recuperación de un incidente que amenaza la vida, la propiedad, las operaciones, o el medio ambiente. (NFPA 1600) 3. Programa que implementa la misión, la visión, los objetivos estratégicos, los objetivos y el marco de gestión del programa y de la organización. (BCI)
Gestión de emergencias	Gestión de emergencias es responsabilidad de los gobiernos y de las autoridades del sector público cumpliendo con las regulaciones y leyes relacionadas con la respuesta a emergencias. [BCI]
Gestión de incidentes	Proceso mediante el cual una organización responde y controla un incidente utilizando procedimientos o planes de respuesta de emergencia. (DRJ)
Gestión de recursos	Proceso para identificar los recursos disponibles y tener acceso oportuno a aquellos necesarios para prevenir, mitigar, preparar, responder y mantener la continuidad durante un incidente o en el proceso de recuperación.
Gestión de riesgos	Desarrollo estructurado y aplicación de la cultura de gestión, a través de políticas, procedimientos y prácticas por medio de la definición de actividades para la identificación, análisis, evaluación y control de los riesgos.

Gestión de riesgos empresariales (ERM por sus siglas en inglés)	Proceso llevado a cabo por el comité directivo y otros ejecutivos, orientado a la definición de la estrategia y que aplica a toda la organización, diseñado tanto para identificar eventos que puedan afectar a la organización como para gestionar los riesgos que forman parte de su apetito al riesgo, y que tiene como objetivo proporcionar una garantía razonable relacionada con el logro de los objetivos de la organización. Generalmente se evalúan en términos de probabilidad y magnitud del impacto, para poder así determinar una respuesta estratégica y monitorear su progreso.
Gestión del cambio	Enfoque sistemático para hacer frente a los cambios, tanto desde una perspectiva organizacional como individual.
Gobierno	Función a través de la cual una organización se asegura de que las políticas y la estrategia se están implementando y de que los procesos requeridos se siguen correctamente. Incluye la definición de funciones y responsabilidades, mediciones y estructura de reporte, y la toma de decisiones para resolver los problemas identificados.
Gobierno corporativo	Sistema o proceso por el cual se requiere que los directores de una organización lleven a cabo y cumplan sus responsabilidades y obligaciones legales, morales y regulatorias.
Gobierno, riesgo y cumplimiento (GRC por sus siglas en inglés)	GRC es el término general que abarca el enfoque de una organización sobre el riesgo y éstas tres áreas. Interpretado de manera diferente en distintas organizaciones, GRC típicamente incluye actividades como gobierno corporativo, gestión de riesgo empresarial (ERM por sus siglas en inglés) y cumplimiento corporativo con las leyes y reglamentos aplicables. (BCI)

H

Hot site	Ubicación alterna que ya cuenta con el equipo de cómputo, los servidores, las telecomunicaciones y la infraestructura ambiental necesarios para recuperar las funciones del negocio o los sistemas de información críticos.

I

Impacto	Efecto, aceptable o no, que un evento tiene en una organización. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos, dependiendo del sector.
Incidente	Suceso que tiene el potencial para generar una interrupción, alteración, pérdida, emergencia, crisis, desastre o catástrofe.
Infraestructura crítica	Componentes físicos o servicios de apoyo que sirven de base para la operación y que si dejaran de funcionar o fueran destruidos, provocarían un impacto que afectaría gravemente a una organización, comunidad, nación, etc.
Instalación	Planta, maquinaria, equipos, inmuebles, edificios, vehículos, sistemas de información, facilidades de transporte y otros artículos de la infraestructura o de la planta y los sistemas relacionados que tienen una función o servicio distinto y cuantificable.(BCI) Edificio permanente, disponible para su uso cuando es necesario para el Plan de Continuidad del Servicio de TI. [ITIL]
Instalación de respaldo	Una instalación "fallback" es otro sitio o edificio que puede ser utilizado cuando el sitio original no se puede utilizar o no está disponible. Término utilizado también para indicar un plan alternativo, plan B o plan de respaldo y como último recurso alternativo
Instalaciones primarias	Ubicación en donde se desarrollan las operaciones cotidianas en tiempos de operación normal.
Integridad de los datos	Propiedad que garantiza que los datos no se han modificado, destruido o perdido debido a acciones no autorizadas o accidentales.
Interdependencias	Relación por la cual dos o más procesos o aplicaciones están vinculados entre sí para su funcionamiento, es decir, uno de ellos es proveedor del otro.
Interrupción	Evento que detiene las funciones, operaciones o procedimientos habituales de la organización, sea éste previsto (por ejemplo, huracanes, disturbios políticos) o imprevisto (por ejemplo, un apagón, un ataque terrorista o una falla de la tecnología).

J

Just-in-time (JIT)	Sistema que permite obtener los materiales, los recursos o la información de los que dependen los procesos críticos del negocio exactamente en el momento en que son requeridos, sin necesidad de mantener un inventario intermedio.

