

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



UCI

Universidad para la
Cooperación Internacional

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

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

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

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

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

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

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

Las Prácticas Profesionales para la Gestión de Continuidad de Negocios



Acerca de las Prácticas Profesionales

Abril 2017

Mantenido por DRI Internacional

Para preguntas sobre
este documento
contacte a
driinfo@drii.org.
Para más información,
visite www.drii.org.

Acerca de las Prácticas Profesionales

Creadas y mantenidas por el Instituto de Recuperación Ante Desastres Internacional (Disaster Recovery Institute International), *Las Prácticas Profesionales para la Gestión de Continuidad de Negocios* se trata de un cuerpo de conocimiento diseñado para ayudar en el desarrollo, implementación y mantenimiento de programas de Continuidad de Negocio. También está designado a servir como una herramienta para realizar evaluaciones a programas BCM ya existentes.

El uso del marco de trabajo de las Prácticas Profesionales para desarrollar, implementar y mantener un programa de continuidad de negocio puede reducir la probabilidad de brechas significativas en el programa e incrementar la cohesión. El uso de las Prácticas Profesionales para evaluar un programa puede identificar brechas o deficiencias para que puedan ser corregidas.

Gestión de continuidad de negocio (Business continuity management – BCM por sus siglas en inglés), tal como está definido en este documento, es un proceso de gestión que identifica riesgos, amenazas y vulnerabilidades que pueden impactar a operaciones continuas. La Continuidad de Negocio provee un marco de trabajo para construir resiliencia organizacional y la capacidad para una respuesta eficaz

Todos los otros términos están definidos en *El Glosario Internacional de Resiliencia* publicado y mantenido por el DRI Internacional.

El DRI crea ambos *Las Prácticas Profesionales para la Gestión de Continuidad de Negocios* y *El Glosario Internacional para Resiliencia*, y están disponibles para su descarga gratuita en drii.org. *Las Prácticas Profesionales para la Gestión de Continuidad de Negocios* están disponibles en múltiples idiomas.



Acerca de las Prácticas Profesionales

Prácticas Profesionales 2017

Como parte de los esfuerzos continuos del DRI Internacional por mantener la relevancia y la utilidad de las Prácticas Profesionales, una revisión extensiva de la sustancia, forma y función de las mismas fue llevada a cabo desde la mitad del 2015 y finalizó a inicios del 2017. La meta fue proporcionar información que incluiría:

- Avances en tecnología
- Consideraciones de amenazas cibernéticas
- Utilización de seguros como herramienta de transferencia de riesgos
- Estrategias para manufactura
- Procesamiento de la cadena de suministro
- Conceptos de gestión de riesgos
- Preocupaciones legales y regulatorias

Además, los títulos de dos de las Prácticas Profesionales fueron modificados para que sean consistentes con los estándares de la industria y de la profesión, específicamente:

- La Práctica Profesional 2 fue cambiada de “Evaluación y Control de Riesgos” a “Evaluación de Riesgos”
- La Práctica Profesional 5 fue cambiada de “Preparación y Respuesta de Emergencia” a “Respuesta a Incidentes”

Estos nuevos títulos colocan a las Prácticas Profesionales en línea con la terminología generalmente usada por la mayoría de los profesionales y los organismos reguladores.

Como un complemento a la creación de una terminología más generalmente aceptada, se hicieron revisiones en los resúmenes y detalles de las Prácticas Profesionales para alinearlos con el *Glosario Internacional para la Resiliencia* publicado y mantenido por el DRI Internacional. Se utilizó el análisis lingüístico para reducir el número de expresiones coloquiales en su versión en inglés y lenguaje idiosincrásico. Esto ha facilitado la traducción de las Prácticas Profesionales a los numerosos idiomas a los que han sido traducidas.

Por último, la numeración y la paginación se han modificado para permitir una referenciación más simple y la facilidad de uso.

Resumen Ejecutivo

Los Objetivos de las Prácticas Profesionales para la Gestión de Continuidad de Negocios

1. Inicio y Administración del Programa

- Establecer la necesidad de un programa de continuidad de negocio.
- Obtener el apoyo y el financiamiento para el programa de continuidad de negocio.
- Construir el marco de trabajo organizacional que apoye el programa de continuidad de negocio.
- Introducir conceptos claves, tales como gestión del programa, conciencia del riesgo, identificación de funciones / procesos críticos, estrategias de recuperación, concientización y entrenamiento, y ejercicios / pruebas.

2. Evaluación de Riesgos

- Identificar riesgos que puedan afectar de manera adversa los recursos o la imagen de una entidad.
- Evaluar los riesgos para determinar los impactos potenciales a la entidad, permitiendo a la entidad determinar el uso más efectivo de los recursos para reducir esos impactos potenciales.

3. Análisis de Impacto al Negocio

- Identificar y priorizar las funciones y procesos de la entidad con el fin de determinar cuáles van a tener el mayor impacto en caso de que no estén disponibles.
- Evaluar los recursos requeridos para apoyar el proceso de análisis de impacto al negocio.
- Analizar los resultados para determinar las brechas entre los requerimientos de la entidad y su capacidad para ofrecer esos requerimientos.

4. Estrategias de Continuidad de Negocio

- Seleccionar las estrategias costo-efectivas para reducir las deficiencias que se encontraron durante los procesos de evaluación de riesgos y de análisis de impacto al negocio.

5. Respuesta a Incidentes

- Desarrollar y ayudar con la implementación de un sistema de gestión de incidentes que defina los roles organizacionales, las líneas de autoridad y la sucesión de autoridad.
- Definir los requerimientos para desarrollar e implementar el plan de respuesta a incidentes de la entidad.
- Asegurar que la respuesta a incidentes se coordina con las organizaciones externas de manera oportuna y efectiva cuando es apropiado.

6. Desarrollo e Implementación del Plan

- Documentar los planes que serán usados durante un incidente y que permitan a la entidad continuar con su función.

7. Programas de Concientización y Entrenamiento

- Establecer y mantener programas de entrenamiento y concientización que permitan que el personal pueda responder a incidentes de una forma tranquila y eficiente.

8. Ejercicio, Evaluación y Mantenimiento del Plan de Continuidad del Negocio

- Establecer un programa de ejercicio, evaluación y mantenimiento para mantener un estado de preparación.



Resumen Ejecutivo

9. Comunicación de Crisis

- Proveer un marco de trabajo para desarrollar un plan de comunicación de crisis.
- Asegurar que el plan de comunicación de crisis pueda proveer comunicación oportuna y efectiva con las partes, tanto internas como externas.

10. Coordinación con Dependencias Externas

- Establecer políticas y procedimientos para coordinar actividades de respuesta a incidentes con entidades públicas.

Práctica Profesional Uno: Inicio y Administración del Programa

Objetivos

- Establecer la necesidad de un programa de continuidad de negocio.
- Obtener el apoyo y el financiamiento para el programa de continuidad de negocio.
- Construir el marco de trabajo organizacional que apoye el programa de continuidad de negocio.
- Introducir conceptos claves, tales como gestión del programa, conciencia del riesgo, identificación de funciones / procesos críticos, estrategias de recuperación, concientización y entrenamiento, y ejercicios / pruebas.