M

Manejo de crisis	Proceso por el cual una organización dirige una serie de actividades ante una interrupción que amenaza a la organización, a las partes interesadas y al público en general, con el objetivo de evitar o reducir al mínimo el daño a la rentabilidad, la imagen y la capacidad operativa de la organización.
Mantenimiento del plan	Proceso de gestión por el cual se asegura la actualización, vigencia y pertinencia de la información relacionada con la continuidad.
Medidas preventivas	Controles para impedir eventos no deseables o mitigar sus efectos.
Mejora continua	Proceso recurrente de optimización del programa de gestión con el fin de lograr mejoras en el rendimiento general de manera consistente con la política, las metas y objetivos de la entidad.
Mejores prácticas	Conjunto de actividades o procesos que han sido aplicados con éxito en un determinado contexto y que se espera que, en contextos similares, rindan resultados similares.
Métrica	Medición de un proceso, servicio o actividad de TI y reporte de los resultados para apoyar su gestión. (ITIL)
Misión	Descripción completa, pero breve, del propósito y las intenciones globales de la organización. Se establece lo que debe ser alcanzado, pero no cómo debe hacerse.
Mitigación de riesgos	Priorización, evaluación e implementación de controles o medidas de reducción de riesgos apropiadas recomendadas en el proceso de gestión de riesgos.
Mitigación del riesgo	Decisión informada para no involucrarse o retirarse de una situación de riesgo. (BCI)
Modelo de madurez de la continuidad del negocio (BCMM por sus siglas en inglés)	Metodología que permite evaluar el nivel de preparación de una organización en función de su plan de continuidad del negocio.
Monitoreo activo	Proceso por el cual se revisa continuamente y de manera automatizada el comportamiento de un elemento de configuración o de un servicio de TI.
Movilización	Desplazamiento del personal involucrado en las actividades de recuperación a las diversas ubicaciones alternas una vez que se ha activado el plan.

N

Nivel de preparación	Grado de conocimiento y capacidad de actuación ante un evento inesperado que pudiera derivar en una interrupción de las operaciones. Aplica tanto a nivel organización como individual.
Norma/Estándar	1. Descripción detallada, elaborada con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado. Para efectos de una certificación, la norma se vuelve obligatoria. 2. Un requisito obligatorio. Algunos ejemplos: ISOIIEC 20000 (norma internacional), estándar de seguridad interna para la configuración de Unix, o un estándar del gobierno que establece cómo deben mantenerse los registros financieros. El término "norma" también se utiliza para referirse a un código de práctica o especificación publicado por una organización de estándares, como ISO o BSI.

O

Objetivo de punto de recuperación (RPO por sus siglas en inglés)	Punto de referencia anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Cada organización deberá definir su "pérdida máxima de información".
Objetivo de tiempo de recuperación (RTO por sus siglas en inglés)	Periodo inmediatamente posterior a la ocurrencia de un incidente dentro del cual deben reanudarse o recuperarse: — la entrega de productos o servicios — las actividades críticas — los recursos NOTA: El RTO debe ser menor al tiempo en el que los impactos financieros y operacionales identificados en el BIA sean inaceptables.
Objetivo del negocio	Meta de un proceso de negocio o de la organización en general.

P

Pandemia	Enfermedad epidémica o infecciosa que puede tener un impacto a nivel mundial.
Partes interesadas	Individuo o grupo que tiene un interés en el desempeño o éxito de una organización, por ejemplo, clientes, socios, empleados, accionistas, propietarios, la comunidad local, organizaciones del primer nivel de respuesta, gobierno o instituciones regulatorias.
Peligro	Fenómeno, sustancia, actividad humana o condición peligrosa que puede causar la pérdida de vidas, lesiones u otros impactos a la salud, así como daños a la propiedad, pérdida de servicios, trastornos sociales y económicos o daños ambientales. Nota del Editor del UNDR: Los peligros de interés para la reducción del riesgo de desastres como indicados en la nota 3 del marco de referencia de Hyogo son "... peligros de origen natural y los peligros ambientales y tecnológicos relacionados." Tales riesgos se derivan de una variedad de características geológicas, meteorológicas, hidrológicas, fuentes oceánicas, biológicas y tecnológicas, actuando a veces en combinación. En ajustes técnicos, los riesgos se describen cuantitativamente por la frecuencia probable de ocurrencia de diferentes intensidades para diferentes áreas, como se determina a partir de datos históricos o análisis científico. (UNDR)
Peligro biológico	Propiedad que tiene alguna actividad, servicio o substancia, de producir efectos nocivos o perjudiciales en la salud humana. (Protección Civil - México)
Peligro natural	Proceso o fenómeno natural que tiene lugar en la biosfera que puede resultar en un evento perjudicial y causar la muerte o lesiones, daños materiales, interrupción de la actividad social y económica o degradación ambiental. CENAPRED (Centro Nacional de Prevención de Desastres - México)
Peligro tecnológico	Amenaza originada por accidentes tecnológicos o industriales, procedimientos peligrosos, fallos de infraestructura o de ciertas actividades humanas, que pueden causar muerte o lesiones, daños materiales, interrupción de la actividad social y económica o degradación ambiental. Algunos ejemplos son: contaminación industrial, radiación nuclear, desechos tóxicos, rupturas de presas, accidentes de transporte, explosiones de fábricas, incendios y derrames químicos. También pueden generarse directamente como resultado de la materialización de un riesgo de origen natural.
Pérdidas	Recursos irrecuperables como consecuencia de una interrupción. Puede referirse a vidas, ingresos, participación en el mercado, imagen pública, instalaciones o capacidad operativa.
Plan de contingencias	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, que serán utilizados en incidentes menores que afecten únicamente la operación (no a las personas) cuya duración sea menor al RTO.
Plan de continuidad de operaciones (COOP por sus siglas en inglés)	Plan de continuidad del sector público en Estados Unidos.

Plan de continuidad del negocio (BCP por sus siglas en inglés)	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para ser ejecutados después de una interrupción de las operaciones, con el objetivo de cumplir con la entrega de los productos y servicios críticos a un nivel aceptable y dentro de los marcos de tiempo predefinidos.
Plan de manejo de crisis	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para enfrentar un incidente mayor o crisis. Ver definición de "crisis". El responsable de su desarrollo e implementación es el comité directivo.
Plan de recuperación ante desastres (DRP por sus siglas en inglés)	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para la recuperación del componente tecnológico, sistemas y servicios de telecomunicaciones.
Plan de respuesta a emergencias	Documento que contiene un conjunto de acciones y procedimientos definidos previamente, con responsabilidades claramente establecidas, para estabilizar un incidente que ponga en riesgo las vidas y la propiedad.
Plan de sucesión de gestión ejecutiva	Documento que permite asegurar la continuidad de la autoridad, la toma de decisiones y la comunicación en caso de que, repentinamente, algún miembro clave de la dirección no pueda ejercer sus funciones.
Plan del ejercicio	Ver Planificación de la prueba
Planificación de contingencias	Proceso de elaboración de acuerdos y procedimientos avanzados que permiten a una organización responder a un evento no deseado que repercute negativamente en la organización. (DRJ)
Planificación de continuidad del negocio	Proceso de desarrollar procedimientos y lineamientos que permitan a las organizaciones responder a una interrupción, de tal manera que las funciones críticas del negocio puedan continuar dentro de los niveles acordados. El resultado final del proceso de planificación es el plan de continuidad del negocio. (BCI)
Planificación de la prueba	Programación de las diversas actividades que serán llevadas a cabo antes, durante y después de la prueba con el objetivo de evaluar los componentes del plan, por ejemplo, las tareas, equipos y procedimientos.
Planificación de recuperación ante desastres	Actividades asociadas con la planificación para la disponibilidad continua y restauración de la infraestructura de TI. (BCI)
Política de continuidad del negocio	Marco de referencia que establece los objetivos, los principios y el enfoque de la gestión de continuidad de una organización, los productos y servicios de la misma y cómo serán entregados, y las funciones y responsabilidades principales de la gestión de continuidad y cómo se reportará el estatus a la dirección ejecutiva.
Póliza todo riesgo	Seguro en el que, respecto al objeto asegurado, se garantizan conjunta y simultáneamente todos los riesgos que puedan afectarle, excepto los riesgos explícitamente excluidos de la póliza. Ver Todos los peligros
Preparación	Actividades implementadas antes de un incidente que pueden ser utilizadas para apoyar y mejorar la mitigación de interrupciones, así como la respuesta y recuperación ante las mismas. (BCI)
Preparación ante emergencias	Situación en la que se encuentra una organización o comunidad en relación con su capacidad de respuesta a una emergencia de forma coordinada, oportuna y efectiva, con el fin de minimizar el daño a las personas y a la propiedad.

Prevención	Medidas que permiten a una organización evitar, impedir o reducir el impacto de un incidente.
Primer nivel de respuesta	Personas o instituciones de algún servicio de emergencia del sector público que llegan primero a la escena de una emergencia. Generalmente es la policía, los bomberos o los servicios médicos de emergencia.
Prioridad	Categoría utilizada para identificar la importancia relativa de un incidente, problema o cambio. Está basada en el impacto y la urgencia, y se utiliza para identificar los tiempos requeridos en las acciones a seguir. Por ejemplo, un acuerdo de nivel de servicio (SLA por sus siglas en inglés) puede especificar los incidentes prioritarios que deben resolverse en un plazo máximo de 12 horas.
Probabilidad	Posibilidad verosímil y fundada de que algo suceda, haya sido esto definido, medido o estimado objetiva o subjetivamente. Se pueden utilizar términos descriptivos generales (tales como "improbable", "poco probable", "probable", "casi seguro"), frecuencias o probabilidades matemáticas. Puede ser expresado cualitativa o cuantitativamente.
Procedimientos de recuperación	Acciones documentadas necesarias para restaurar los datos de un sistema de información y la capacidad de cómputo después de una falla del sistema.
Procedimientos manuales	Método alternativo de trabajo en el que no se utilizan los sistemas o el software que regularmente está disponible. Las medidas y métodos de trabajo provisionales ayudan a mitigar el impacto de un evento durante un periodo corto.
Proceso de negocio	Secuencia de procedimientos interdependientes y vinculados que contribuyen a la entrega de un producto o servicio. Algunos ejemplos son pago de nómina, reclutamiento y selección de personal, cuentas por cobrar, etc.
Programa	Grupo de iniciativas relacionadas que se gestionan en forma coordinada, con el fin de obtener un nivel de control y los beneficios que no serían posibles a partir de la gestión individual de las iniciativas. Los programas pueden incluir elementos de trabajos relacionados fuera del alcance de las iniciativas distintas del programa. (FCD-1)
Programa de continuidad del negocio	Proceso de gestión y gobierno en curso, que es apoyado por la alta dirección, con los recursos adecuados para implementar y mantener la gestión de continuidad del negocio. (ISO 22301)
Programa de gestión de continuidad del negocio	Proceso de gestión y gobierno continuo que cuenta con el apoyo de la alta dirección y con los recursos apropiados para asegurar que se toman las medidas necesarias para identificar el impacto de pérdidas potenciales, mantener planes y estrategias viables de recuperación y asegurar la continuidad de productos y servicios a través de la capacitación, las pruebas y ejercicios y la actualización. En general, en América Latina los términos "programa de gestión de la continuidad del negocio" y "sistema de gestión de la continuidad del negocio" se usan indistintamente.
Proveedor/Suplidor	Ver Suplidor/Proveedor
Proveedor/Suplidor de Servicios	Ver Suplidor/Proveedor de servicios
Prueba	Simulación de una interrupción de las operaciones para evaluar los componentes de un plan (por ejemplo, tareas, equipos y procedimientos) con el objetivo de comprobar su viabilidad.