El Rol del Profesional

1. Establecer la necesidad de un programa de continuidad de negocio.
2. Obtener el apoyo y el financiamiento para el programa de continuidad de negocio.
3. Coordinar y gestionar la implementación del programa de continuidad de negocio a través de la entidad.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Establecer la necesidad de un programa de continuidad de negocio.
 - 1.1. Investigar y hacer referencia a los requerimientos y restricciones relevantes de negocio, comerciales, legales, regulatorios, estatutarios y contractuales, tanto desde una perspectiva interna como externa, proporcionando recomendaciones relativas al cumplimiento y la conformidad de la entidad.
 - 1.2. Hacer referencia a estándares relevantes desarrollados por organismos desarrolladores de normas nacionales o internacionales, o por asociaciones de comercio o de la industria.
 - 1.3. Identificar y resolver cualquier conflicto entre las políticas de la entidad y requerimientos externos relevantes.
 - 1.4. Revisar reportes de auditoría existentes con el fin de asegurar el que programa de continuidad de negocio propuesto aborda adecuadamente las brechas y oportunidades.
 - 1.5. Indicar los beneficios de continuidad de negocio en el contexto de la misión, los objetivos y las operaciones de la entidad.
 - 1.6. Explicar el rol de los líderes, incluyendo la rendición de cuentas y su responsabilidad en relación con continuidad de negocio.
 - 1.7. Desarrollar reportes y presentaciones formales que se enfoquen en incrementar la conciencia acerca del impacto potencial de los riesgos de la entidad.



Práctica Profesional Uno: Inicio y Administración del Programa

2. Obtener el apoyo y el financiamiento para el programa de continuidad de negocio.
 - 2.1. Desarrollar una declaración de misión o una carta de inicio (*charter*) para el programa de continuidad de negocio en el contexto de la misión de la entidad.
 - 2.2. Desarrollar objetivos, supuestos y alcance del programa de continuidad de negocio en el contexto de la misión, los objetivos y las operaciones de la entidad.
 - 2.3. Desarrollar los requerimientos de presupuesto para el programa de continuidad de negocio.
 - 2.4. Definir la estructura del programa de continuidad de negocio. Identificar las necesidades potenciales de política y factores críticos de éxito.
 - 2.5. Presentar la estructura del programa BCM propuesta para obtener el apoyo y la aprobación de los líderes para el programa BCM.
 - 2.6. Identificar los patrocinadores líderes para el desarrollo del programa de continuidad de negocio.
 - 2.7. Obtener la aprobación de los líderes para los requerimientos de presupuesto.
 - 2.8. Establecer un comité u otro órgano de control tal como un Comité de Dirección¹ (*Steering Committee*) para dirigir el programa de continuidad de negocio.
 - 2.9. Definir el alcance, las responsabilidades y la rendición de cuentas global de cada miembro del Comité de Dirección y sus funciones de apoyo.
3. Coordinar y gestionar la implementación del programa de continuidad de negocio a través de la entidad.
 - 3.1. Dirigir al Comité de Dirección para impulsar la implementación de los objetivos, la estructura del programa y los factores críticos de éxito. Dirigir el alineamiento con las políticas organizacionales existentes y mantener los procesos consistentes.
 - 3.2. Desarrollar políticas, estándares y procedimientos para el programa de continuidad de negocio, dentro del contexto de la misión, objetivos y las operaciones de la entidad.
 - 3.3. Definir el propósito y obtener los recursos necesarios para el programa de continuidad de negocio.
 - 3.4. Identificar equipos que apoyen la implementación del programa de continuidad de negocio, incluyendo aquellos equipos que estarán participando en la ejecución de las siguientes actividades²:
 - 3.4.1. evaluación de riesgos y estrategias,
 - 3.4.2. análisis de impacto al negocio,
 - 3.4.3. selección e implementación de la estrategia de recuperación,
 - 3.4.4. gestión global de incidentes,
 - 3.4.5. respuesta y recuperación de incidentes,
 - 3.4.6. gestión y comunicación de crisis,
 - 3.4.7. análisis de brechas posterior al incidente e implementación de las lecciones aprendidas,
 - 3.4.8. documentación del plan de continuidad de negocio,
 - 3.4.9. pruebas, ejercicios y mantenimiento del plan y actividades de auditoría, y
 - 3.4.10. actividades de respuesta, recuperación y restauración durante un evento.
 - 3.5. Supervisar el estado del impacto del presupuesto del programa de continuidad de negocio según se vaya ejecutando, de acuerdo con el proceso de gestión de presupuesto ya existente en la entidad.

¹ Si bien no es de aplicación universal, Comité de Dirección (*Steering Committee*) se utiliza en este documento en lugar del Comité (*Committee*) con el propósito de claridad.

² Estas actividades están definidas y detalladas en las Prácticas Profesionales de la Dos a la Diez.



Práctica Profesional Uno: Inicio y Administración del Programa

- 3.6. Desarrollar planes de proyecto para los componentes principales, tales como los procesos de evaluación de riesgos y análisis de impacto al negocio. Detallar cualquier tarea requerida para apoyar los factores críticos de éxito aprobados, que pueden incluir, pero no están limitadas a:
 - 3.6.1. un cronograma de implementación
 - 3.6.2. estimaciones de tiempo,
 - 3.6.3. hitos del programa, y
 - 3.6.4. requerimientos de personal.
- 3.7. Supervisar la efectividad continua del programa de continuidad de negocio.
 - 3.7.1. Desarrollar, monitorear, rastrear y hacer reportes sobre los continuos requerimientos de documentación y gestión para el programa de continuidad de negocio.
 - 3.7.2. Monitorear, rastrear y hacer reportes sobre el cumplimiento con estándares relevantes de la industria tal como se definió en la Sección 2.1 en este documento.
 - 3.7.3. Desarrollar y ejecutar estrategias de *benchmarking* (evaluaciones comparativas) internas y externas.
- 3.8. Reportar a los líderes el estado del programa de continuidad de negocio de forma regular.
 - 3.8.1. Desarrollar un cronograma para realizar reportes del progreso del programa de continuidad de negocio a los líderes.
 - 3.8.2. Preparar reportes de estado regulares para los líderes que contengan información concisa, pertinente, precisa y oportuna sobre los elementos clave del programa de continuidad de negocio.
 - 3.8.3. Proveer actualizaciones sobre el estado del programa de continuidad de negocio y realizar recomendaciones para mejoras en el programa de forma continua.
 - 3.8.4. Monitorear los estándares relevantes de la industria tal como se definió en la Sección 1.2 de este documento para asegurarse de que el programa de continuidad de negocio está generando valor de forma consistente con las mejores prácticas actuales.

Práctica Profesional Dos: Evaluación de Riesgos

Objetivos

- Identificar riesgos³ que puede afectar de forma adversa los recursos o la imagen de una entidad.
- Evaluar los riesgos para determinar los impactos potenciales a la entidad, lo que permite a la entidad determinar el uso más efectivo de los recursos para reducir estos impactos potenciales.