Prueba a gran escala/Prueba integral	Ejecución de todos los planes y procedimientos de recuperación de la organización completa. Evaluación de las capacidades alternas de operación en un ambiente altamente estresado. Eventualmente, se podría involucrar al sector público.
Prueba de escritorio	Método de ensayo para ejercitar los planes, en el que los participantes revisan y discuten los planes de acción y procedimientos sin ejecutarlos, en un ambiente seguro y libre de estrés. Puede llevarse a cabo con uno o varios equipos o departamentos. Por lo general, requiere la guía de un facilitador.
Prueba de recuperación ante desastres	Método de ensayo o ejecución (dependiendo del objetivo y el alcance definido para el ejercicio) de los planes de acción y procedimientos de recuperación de los servicios de TI y telecomunicaciones.
Prueba del árbol de llamadas	Proceso manual o automatizado para validar la información contenida en el árbol de llamadas.
Prueba funcional	Ejecución de los planes y procedimientos de recuperación de un área o línea del negocio.
Prueba paso a paso	Método similar a la prueba de escritorio en el que se siguen todos los pasos del plan y sólo se ejecutan algunas acciones seleccionadas en la planificación de la prueba.
Punto único de falla (SPOF por sus siglas en inglés)	Componente único que forma parte de un sistema o proceso, y que en caso de falla, detendría completamente dicho sistema o proceso. Deberían ser identificados en cualquier sistema o proceso con un objetivo de alta disponibilidad.

R

Reanudación	Conjunto de actividades orientadas a retomar o continuar las funciones y operaciones predefinidas del negocio después de una interrupción.
Recuperación	Actividades y programas diseñados para regresar las condiciones a un nivel que sea aceptable para la entidad. (NFPA 1600)
Recuperación ante desastres (DR por sus siglas en inglés)	Capacidad de una organización para recuperar y restablecer el componente TI (infraestructura, telecomunicaciones, sistemas, aplicaciones y datos) después de una interrupción. Aspecto tecnológico de la continuidad del negocio.
Recuperación de datos	Restauración de los archivos de la computadora desde dispositivos de copia de seguridad, con el objetivo de restaurar programas y datos de producción al estado que tenían en el momento de la última copia de seguridad segura, almacenada en el exterior.
Red alterna de comunicaciones	Respaldo de la red de comunicaciones primaria en caso de su indisponibilidad.
Reducción de riesgos	Aplicación selectiva de técnicas y principios de gestión adecuados para reducir la probabilidad de la ocurrencia de una interrupción o mitigar su impacto, o ambos.
Reducción del riesgo de desastre	Concepto y práctica de reducir el riesgo de desastres mediante esfuerzos sistemáticos dirigidos al análisis y a la gestión de los factores causales de los desastres, lo que incluye la reducción del grado de exposición a las amenazas, la disminución de la vulnerabilidad de la población y la propiedad, una gestión sensata de los suelos y del medio ambiente, y el mejoramiento de la preparación ante los eventos adversos. (UNISDR)
Redundancia	Estrategia para duplicar recursos, ya sean tecnológicos, físicos o humanos, cuando el recurso original es único y crítico. Este concepto está relacionado con el punto único de falla.
Registros vitales	Información, en formato electrónico o físico, que es esencial para preservar, continuar o recuperar las operaciones de la organización y para proteger los derechos de la organización y a sus empleados, clientes y partes interesadas.
Remediación	Acción enfocada a la solución de un problema determinado ante un evento. Ejemplo: identificar un nuevo sitio para reubicar un equipo que fue dañado por causa de una inundación.
Resiliencia	Capacidad de una organización para mantener sus funciones y su estructura críticas ante cualquier cambio interno o externo y regresar a un nivel aceptable de rendimiento en un periodo mínimo después de una interrupción.
Respaldo	En TI, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
Respuesta a emergencias	Reacción inmediata y acciones posteriores ante una situación inesperada, con el objetivo de proteger vidas y reducir la severidad del impacto. Dependiendo del evento, las autoridades del sector público tienen la responsabilidad de cumplir con las regulaciones y leyes relacionadas con esta respuesta.