El Rol del Profesional

1. Trabajar con los líderes y con cualquier grupo interno y/o externo de gestión de riesgos o de gestión de riesgos empresariales para obtener un acuerdo sobre una metodología de evaluación de riesgos estandarizada.
2. Identificar, desarrollar e implementar actividades de recolección de información a través de la entidad para identificar riesgos y amenazas.
3. Determinar la probabilidad y el impacto de los riesgos identificados.
4. Identificar y evaluar la efectividad de los controles y salvaguardas que están actualmente implementados.
5. Identificar estrategias de resiliencia que reduzcan los riesgos de la entidad y/o que puedan controlar o mitigar el impacto potencial del riesgo.
6. Documentar y presentar la evaluación de riesgos y vulnerabilidades y las recomendaciones a los líderes para su aprobación.
7. Al recibir la aprobación de los líderes, desarrollar el apetito al riesgo de la entidad y el umbral para utilizar como base para la gestión continua de un proceso de evaluación de riesgos sostenible.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Trabajar con los líderes y con cualquier grupo interno y/o externo de gestión de riesgos o de gestión de riesgos empresarial (en adelante, los grupos de gestión de riesgos) dentro de la entidad para obtener un acuerdo sobre una metodología de evaluación de riesgos clara y estandarizada, y para ganar la comprensión de la tolerancia al riesgo y el umbral de riesgo de la entidad.
 - 1.1. Identificar metodologías y herramientas de análisis de riesgo, que pueden incluir, pero no se limitan a, las metodologías cuantitativas (tales como el uso de fórmulas matemáticas) y las metodologías cualitativas (como la evaluación de las ventajas y desventajas). Revisar e incorporar los factores de fiabilidad y confianza de los datos y el contenido que se está utilizando.
 - 1.2. Seleccionar la metodología y herramientas para la implementación en toda la entidad, que sean apropiadas para el apetito de riesgo y el umbral de la entidad.

³ 'Riesgo' se utiliza a menudo como sinónimo de 'amenaza'. El DRI ha elegido usar 'riesgo' para los propósitos de este documento.



Práctica Profesional Dos: Evaluación de Riesgos

- 1.3. Establecer criterios de medición necesarios para cuantificar la probabilidad y el impacto de los riesgos identificados y la efectividad de los controles existentes.
2. Identificar, desarrollar e implementar actividades de recopilación de información a través de la entidad para identificar riesgos.
 - 2.1. Identificar la metodología que se utilizará en el proceso de recopilación de información.
 - 2.2. Colaborar con los grupos relevantes de la entidad, incluyendo, pero no limitado a, los grupos de gestión de riesgos, asesoría legal, seguridad física y seguridad de la información, para identificar los riesgos conocidos.
 - 2.3. Determinar y evaluar la credibilidad de todas las fuentes de información que estarán siendo usadas para recopilar datos sobre los riesgos.
 - 2.4. Desarrollar una estrategia para reunir información que sea consistente con las políticas de la entidad.
 - 2.5. Crear métodos de recopilación y distribución de información que apliquen a toda la entidad, incluyendo, pero no limitado a, formularios, cuestionarios, entrevistas, reuniones y / o combinaciones de estos procesos.
 - 2.6. Identificar los riesgos de la entidad.
 - 2.6.1. Lograr una visión holística del riesgo en toda la entidad mediante la identificación de riesgos, tomando en cuenta la frecuencia, la probabilidad, la velocidad de desarrollo, la gravedad e impacto en la reputación de la entidad.
 - 2.6.2. Identificar las exposiciones de riesgo tanto de fuentes internas como externas, que pueden incluir, pero no se limitan a, los fenómenos naturales, exposiciones tecnológicas, y los actos realizados por el ser humano; exposiciones de la industria o del modelo de negocio; actos accidentales e intencionales; exposiciones o riesgos controlables, así como aquellos que están fuera del control de la entidad; y los eventos con y sin advertencia previa.
3. Determinar la probabilidad y el impacto de los riesgos identificados.
 - 3.1. Desarrollar un método para evaluar cualquier exposición y los riesgos en términos de la frecuencia del riesgo, la probabilidad, la velocidad de desarrollo, la gravedad, el impacto, y si hay advertencias anteriores a los incidentes como en el caso de los huracanes.
 - 3.2. Identificar los impactos de los riesgos identificados por categoría, que pueden incluir, pero no se limitan a, la cadena de suministro, la seguridad cibernética, tecnologías de información incluyendo la infraestructura operativa, seguros, fabricación, instalación, seguridad física, la reputación, temas legales, los clientes y los procedimientos.
 - 3.3. Evaluar los riesgos identificados y clasificarlos de acuerdo con los criterios relevantes, incluyendo, pero no limitado a, aquellos riesgos que se encuentran bajo el control de la entidad y aquellos riesgos que están fuera del control de la entidad.
 - 3.4. Evaluar el impacto de los riesgos en aquellos factores que son esenciales para llevar a cabo operaciones de la entidad, incluyendo, pero no limitado a, la disponibilidad de personal, tecnología de la información y tecnología de las comunicaciones, así como el estado de la infraestructura, tal como el transporte.
4. Identificar y evaluar la efectividad de los controles y salvaguardas que se encuentren actualmente implementados.
 - 4.1. Identificar y evaluar la efectividad de los medios de protección que ofrecen.
 - 4.2. Identificar y evaluar la efectividad de cualquier control y salvaguarda que se encuentren instalados para los grupos internos y externos sobre los que la entidad es dependiente con el fin de realizar sus operaciones.

- 4.3. Identificar y evaluar la efectividad de las acciones tomadas para reducir la probabilidad de la ocurrencia de incidentes que puedan poner en peligro la capacidad de hacer negocios, que pueden incluir, pero no se limitan a, la ubicación de instalaciones, las políticas y procedimientos de seguridad de las personas (*safety*), entrenamiento sobre el uso adecuado de equipos y herramientas, y el mantenimiento preventivo.
- 4.4. Identificar y evaluar la efectividad de los controles existente para mitigar los impactos a que se está expuesto, tales como los controles preventivos⁴, que pueden incluir, pero no se limitan a, las prácticas de seguridad física (por ejemplo, control de acceso, cámaras y personal de seguridad); prácticas de seguridad de la información (por ejemplo, firewalls, detección de intrusos y contraseñas); prácticas de empleo (por ejemplo, las investigaciones de antecedentes y prácticas de contratación); y prácticas de privacidad (por ejemplo, una política de escritorio limpio y eliminación de residuos adecuado).
- 4.5. Identificar y evaluar la efectividad de los controles empleados para reducir el impacto de la exposición, que pueden incluir, pero no se limitan a, sistemas de riego, cuerpos de bomberos, generadores y sistemas de alimentación eléctrica ininterrumpida (*uninterruptible power supply*, UPS).
- 4.6. Evaluar la distribución de las comunicaciones relacionadas con la seguridad con las áreas internas de la entidad, así como con proveedores de servicios externos.
5. Identificar estrategias de resistencia para controlar o mitigar el impacto potencial del riesgo y/o reducir las vulnerabilidades.
 - 5.1. Identificar los puntos de activación (*trigger points*) de las áreas de servicio y soporte para identificar, escalar y ejecutar las estrategias seleccionadas al tratar riesgos.
 - 5.2. Recomendar cualquier cambio necesario para reducir el impacto de los riesgos identificados, que pueden incluir, pero no están limitados a:
 - 5.2.1. Cambios en la protección física:
 - 5.2.1.1. Identificar los requisitos necesarios para restringir el acceso a todos los niveles pertinentes, incluyendo, pero no limitado a, el edificio o cualquier salón o habitación específica.
 - 5.2.1.2. Investigar la necesidad de tener barreras y estructuras reforzadas para determinar la entrada deliberada, accidental, y / o no autorizada.
 - 5.2.1.3. Solucionar vulnerabilidades del lugar / ubicación que puedan resultar de la construcción física, ubicación geográfica, los vecinos corporativos, instalaciones de infraestructura y la infraestructura de la comunidad.
 - 5.2.1.4. Identificar la necesidad de la utilización de personal especializado para llevar a cabo puntos de revisión en la entrada.
 - 5.2.1.5. Evaluar la necesidad de equipos de vigilancia en los puntos de control de acceso.
 - 5.2.1.6. Cambios en los controles de acceso y seguridad, seguros de inquilino y los acuerdos de arrendamiento.
 - 5.2.2. Identificar los cambios en la tecnología de la información y de la seguridad cibernética:
 - 5.2.2.1. Evaluar la necesidad de protección proporcionada por un sistema para proteger datos que se almacenan, en proceso, o en transferencia, así como copia de seguridad (respaldos) de la información y su protección.
 - 5.2.2.2. Evaluar la seguridad de la información incluyendo el hardware, el software, los datos y el monitoreo de redes así como los procesos de detección y notificación.