Respuesta a incidentes	Conjunto de acciones realizadas por una organización ante un desastre u otro evento importante que pueda afectar significativamente a la organización, a su gente o su capacidad de operación normal. Puede incluir: evacuación, activación de un DRP, evaluación de daños o cualquier otra medida necesaria para llevar a la organización a un estatus más estable.
Restauración	Proceso para la reparación de los daños ocasionados por el incidente, por ejemplo, instalaciones físicas, hardware, activos y estaciones de trabajo entre otros, con el fin de regresar al sitio primario y, en consecuencia, a las operaciones normales.
Retorno de la inversión (ROI por sus siglas en inglés)	Medición de los beneficios esperados de una inversión. En el sentido más simple, es el beneficio neto de una inversión dividida por el valor neto de los activos invertidos.
Riesgo	Probabilidad de que se presente un evento que pudiera causar daños o pérdidas o afectar la capacidad para alcanzar los objetivos del negocio, asociado a la vulnerabilidad de la organización ante esa amenaza. En el contexto de gestión del riesgo corporativo, riesgo se refiere al potencial de que el resultado de una acción o actividad (incluyendo la no acción) resulte en un resultado diferente.
Riesgo aceptable	Nivel de pérdida que una sociedad o comunidad considera aceptable, con base en sus condiciones sociales, económicas, políticas, culturales, técnicas y ambientales existentes.
Riesgo de desastre	Posibles pérdidas que ocasionaría un desastre en términos de vidas, las condiciones de salud, los medios de sustento, los bienes y servicios, y que podrían ocurrir en una comunidad o sociedad particular en un período específico de tiempo en el futuro. (UNISDR)
Riesgo del negocio	Exposición a factores tanto internos como externos que pueden afectar la capacidad de la organización para proporcionar un servicio o producto, o que pueden generar una caída en la demanda de los mismos, situaciones que pueden representar un impacto financiero inesperado. Ejemplo: las tabacaleras tienen como riesgo del negocio el enfrentar demandas de salud, campañas para que la gente deje de fumar, etc.
Riesgo operacional	Riesgo de pérdida resultante de controles y procedimientos inadecuados o fallidos. Incluye la pérdida por eventos relacionados con tecnología e infraestructura, fallas, interrupciones de negocios, problemas relacionados con el personal y eventos externos, tales como los cambios regulatorios. Se basa en el riesgo de la operación, independientemente del riesgo del negocio en particular.
Riesgo residual	Nivel de riesgo remanente después de que se han implementado todas las acciones costo-efectivas para reducir el impacto, la probabilidad y las consecuencias de un riesgo o grupo de riesgos específicos, sujeto al apetito al riesgo de una organización.

S

Salvar/Rescatar	Recuperar efectos personales, documentación, oficinas y equipo de cómputo después de un incidente.
Seguridad	Este término se puede utilizar tanto para la información como para las instalaciones físicas. En información, es la práctica de proteger información ante el uso indebido (acceso no autorizado, divulgación, alteración o destrucción). Con respecto a las instalaciones físicas, es la práctica que resulta del establecimiento y el mantenimiento de medidas de protección de las instalaciones y las personas. Estas medidas pueden incluir una combinación de disuasión, prevención, detección, recuperación y corrección, y debe formar parte del enfoque de gestión de riesgos de la empresa.
Seguro	Contrato para financiar el costo del riesgo. Ante la ocurrencia de un evento denominado riesgo (pérdida), el seguro pagará al asegurado el monto contratado. (BCI). Medio para la cobertura de los riesgos al transferirlos a una aseguradora que se va a encargar de garantizar o indemnizar todo o parte del perjuicio producido por la aparición de determinadas situaciones accidentales.
Seguro de pérdidas consecuenciales (BI por sus siglas en inglés)	Cobertura contratada para casos de interrupción de las operaciones. Es un término usado ampliamente en la industria de los seguros para referirse a un seguro que cubre pérdidas (generalmente se cuantifica en ingresos perdidos) debido a la interrupción temporal de las operaciones. Impacto causado a la organización por causa de diferentes tipos de interrupciones. Normalmente se cuantifica en ingresos perdidos.
Servicios en la nube	Modelo de prestación de servicios de negocio y tecnología que permite al usuario acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma flexible y adaptativa.
Servicios esenciales	Servicios de infraestructura sin los cuales un edificio o área estarían inutilizados e impedidos para proporcionar sus servicios normales de operación; típicamente incluye: servicios (agua, gas, electricidad, telecomunicaciones) y también pueden incluir sistemas de respaldo de electricidad y de control ambiental. (BCI)
Servicios subcontratados o tercerizados	Una perspectiva de servicios, comúnmente usada en TI, que hace hincapié en el hecho de que son gestionados de manera externa.
Simulacro	Ejercicio relacionado normalmente con el plan de respuesta a emergencias y que tiene como objetivo que los participantes pongan en práctica los procedimientos de evacuación, refugio en el lugar u otros procedimientos relacionados con la seguridad de las personas, dirigidos normalmente por los brigadistas.
Sistema de comando de incidentes (ICS por sus siglas en inglés)	Estructura organizacional usada por el sector público en Estados Unidos para manejar información, logística y comunicaciones durante un evento de emergencia o desastre.