⁴ Los controles preventivos se definen como controles proactivos que ayudan a prevenir una pérdida.



Práctica Profesional Dos: Evaluación de Riesgos

- 5.2.2.3. Evaluar la ubicación física de los activos de seguridad cibernética y tecnología de la información.
- 5.2.3. Cambios en los procedimientos del personal.
- 5.2.4. Los cambios que incluyen la duplicación y redundancias incorporadas a los servicios públicos.
- 5.3. Interfaz con recursos externos, que pueden incluir, pero no están limitados a, vendedores, proveedores y subcontratistas.
- 6. Documentar y presentar la evaluación del riesgo y vulnerabilidades, así como las recomendaciones a los líderes para su aprobación.
 - 6.1. Preparar un informe de evaluación de riesgos para estandarizar el análisis a través de la entidad.
 - 6.2. Presentar los resultados de la evaluación de riesgos, que puede incluir, pero no se limita a, los siguientes componentes:
 - 6.2.1. La información sobre los riesgos y las exposiciones basadas en el análisis de riesgos y la vulnerabilidad.
 - 6.2.2. Una evaluación de los controles existentes y/o estrategias para gestionar los riesgos conocidos. La evaluación debe incluir una valoración para el control y/o la efectividad como puede ser estrategia plenamente eficaz, parcialmente eficaz o ineficaz.
 - 6.2.3. Recomendaciones para que nuevos controles sean implementados incluyendo un análisis de costo / beneficio.
 - 6.2.4. Priorizar las recomendaciones para la implementación de los nuevos controles.
 - 6.2.5. Recomendaciones para la mejora de los controles incluyendo un análisis de costo / beneficio.
 - 6.2.6. Recomendaciones para las áreas apropiadas para transferir el riesgo.
- 7. Al recibir la aprobación de los líderes, desarrollar la tolerancia al riesgo y el umbral de la entidad para utilizarlos como base para la gestión continua de un proceso de evaluación de riesgos sostenible.

Práctica Profesional Tres: Análisis de Impacto al Negocio

Objetivos

- Identificar y priorizar las funciones y procesos de la entidad con el fin de determinar cuáles tendrían el mayor impacto en caso de que no estén disponibles.
- Evaluar los requerimientos necesarios para apoyar el proceso de análisis de impacto al negocio.
- Analizar los resultados para determinar las brechas entre las necesidades de la entidad y su capacidad para ofrecer esos requerimientos.

El Rol del Profesional⁵

1. Identificar el criterio cualitativo y cuantitativo que se usará para evaluar el impacto a la entidad como resultado de un evento.
2. Obtener el acuerdo de los líderes sobre la metodología para el análisis de impacto al negocio y para el criterio que se usará para establecer el proceso y la metodología del análisis de impacto al negocio.
3. Planear y coordinar la recolección y el análisis de datos.
4. Establecer el criterio y la metodología que se usarán para conducir el proceso del BIA.
5. Analizar los datos recopilados contra el criterio aprobado para establecer un objetivo de tiempo de recuperación (*recovery time objective*, RTO) y un objetivo de punto de recuperación (*recovery point objective*, RPO) para cada área operacional y la tecnología que da soporte a esas áreas.
6. Preparar y presentar los resultados del análisis de impacto al negocio a los líderes. Obtener la aceptación de los objetivos de tiempo de recuperación y los objetivos de punto de recuperación como se detallan en el análisis de impacto al negocio.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Identificar el criterio cualitativo y cuantitativo que se usará para evaluar el impacto a la entidad como resultado de un evento.
 - 1.1. Definir y obtener la aprobación del criterio que se usará para evaluar el impacto en las operaciones de la entidad, que puede incluir, pero no está limitado a, las siguientes actividades:
 - Evaluar el impacto en los clientes, incluyendo, pero no limitado a, qué tan rápido los clientes sabrán que existe un problema, la posibilidad de que van a ir a otro negocio; qué tan preocupados estarán con base en los acuerdos y los impactos en los niveles de servicio a los que la entidad está comprometida; el impacto en la cadena de suministro del cliente; y si hay lesiones o muertes como resultado del evento.
 - Evaluar los impactos financieros, incluyendo, pero no limitado a, la pérdida de ingresos, pérdida de ganancias, el impacto de flujo de caja, el impacto de la cuota de mercado,

⁵ Nota: Aunque al profesional en continuidad de negocio se le puede haber asignado la responsabilidad de gestionar un análisis de impacto al negocio, la propiedad de dicho análisis de impacto al negocio reside en la entidad y en sus líderes o los propietarios del proceso o procesos bajo consideración.

- impacto en el precio de la acción, si aplica; multas contractuales o sanciones, pérdidas resultantes de los pagos requeridos para los costos fijos, y el aumento de los costos de las horas extraordinarias.
- Evaluar el impacto regulatorio, incluyendo, pero no limitado a, multas, sanciones y los requisitos para retirar los productos, y la revocación de cualquier licencia o permiso.
 - Evaluar el impacto operativo, incluyendo, pero no limitado a, los niveles de servicio reducidos o discontinuados, interrupciones del flujo de trabajo y las interrupciones en la cadena de suministro.
 - Evaluar el impacto en la reputación, incluyendo, pero no limitado a, atención negativa por parte de los medios de comunicación, comentarios negativos en las redes sociales, la percepción negativa de la comunidad y el impacto en la confianza de los accionistas.
 - Evaluar el impacto humano, incluyendo, pero no limitado a, la pérdida de vidas, lesiones, impacto en la comunidad, así como impacto emocional tanto a corto como a largo plazo.
2. Obtener el acuerdo de los líderes sobre la metodología para el análisis de impacto al negocio y para el criterio que se usará para establecer el proceso y la metodología del análisis de impacto al negocio.
 - 2.1. Identificar y obtener el apoyo de los líderes y/o identificar la parte responsable para la actividad del análisis de impacto al negocio.
 - 2.2. Definir los objetivos y el alcance del proceso del análisis de impacto al negocio.
 - 2.3. Elegir una metodología o herramienta de planeación apropiada para el análisis de impacto al negocio.
 - 2.4. Elegir una metodología de recopilación de datos apropiada para el análisis de impacto al negocio.
 - 2.4.1. Los datos que se recogen deberían incluir los procesos operativos y las necesidades de recursos incrementales basadas en la duración de recuperación.
 - 2.4.2. Los datos que se recogen deberían incluir el impacto de la pérdida de cualquier tecnología necesaria para ejecutar los procesos.
 - 2.4.3. Los datos que se recogen debe incluir las dependencias internas y externas.
 - 2.4.4. Identificar los requerimientos adicionales que son específicos para las necesidades de la entidad.
 3. Planear y coordinar la recolección y el análisis de datos.⁶
 - 3.1. La recopilación de datos puede realizarse usando cuestionarios.
 - 3.1.1. Desarrollar cuestionarios con instrucciones según se requiera.
 - 3.1.2. Gestionar las reuniones de inicio del proyecto (reuniones de kick-off) para distribuir y explicar los cuestionarios.
 - 3.1.3. Dar apoyo a los encuestados a medida que completan los cuestionarios.
 - 3.1.4. Realizar entrevistas de seguimiento cuando se requieran aclaraciones y/o datos adicionales.
 - 3.2. La recopilación de datos puede realizarse usando entrevistas.
 - 3.2.1. Mantener la coherencia y consistencia mediante el uso de una estructura predefinida para cada entrevista, siguiendo un formato común y usando las mismas preguntas.
 - 3.2.2. Coordinar entrevistas de seguimiento cuando se requiera si el análisis inicial indica la necesidad de aclaraciones o de añadir información a los datos recopilados.
 - 3.3. La recopilación de datos puede realizarse usando talleres de trabajo.
 - 3.3.1. Definir una agenda clara y establecer objetivos.

⁶ Los métodos de recolección se enumeran en la Sección Tres desde la 3.1 a la 3.4 y se enumeran en ningún orden en particular. Las necesidades de las entidades específicas pueden variar.



Práctica Profesional Tres: Análisis de Impacto al Negocio

- 3.3.2. Identificar el nivel apropiado de los participantes en los talleres de trabajo y obtener el acuerdo de los líderes y/o identificar las partes interesadas.
 - 3.3.3. Elegir el lugar adecuado evaluando la ubicación, instalaciones y la disponibilidad de los participantes.
 - 3.3.4. Facilitar y liderar los talleres de trabajo o identificar un recurso apropiado para hacerlo.
 - 3.3.5. Asegurar que los objetivos del taller de trabajo sean alcanzados.
 - 3.3.6. Asegurar que cualquier aspecto pendiente sea identificado al final del taller de trabajo y que se realice un adecuado seguimiento.
 - 3.4. Identificar las principales áreas de la entidad, incluidos los posibles proveedores de servicios tercerizados, con el apoyo de la parte responsable del análisis de impacto al negocio.
 - 3.4.1. Recopilar y revisar los organigramas organizacionales existentes.
 - 3.4.2. Identificar individuos específicos para representar cada área de la entidad.
 - 3.4.3. Identificar a representantes de proveedores de terceros para participar en el proceso de recopilación de datos.
 - 3.4.4. Informar a los individuos seleccionados sobre el proceso del análisis de impacto al negocio y su propósito.
 - 3.4.5. Identificar los requerimientos de entrenamiento y establecer un calendario de entrenamientos.
 - 3.4.6. Ejecutar los entrenamientos para los representantes de las gerencias funcionales identificadas y para los representantes de proveedores de terceros apropiados.
 - 3.5. Usando la metodología seleccionada, llevar a cabo la recopilación de datos necesarios para dar apoyo al proceso del análisis de impacto al negocio.
4. Establecer el criterio y la metodología que se usarán para conducir el proceso del análisis de impacto al negocio.
 - 4.1. Identificar y obtener un acuerdo sobre los métodos de evaluación cuantitativa de los posibles impactos financieros y no financieros en cada área de impacto.
 - 4.2. Identificar y obtener un acuerdo sobre los requisitos para los métodos de evaluación cualitativa en cada área de impacto.
 - 4.3. Crear un calendario para el proceso del análisis de impacto al negocio.
5. Analizar los datos recopilados contra el criterio aprobado para establecer un objetivo de tiempo de recuperación (*recovery time objective*, RTO) y un objetivo de punto de recuperación (*recovery point objective*, RPO) para cada área operacional y la tecnología que da soporte a esas áreas.
 - 5.1. Analizar los datos recopilados para determinar la priorización de los procesos y servicios.
 - 5.2. Documentar todas las interdependencias que existen entre cada proceso de negocio y la infraestructura de apoyo, incluyendo, pero no limitado a, los sistemas de datos y la tecnología relacionada, gestión de la cadena de suministro, terceros proveedores y otros recursos. Estas interdependencias pueden ser intra-departamentales, inter-departamentales, o involucra relaciones externas.
 - 5.3. Determinar el orden de recuperación para las funciones de negocio y de la tecnología usando los datos recopilados.
6. Preparar y presentar los resultados del análisis de impacto al negocio a los líderes. Obtener la aceptación de los objetivos de tiempo de recuperación y los objetivos de punto de recuperación como se detallan en el análisis de impacto al negocio.
 - 6.1. Preparar un borrador del informe del análisis de impacto al negocio utilizando los hallazgos iniciales de impacto, resaltando las brechas identificadas en un análisis de brechas.
 - 6.1.1. Proporcionar una declaración de la misión, los objetivos y las operaciones de la entidad.



Práctica Profesional Tres: Análisis de Impacto al Negocio

- 6.1.2. Resumir el impacto en la misión, objetivos y operaciones de la entidad que puede resultar de un evento.
- 6.1.3. Proporcionar una lista priorizada de los procesos y servicios de la entidad, incluyendo el objetivo de tiempo de recuperación y objetivo de punto de recuperación, un resumen de los requerimientos de recursos necesarios en el tiempo para recuperar y reanudar las operaciones, y un análisis de brechas entre las capacidades actuales y las capacidades necesarias para cumplir con el objetivo de tiempo de recuperación y el objetivo de punto de recuperación definido.
- 6.1.4. Entregar el borrador del informe a los representantes de las gerencias funcionales participantes y a los representantes de proveedores de terceros para obtener su retroalimentación.
- 6.1.5. Revisar la retroalimentación obtenida de los representantes de las gerencias funcionales y representantes de proveedores de terceros. Ajustar los resultados según sea necesario.
- 6.1.6. Calendarizar talleres de trabajo o reuniones con los representantes de las gerencias funcionales y representantes de proveedores de terceros para discutir los hallazgos iniciales según sea necesario.
- 6.1.7. Actualizar los hallazgos según sea necesario para reflejar los cambios derivados de los talleres de trabajo o reuniones.
- 6.2. Preparar el informe final del análisis de impacto al negocio.
- 6.3. Preparar y realizar una presentación formal de los hallazgos en el informe final análisis de impacto al negocio a los líderes.
- 6.4. Lograr la aceptación de los líderes para el objetivo de tiempo de recuperación y el objetivo de punto de recuperación para cada área operativa según se definieron de acuerdo a los hallazgos en el informe final del análisis de impacto al negocio.

Práctica Profesional Cuatro: Estrategias de Continuidad de Negocio

Objetivos

- Seleccionar estrategias rentables (costo-efectivas) para reducir las deficiencias identificadas durante los procesos de evaluación del riesgo y el análisis de impacto al negocio.