Sistema de gestión	Conjunto de elementos interrelacionados o interacción de una organización para establecer políticas y objetivos y los procesos para alcanzar esos objetivos. 1) Un sistema de gestión puede abordar una sola disciplina o varias disciplinas 2) Los elementos del sistema incluyen la estructura de la organización, las funciones y responsabilidades, la planificación, la operación, etc. 3) El alcance de un sistema de gestión puede incluir la totalidad de la organización o una o varias funciones o secciones específicas dentro de un grupo de organizaciones.
Sistema de gestión de continuidad del negocio (BCMS por sus siglas en inglés)	Ver "Programa de gestión de continuidad del negocio".
Sitio alterno	Ubicación alterna usada por el negocio cuando la principal no está disponible. Se recomienda que esté a una distancia considerable de las instalaciones primarias. a.- Localidad física donde puede ubicarse un centro de cómputo alterno designado para la recuperación b.- Localidad física preparada para la recuperación de las unidades de negocio con los elementos críticos requeridos, por ejemplo, escritorios, teléfonos, hardware, software, comunicaciones, entre otros.
Sitio secundario	Ver sitio alterno
Subcontratación	Transferencia de las funciones del negocio a un proveedor externo independiente. También denominado Servicios tercerizados.
Suplidor/Proveedor	Tercera parte responsable del suministro de bienes o servicios. (ITIL)
Suplidor/Proveedor de servicios	Organización externa o área interna de la propia organización que proporciona productos o servicios.
Suspensión temporal	Período de tiempo después de una interrupción en el que se espera que un servicio, sistema, proceso o función de negocio esté inutilizable o inaccesible.

T

Táctico	Segundo nivel de los tres niveles de planificación y entrega (estratégico, táctico, operativo). Las actividades tácticas incluyen los planes a medio plazo necesarios para alcanzar objetivos específicos, por lo general en un periodo de semanas a meses.
Tarjeta de bolsillo	Información de contacto de emergencia en formato portátil reducido.
Tecnologías de información - TI (IT por sus siglas en inglés)	Utilización de la tecnología para almacenar, comunicar o procesar información. La tecnología generalmente incluye computadoras, telecomunicaciones, aplicaciones, servidores, bases de datos y cualquier otro programa o sistema. La información puede incluir datos del negocio, imágenes, video, voz, etc. Las tecnologías de información se utilizan con frecuencia para apoyar los procesos del negocio a través de los servicios de TI.
Tiempo de respuesta	Una medida del tiempo entre la solicitud del servicio y su obtención. El término aplica en tecnología, respuesta a emergencias, etc.
Tiempo máximo tolerable de inactividad (MTD por sus siglas en inglés)	Tiempo máximo que un proceso puede ser interrumpido sin causar un daño significativo a la misión de la organización.
Todos los peligros	Plan o enfoque de continuidad o emergencias que cubre o es aplicable a todos los riesgos posibles. FEMA Ver Póliza todo riesgo
Tolerancia al riesgo	Estado de preparación de una organización para soportar el riesgo después de los tratamientos de riesgo, con el fin de lograr sus objetivos. La tolerancia al riesgo puede estar limitada por requisitos legales o regulatorios.
Transferencia del riesgo	Técnica común utilizada por los gerentes de riesgos para hacer frente o mitigar los posibles riesgos de la organización. Una serie de técnicas que describen los distintos medios para hacer frente a los riesgos a través de seguros y productos similares. (DRJ)
Tratamiento del riesgo	Proceso de modificación de los riesgos que consiste en la selección e implementación de una o más opciones, como por ejemplo: eliminar el riesgo (hacer que el origen del riesgo desaparezca), mitigar el riesgo, modificar la probabilidad, compartir el riesgo, retener el riesgo o incluso incrementarlo buscando una oportunidad o beneficio. Una vez implementado el tratamiento, éste se convierte en un control (o también puede llegar a modificar controles existentes).

U

Unidad de negocio/ Departamento/Área	Cada una de las divisiones de una organización que realiza una serie de funciones específicas. Ejemplos de unidades de negocio incluyen los puntos de venta y el departamento de Recursos Humanos.

V

Vulnerabilidad	Grado de exposición de una persona, activo, proceso, información, infraestructura y otros recursos a las acciones o efectos de un riesgo, suceso u otro acontecimiento.

W

Warm site	Ubicación alterna de procesamiento que está equipada con algún hardware e interfases de comunicaciones, acondicionamiento eléctrico y ambiental, que sólo estará en capacidad operacional una vez que sean suministrados los componentes faltantes y se desarrolle una labor de configuración.