Rol del Profesional

1. Utilizar los datos recopilados durante los procesos de la evaluación del riesgo y del análisis de impacto al negocio para identificar las estrategias de continuidad y recuperación disponibles para las operaciones de la entidad que permitan alcanzar el objetivo de tiempo de recuperación y el objetivo de punto de recuperación como se define en el análisis de impacto al negocio.
2. Utilizar los datos recopilados durante los procesos de la evaluación del riesgo y del análisis de impacto al negocio para identificar las estrategias de continuidad y recuperación disponibles para la tecnología de la entidad que permitan alcanzar el objetivo de tiempo de recuperación y el objetivo de punto de recuperación como se define en el análisis de impacto al negocio.
3. Identificar los problemas de la cadena de suministro, tanto para los proveedores como para los clientes, a partir del análisis de impacto al negocio, que pueden afectar a la selección de una estrategia de recuperación.
4. Consolidar estrategias cuando sea apropiado para reducir costos y / o complejidad.
5. Evaluar el costo de implementar las estrategias identificadas a través de un análisis de costo / beneficio.
6. Recomendar estrategias y obtener la aprobación para implementarlas.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Utilizar los datos recopilados durante los procesos de la evaluación del riesgo y del análisis de impacto al negocio para identificar las estrategias de continuidad y recuperación disponibles para las operaciones de la entidad que permitan alcanzar el objetivo de tiempo de recuperación y el objetivo de punto de recuperación como se define en el análisis de impacto al negocio.
 - 1.1. Revisar los requisitos de recuperación identificados para cada área operacional de la entidad.
 - 1.2. Identificar estrategias alternas de continuidad de negocio. Opciones potenciales incluyen, pero no están limitadas a, las siguientes estrategias⁷:
 - 1.2.1. Desarrollar procedimientos manuales alternativos.
 - 1.2.2. Desarrollar acuerdos recíprocos.⁸ Los acuerdos recíprocos deben ser probados para asegurar su viabilidad como opción de recuperación; estas estrategias pueden no ser una

⁷ Las estrategias listadas en la Sección Uno desde la 1.2.1 a 1.2.13 se enumeran en ningún orden en particular. Las necesidades de las entidades específicas pueden variar.

⁸ Los acuerdos recíprocos son los más comúnmente utilizados en las operaciones de pequeñas empresas, acuerdos de ayuda mutua del sector público, y ambientes de manufactura.



Práctica Profesional Cuatro: Estrategias de Continuidad de Negocio

- opción viable para un período prolongado y pueden requerir una estrategia adicional de recuperación a más largo plazo.
- 1.2.3. Identificar el espacio interno de doble uso que podría ser equipado para apoyar la recuperación, tales como salas de conferencias, salas de entrenamiento o cafeterías. Asegúrese de que el tiempo necesario para preparar y equipar el espacio es consistente con los requisitos de objetivo de tiempo de recuperación y el objetivo de punto de recuperación.
 - 1.2.4. Identificar un sitio alternativo externo.
 - 1.2.5. Contratar proveedores de servicios tercerizados o subcontratistas
 - 1.2.6. Transferir la carga de trabajo a un sitio sobreviviente.
 - 1.2.7. Transferir al personal y la carga de trabajo a un sitio sobreviviente.
 - 1.2.8. Suspender las operaciones que no son sensibles al tiempo en un sitio de sobrevivencia y transferir el personal y / o la carga de trabajo desde el lugar afectado a el sitio de sobrevivencia. Esto también se conoce como el desplazamiento.
 - 1.2.9. Construir un sitio alternativo dedicado.
 - 1.2.10. Dirigir personal impactado para que trabajen desde casa.
 - 1.2.11. Ambientes de manufactura tienen necesidades específicas y pueden usar las siguientes estrategias de recuperación:
 - Reparar / reconstruir en el momento del evento.
 - Cambiar la producción a otra línea o sitio.
 - Utilizar el inventario existente.
 - Utilizar el exceso de capacidad en otras plantas.
 - Comprar producto de vuelta al cliente(s) y redistribuirlo según sea necesario.
 - Proporcionar un producto sustituto en lugar de los productos que no están disponibles.
 - Tercerizar / externalizar la producción.
 - 1.2.12. Cumplir con el objetivo de punto de recuperación para la recuperación de los registros vitales en papel y aquellos que están en proceso de trabajo y asegurar que sean accesibles después de un evento, se pueden usar las siguientes estrategias: fotocopias, escaneos o almacenamiento en la nube.
 - 1.2.13. Revisar las opciones de sitio alternativo utilizando los siguientes criterios según corresponda: la ubicación, la disponibilidad y adecuación del espacio, capacidades de comunicación incluyendo voz y datos, la disponibilidad de equipos y materias primas y la dureza y la sostenibilidad de la instalación, incluida la disponibilidad de recursos tales como fuente de alimentación eléctrica redundante y agua.
 - 1.3. Evaluar la viabilidad de las estrategias alternas contra los resultados del análisis de impacto al negocio utilizando los siguientes criterios según corresponda: la capacidad de cumplir el objetivo de tiempo de recuperación y objetivo de punto de recuperación definido, una comparación de las soluciones, las ventajas y desventajas, costos incurridos durante la preparación, mantenimiento y ejecución y la capacidad de mitigación y opciones de control.
 - 1.4. Revisar las coberturas de seguros existentes, que puede incluir, pero no se limitan a, gasto extra, interrupción del negocio, interrupción del negocio contingente, nómina y las inundaciones, por lo que las estrategias de continuidad de negocio seleccionadas complementarán la cobertura que se utiliza durante el proceso de recuperación.
 - 1.5. Desarrollar un análisis de costo / beneficio preliminar de las estrategias seleccionadas para las operaciones de la entidad.



Práctica Profesional Cuatro: Estrategias de Continuidad de Negocio

2. Utilizar los datos recopilados durante la evaluación del riesgo y el análisis de impacto al negocio para identificar las estrategias de continuidad y recuperación disponibles para la tecnología de la entidad, que cumplan con el objetivo de tiempo de recuperación y el objetivo de punto de recuperación como se define en el análisis de impacto al negocio.
 - 2.1. Revisar los requerimientos de recuperación identificados para la tecnología de la entidad en cada área operativa.
 - 2.2. Identificar las estrategias de recuperación alternas para la tecnología. Las opciones potenciales incluyen, pero no se limitan a, las siguientes estrategias⁹:
 - 2.2.1. Desarrollar procedimientos de ejecución manual para cada área operativa en conjunto con representantes de las gerencias funcionales.
 - 2.2.2. Implementar un entorno de tecnología de activo / activo a través de un centro de datos dual, eliminando así la necesidad de recuperación.
 - 2.2.3. Implementar un entorno de tecnología activo / pasivo para alta disponibilidad de la tecnología sensible al tiempo, proporcionando un modo para un reinicio rápido de la tecnología necesaria.
 - 2.2.4. Contratar proveedores de servicios tercerizados o subcontratistas para proporcionar el entorno de recuperación de la tecnología, que puede incluir un contrato tradicional de sitio caliente o *hot site* con un proveedor en el que el proveedor proporciona el equipo para recuperarse (el equipo pertenece al inventario del proveedor), o un contrato por el cual la entidad pone su propio equipo para recuperación en las instalaciones del proveedor.
 - 2.2.5. Tercerizar todo el entorno de la tecnología a través de una estrategia como la computación en nube.
 - 2.2.6. Identificar un sitio donde se produciría la recuperación, pero la construcción previa tendría solamente calefacción, ventilación y aire acondicionado (HVAC), así como las capacidades eléctricas; se instala la tecnología en el momento de un desastre (sitio tibio / *warm site*).
 - 2.2.7. Identificar un sitio donde se produciría la recuperación, pero todo se construye e instala solamente en el momento de un desastre (sitio frío / *cold site*).
 - 2.2.8. Identificar estrategias para la recuperación de datos en forma electrónica que cumplan con el objetivo de punto de recuperación establecido para estos registros y asegurar que están disponibles después de un desastre. Garantizar que el tiempo para restaurar los datos está dentro de los objetivos de tiempo de recuperación y objetivos de punto de recuperación identificados y establecidos en el análisis de impacto al negocio.
 - 2.2.9. Revisar las opciones de sitio alternativo utilizando los siguientes criterios, según corresponda: la ubicación, la disponibilidad y adecuación del espacio, las capacidades de comunicación (incluyendo voz y datos), la disponibilidad de equipos y materias primas, y la dureza y la sostenibilidad del sitio (incluida la disponibilidad de recursos tales como fuente de alimentación eléctrica redundante y agua).
 - 2.3. Evaluar la viabilidad de las estrategias alternas contra los resultados del análisis de impacto al negocio utilizando los siguientes criterios, según corresponda: la capacidad de cumplir el objetivo de tiempo de recuperación y objetivo de punto de recuperación definidos, una comparación de las soluciones, las ventajas y desventajas, costos incurridos durante la preparación, mantenimiento y ejecución; y la capacidad de mitigación y opciones de control.
 - 2.4. Desarrollar un análisis costo / beneficio preliminar para las estrategias seleccionadas para la tecnología de la entidad.

⁹ Las estrategias listadas en la Sección Dos desde la 2.2.1 a la 2.2.9 se enumeran en ningún orden en particular. Las necesidades de las entidades específicas pueden variar.



Práctica Profesional Cuatro: Estrategias de Continuidad de Negocio

3. Identificar los problemas de la cadena de suministro, tanto para los proveedores como para los clientes, a partir del análisis de impacto al negocio, que pueden afectar a la selección de una estrategia de recuperación.
 - 3.1. Identificar cualquier problema en la entrega que pueda derivarse de la reubicación en otro sitio.
 - 3.2. Asegurar que el efecto en la operación y los procesos de la entidad es mínimo en el caso de un evento que sufra el proveedor.
 - 3.3. Identificar cualquier problema que pueda producirse con la entrega del producto a un cliente en el caso de una interrupción de las operaciones del cliente.
4. Consolidar estrategias cuando sea apropiado para reducir costos y / o complejidad. Identificar las áreas en las que la misma estrategia de recuperación podría ser utilizada para cumplir con los requisitos para múltiples áreas de operaciones, tales como el uso de un solo sitio alternativo para la recuperación de las operaciones del negocio, en diferentes sitios que no se espera que se vean afectados por el mismo evento.
5. Evaluar el costo de implementar las estrategias identificadas a través de un análisis de costo / beneficio.
 - 5.1. Estimar el costo de la implementación y el costo de mantener la recuperación para las estrategias de recuperación identificadas.
 - 5.2. Validar que la estrategia de recuperación que está siendo implementada es adecuada para el área operativa impactada.
 - 5.2.1. Considerar factores económicos, regulatorios y factores adicionales que podrían afectar la recuperación.
 - 5.2.2. Asegurar que la solución de recuperación se encuentra alineada a los objetivos de recuperación.
 - 5.2.3. Asegurar de que el costo de la recuperación está en línea con el valor de lo que ha de ser recuperado.
6. Recomendar estrategias y obtener la aprobación para implementarlas.

Práctica Profesional Cinco: Respuesta a Incidentes

Objetivos

- Desarrollar y ayudar con la implementación de un sistema de gestión de incidentes que defina los roles organizacionales, las líneas de autoridad y la sucesión de autoridad.
- Definir los requerimientos para desarrollar e implementar el plan de respuesta a incidentes de la entidad.
- Asegurar que la respuesta a incidentes se coordina con organizaciones externas de una manera oportuna y eficaz cuando sea apropiado.

Rol del Profesional

1. Identificar las directrices de preparación para emergencias y respuesta a incidentes aplicables.
2. Identificar tipos potenciales de incidentes que pueden ocurrir y los impactos que pueden generar.
3. Identificar las capacidades de respuesta necesarias.
4. Revisar los procedimientos de respuesta a incidentes existentes y evaluar las capacidades para proteger la vida, la propiedad y el medio ambiente.
5. Recomendar el desarrollo e implementación de un sistema de gestión de incidentes para el comando, control y coordinación de personal y recursos durante las actividades de respuesta a incidentes. Desarrollar y apoyar en la implementación de una delegación de autoridad que defina los roles organizacionales, las líneas de autoridad y la sucesión de la autoridad.
6. Revisar y coordinar los planes y procedimientos de respuesta a incidentes con el personal y las organizaciones pertinentes, según sea apropiado.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Identificar directrices aplicables sobre preparación para emergencias respuesta a incidentes, incluyendo, pero no limitado a, la salud y la seguridad de vida, prevención de incendios, y los requeridos por las regulaciones emitidas por los gobiernos federal, estatal, provincial, de condado, parroquia, tribal o niveles locales de gobierno.
2. Identificar tipos potenciales de incidentes que pueden ocurrir y los impactos que pueden generar.
 - 2.1. Para cada tipo de incidente, identificar escenarios potenciales que se puedan generar y tomar nota de la siguiente información:
 - 2.1.1.El origen o la ubicación y si el evento fue interno o externo.
 - 2.1.2.El alcance o magnitud.
 - 2.1.3.El área de impacto.
 - 2.2. Para cada tipo de incidente, identificar los impactos potenciales, incluyendo, pero no limitado a, las víctimas, daños materiales y la contaminación ambiental.