Fuentes

ASIS	ASIS Internacional es una comunidad global con más de 38,000 profesionales de la seguridad que desarrollan funciones relacionadas con la protección de los activos (personas, propiedad e información).
AS/NZ 5050	AS/NZS 5050 explica cómo aplicar AS/NZS ISO 31000 a riesgos relacionados con alguna interrupción e incluye una guía detallada de las características de estos riesgos y el marco de gestión de riesgos a través del cual se administran.
ASIS/BSI BCM.01-2010	Este estándar, que reunió a expertos mundiales en gestión de la continuidad y planificación para contingencias, representa un consenso de las mejores prácticas en la gestión de la continuidad del negocio. Es una herramienta útil para cualquier tamaño o tipo de organización que desee mejorar su preparación, desempeño y resultados. Especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, probar, actualizar y mejorar un sistema de gestión de continuidad del negocio.
Business Continuity Institute (BCI)	El BCI se ha establecido como una organización líder de afiliación y certificación de los profesionales de la continuidad de todo el mundo y ofrece una amplia gama de recursos para los profesionales que quieren elevar los niveles de resiliencia dentro de su organización o que quieren dedicarse a la continuidad del negocio.
British Standards Institute (BSI)	El British Standards Institute ayuda a las organizaciones de todo el mundo a hacer de la excelencia un hábito. Durante más de un siglo han estado desafiando la mediocridad y la complacencia para ayudar a desarrollar la excelencia en la gente y los productos y servicios. Esto significa que enseña a las empresas a mejorar su desempeño, a reducir los riesgos y a lograr un crecimiento sustentable. Es el organismo nacional de estándares del Reino Unido y el primer organismo nacional de normalización.
Norma Británica BS 25999	Fue la primera norma dedicada a la gestión de la continuidad del negocio a nivel mundial, y fue desarrollada por un grupo de expertos de clase mundial que representan una sección transversal de los sectores de la industria y el gobierno para establecer el proceso, los principios y la terminología de la gestión de la continuidad del negocio, para minimizar el impacto de cualquier interrupción de las operaciones que pudiera afectar a una organización.
Committee on National Security Systems (CNSS)	El CNSS proporciona un foro para la discusión de asuntos políticos y es responsable de establecer las políticas, lineamientos, instrucciones, procedimientos operativos, orientación y asesorías de seguridad de la información a nivel nacional para los departamentos del gobierno de los EE.UU. y los organismos del Sistema Nacional de Seguridad (NSS por sus siglas en inglés) a través de su sistema de emisión.
DRI Internacional (DRII)	El DRI Internacional, originalmente Disaster Recovery Institute, fundado en 1988, es una organización sin fines de lucro con la misión de hacer que el mundo esté preparado. Como organismo global de educación y certificación en continuidad del negocio y planificación de recuperación ante desastres, establece el estándar de profesionalismo. Después de más de 25 años de servicio, sigue siendo la organización más antigua, más grande y la más extendida de su tipo.

Disaster Recovery Journal (DRJ)	Proporciona conocimiento profundo por parte de expertos en la planificación de continuidad del negocio. Es una publicación ampliamente leída en el sector y ofrece conferencias que tienden a ser los eventos con mayor asistencia en la industria de la continuidad. Tiene abundancia de recursos y materiales disponibles para su uso y consulta.
European Central Bank (ECB)	El ECB y los bancos centrales nacionales constituyen el eurosistema, es decir, el sistema central bancario del área europea. Su objetivo principal es mantener la estabilidad de precios, salvaguardando el valor del euro.
FCD 1 Federal Continuity Directive	Es un documento desarrollado y promulgado por el Department of Homeland Security (DHS) de EE.UU., en coordinación con el CAG y en consulta con el CPCC, que dirige los departamentos ejecutivos y las agencias para la elaboración de los requisitos de planificación de continuidad identificados y los criterios de evaluación. Las directrices federales de continuidad proveen dirección al poder ejecutivo federal para el desarrollo de planes y programas de continuidad.
Federal Final Institutions Examination Council (FFIEC)	Responsable de desarrollar sistemas de notificación uniformes para las instituciones financieras supervisadas por el gobierno federal y sus sociedades, así como para las filiales de ambas. Dirige a las escuelas para los examinadores empleados por las cinco agencias federales miembros representadas en el Consejo y pone a disposición aquellas escuelas de empleados de agencias estatales que supervisan instituciones financieras.
Health Insurance Portability and Accountability Act of 1996 (HIPPA)	Acrónimo de Health Insurance Portability and Accountability Act. El objetivo principal de este estatuto federal de los EE.UU. es ayudar a los asegurados a mantener su cobertura de seguro. Las regulaciones de HIPAA se aplican a los planes de salud, centros de atención de salud (entidades que facilitan las transacciones electrónicas de datos a través de la "traducción" de los mismos entre los planes de salud y proveedores cuando se utilizan sistemas de información no compatibles).
Health Information Technology for Economic and Clinical Health Act (HITECH)	HITECH fue promulgada como parte de la ley estadounidense de Recuperación y Reinversión de 2009; se convirtió en ley el 17 de febrero de 2009 y promueve la adopción y uso significativo de la tecnología de la información. La sección D de esta ley aborda los problemas de privacidad y seguridad asociados con la transmisión electrónica de información sobre la salud, en parte, a través de varias disposiciones que refuerzan la imposición civil y criminal de las reglas de HIPAA.
International Organization for Standardization (ISO)	ISO es el desarrollador más grande del mundo de normas internacionales voluntarias. Las normas internacionales dan especificaciones de vanguardia para productos, servicios y buenas prácticas, ayudando a que la industria sea más eficiente y eficaz. Desarrolladas a través de un consenso global, ayudan a romper las barreras del comercio internacional. ISO es una red de organismos nacionales de estandarización.
Norma ISO 31000	Esta norma, llamada "Gestión de riesgos, principios y directrices", proporciona los principios, el marco de referencia y el proceso de gestión de riesgos. Puede ser utilizada por cualquier organización sin importar su tamaño, actividad o sector. Implementar ISO 31000 aumenta la probabilidad de las organizaciones para lograr sus objetivos, mejorar el proceso de identificación de oportunidades y amenazas y asignar y utilizar de manera efectiva los recursos para el tratamiento de riesgos.

Information Technology Infrastructure Library (ITIL)	ITIL es un marco ampliamente adoptado para la gestión de servicios de TI. Proporciona un enfoque práctico, sin complicaciones, para la identificación, planificación, entrega y soporte de servicios de TI a las organizaciones.
Monetary Authority of Singapore (MAS)	Banco central de Singapur que promueve el crecimiento económico sostenido y no inflacionista a través de la formulación de una política monetaria adecuada y la vigilancia de las tendencias emergentes y las potenciales vulnerabilidades macroeconómicas. Gestiona el tipo de cambio de Singapur, así como las reservas de divisas y liquidez en el sector bancario. MAS también es una superintendencia integrada que supervisa todas las instituciones financieras de Singapur: bancos, aseguradoras, intermediarios del mercado de capitales, asesores financieros y la bolsa de valores.
National Fire Protection Association (NFPA)	Organización internacional sin fines de lucro con la misión de reducir la carga mundial de incendios y otros peligros sobre la calidad de vida proveyendo y abogando por códigos y normativas consensuadas, así como por la investigación, la formación y la educación. Es el recurso principal para el estudio, la investigación y el análisis de datos sobre incendios.
Norma NFPA 1600	La Norma NFPA de Preparación Nacional está siendo ampliamente utilizada tanto por entidades públicas y privadas, como por instituciones sin fines de lucro y no gubernamentales en el ámbito local, regional, nacional e internacional. Ha sido adoptada por el Departamento de Seguridad Nacional de Estados Unidos bajo consenso voluntario como estándar para la preparación en casos de emergencia.
National Institute of Standards and Technology (NIST)	El NIST es responsable de desarrollar estándares y directrices, incluyendo los requisitos mínimos, para proporcionar la seguridad de la información adecuada para todas las operaciones de una organización y sus activos, pero tales normas y directrices no se aplican a los sistemas de seguridad nacional. Es uno de los laboratorios de física más antiguos de la nación. Es una agencia federal no regulatoria dentro del Departamento de Comercio de Estados Unidos.
NIST SP 800-34	Guía de planificación de contingencia para los sistemas de información federal. Proporciona instrucciones, recomendaciones y consideraciones para la planificación ante contingencias que afecten al sistema de información federal. Esta publicación ayuda a las organizaciones a comprender el objetivo, el proceso y el formato de desarrollo de la planificación de contingencias relacionadas con los sistemas de información mediante directrices prácticas basadas en sucesos reales.
National Emergency Crisis and Disaster Management Authority (NCEMA)	La NCEMA trabaja bajo la supervisión del Consejo Nacional Superior de Seguridad. Es el cuerpo nacional principal que establece el estándar de los Emiratos Árabes Unidos responsable de regular y coordinar todos los esfuerzos de emergencia y manejo de crisis así como el desarrollo de un plan nacional para responder a emergencias. La misión del NCEMA es coordinar todos los esfuerzos nacionales para salvar vidas, conservar propiedades y activos nacionales dificultando el efecto de emergencias y crisis.

Singapore SS-540	Estándar que establece el marco para el análisis y la implementación de estrategias, procesos y procedimientos. La norma se centra en la resiliencia y la protección de los activos críticos (humanos, del medio ambiente, intangibles y físicos) y en la gestión de la continuidad y la recuperación de las funciones críticas de una organización de cualquier tamaño.
United Nations International Strategy for Disaster Reduction (UNISDR)	La UNISDR se creó como un departamento de la Secretaría de las Naciones Unidas con el objetivo de asegurar la ejecución de la estrategia internacional para la reducción de desastres. El objetivo de UNISDR es servir como punto focal en el sistema de las Naciones Unidas en los esfuerzos de coordinación de la reducción del desastre y asegurar sinergias entre actividades de reducción del desastre. La reducción del riesgo de desastres (DRR por sus siglas en inglés) pretende reducir el daño causado por riesgos naturales como terremotos, inundaciones, sequías y ciclones, a través de una ética de la prevención. La estrategia internacional para la reducción de desastres refleja un cambio del enfoque tradicional en la atención de desastres a la reducción de desastres, y en efecto procura promover una "cultura de la prevención".