Práctica Profesional Cinco: Respuesta a Incidentes

3. Identificar las capacidades de respuesta necesarias.
 - 3.1. Capacidades necesarias para proteger la seguridad de la vida pueden incluir, pero no se limitan a, evacuación, refugio en el lugar para ser utilizado en caso de un evento de peligro exterior o en el aire, bloqueo, y el conteo de todas las personas relacionadas a la organización y visitantes afectados por el incidente.
 - 3.2. Las capacidades necesarias para proteger la propiedad incluyendo:
 - 3.2.1. La supervisión y la operación de los sistemas de construcción y equipamiento, incluidos los servicios públicos, ventilación y aire acondicionado, detección y extinción de incendios, las comunicaciones y la advertencia.
 - 3.2.2. Conservación de la propiedad para preparar una instalación para un evento previsto, tales como el cierre ordenado ante un huracán, y para minimizar el daño con el salvamento y la limpieza después de un evento.
 - 3.2.3. Extinción de incendios, incluyendo actividades tales como la planificación coordinada con el departamento público de bomberos y entrenamiento en el uso del extintor.
 - 3.3. Capacidades necesarias para evitar la contaminación del medio ambiente, tales como la supervisión y la operación de los sistemas diseñados para contener materiales peligrosos en el lugar.
4. Revisar los procedimientos de respuesta a incidentes existentes y evaluar las capacidades para proteger la vida, la propiedad y el medio ambiente.
 - 4.1. Realizar un proceso de recopilación de información.
 - 4.1.1. Identificar las capacidades de respuesta necesarias para proteger la vida, la propiedad y el medio ambiente de los tipos de incidentes identificados.
 - 4.1.2. Identificar y establecer relaciones con los departamentos internos y organismos externos que tienen responsabilidades en la preparación para emergencias y respuesta a incidentes.
 - 4.1.3. Reunir los procedimientos de respuesta a incidentes de los departamentos internos y aquellos individuos que tienen la responsabilidad asignada para la respuesta a incidentes, incluyendo, pero no limitado a, el medio ambiente, la salud, la seguridad de vida (*safety*), la seguridad física (*security*) y la gestión.
 - 4.1.4. Reunir los procedimientos de respuesta a incidentes y una descripción de las capacidades de respuesta de fuentes externas que tengan capacidades de respuesta u obligaciones conocidas.
 - 4.1.5. Contactar a las agencias públicas, incluyendo, pero no limitado a, servicios médicos, bomberos, policías y equipos de materiales peligrosos, para identificar las necesidades, prácticas y recursos y establecer relaciones de enlace con ellos.
 - 4.2. Llevar a cabo una evaluación de las necesidades de recursos.
 - 4.2.1. Identificar los recursos necesarios para proteger la vida, la propiedad y el medio ambiente de los tipos de incidentes identificados.
 - 4.2.2. Identificar al personal interno y externo, incluidos los de los organismos públicos, que están capacitados para responder a los incidentes identificados.
 - 4.2.3. Identificar los sistemas y equipos, incluyendo, pero no limitado a, la detección, alarma, comunicaciones, supresión, y los sistemas de contención disponibles para respuesta a incidentes.
 - 4.3. Verificar que los acuerdos de ayuda mutua o asociación se documentan y se mantienen actualizados, si aplica.



Práctica Profesional Cinco: Respuesta a Incidentes

- 4.4. Revisar los planes de respuesta a incidentes para determinar si los procedimientos siguientes se abordan: monitoreo de peligros o amenazas y detección de incidentes; la notificación inmediata a la persona responsable, el departamento y / o entidad; alertar a los primeros en responder y advertir a las personas afectadas o potencialmente afectadas; y llevar a cabo escalamientos de acuerdo a como se desarrollan los acontecimientos
- 4.5. Identificar las discrepancias y / o brechas entre las necesidades y las capacidades identificadas.
5. Recomendar el desarrollo e implementación de un sistema de gestión de incidentes para el comando, control y coordinación de personal y recursos durante las actividades de respuesta a incidentes. Desarrollar y apoyar en la implementación de una delegación de autoridad que defina los roles organizacionales, las líneas de autoridad y la sucesión de la autoridad.
 - 5.1. Documentar procedimientos para la evaluación y el escalamiento, incluyendo la participación de los servicios internos y externos adicionales y el proceso para la obtención de recursos adicionales si fuera necesario.
 - 5.2. La notificación de incidentes debe incluir actualizaciones iniciales y periódicas de análisis de situación.
 - 5.3. Un centro físico o virtual llamado centro de operaciones de emergencia (*emergency operations center, EOC*) debe ser establecido para facilitar la coordinación de las actividades de respuesta, de continuidad y recuperación.
 - 5.4. El EOC debe ser dimensionado para albergar el número previsto de personas y equipado para soportar la ocupación durante los tipos de incidentes identificados.
 - 5.5. El EOC debe estar equipado con capacidades de comunicaciones completas, tales como la radio de dos vías, correo electrónico, mensajes de texto, buscapersonas, teléfonos fijos y móviles de voz y comunicaciones de datos necesarios para apoyar la gestión de incidentes.
 - 5.6. Las Comunicaciones durante un incidente deben ser documentadas en la medida posible y de forma práctica.
 - 5.7. Los procedimientos operativos deben incluir la gestión y las operaciones del EOC incluidas las comunicaciones y el flujo de información, así como el cierre del EOC cuando sea apropiado.
6. Revisar y coordinar los planes y procedimientos de respuesta a incidentes con el personal y las organizaciones pertinentes, según sea apropiado.
 - 6.1. Identificar los documentos, tales como los utilizados para los planes de prevención de incendios y manejo de materiales peligrosos, que deben ser presentados a los organismos públicos para mantener el cumplimiento de la normativa aplicable.
 - 6.2. Asistir en la coordinación de los planes y procedimientos de respuesta con los organismos públicos y los recursos externos.

Práctica Profesional Seis: Desarrollo e Implementación del Plan

Objetivos

- Documentar los planes que serán usados durante un incidente que permitan a la entidad seguir funcionando.

Rol del Profesional

1. Utilizar las estrategias aprobadas desarrolladas en la Práctica Profesional Cuatro como base para la documentación del plan.
2. Definir la estructura para la documentación del plan.
3. Coordinar el esfuerzo para documentar los planes de recuperación para las operaciones de la entidad y la infraestructura de apoyo.
4. Publicar los documentos del plan.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Utilizar las estrategias aprobadas desarrolladas en la Práctica Profesional Cuatro como base para la documentación del plan.
 - 1.1. Diseñar, desarrollar e implementar estrategias de recuperación para las operaciones de la entidad.
 - 1.1.1. Identificar los requerimientos que serán usados en la creación del plan de continuidad de negocio.
 - 1.1.2. Dar reportes sobre el progreso del desarrollo e implementación del plan a los líderes y / o al Comité de Dirección¹⁰.
 - 1.1.3. Completar todas las tareas requeridas para la implementación del plan, que pueden incluir, pero no se limitan a:
 - 1.1.3.1. Adquirir recursos del plan de recuperación y continuidad de negocio que garanticen que se incluyen los requisitos de recursos internos y externos.
 - 1.1.3.2. Establecer de contratos de respuesta, recuperación, restauración y continuidad del negocio.
 - 1.1.3.3. Establecer controles de acceso para el desarrollo y mantenimiento de la documentación.
 2. Definir la estructura para la documentación del plan.
 - 2.1. Determinar cómo se organizará el plan e identificar los equipos necesarios para documentar los planes¹¹.
 - 2.1.1. Asegurar el alineamiento con el alcance del proceso de planeación.

¹⁰ Ver Práctica Profesional Uno para más detalles sobre la definición de la estructura de reporte.

¹¹ Esto se refiere a los equipos que se crean para documentar los planes y pueden diferir de los equipos que ejecutan planes.



Práctica Profesional Seis: Desarrollo e Implementación del Plan

- 2.1.2. Los tipos de planes a ser documentados pueden incluir, pero no se limitan a, estratégico (incluida la planificación de la sucesión), operacional, de respuesta a incidentes, recuperación, restauración y de vuelta a la operación normal.
- 2.1.3. Consideraciones sobre la estrategia pueden incluir, pero no se limitan a, si el término será corto (por ejemplo, un día o un mes) o largo (tales como más de un mes); si los impactos serán locales (sitio o campus específico), regional o de toda la empresa; y si es posible un impacto en cascada.
- 2.2. Definir los roles y responsabilidades para el desarrollo del plan, incluyendo:
 - 2.2.1. Identificar las tareas que deben emprenderse.
 - 2.2.2. Desarrollar una línea de tiempo (*timeline*) para la finalización del plan.
 - 2.2.3. Revisar, evaluar y recomendar herramientas, que pueden incluir, pero no se limitan a, software de planificación, bases de datos, software especializado y plantillas.
 - 2.2.4. Plantillas de desarrollo que se pueden utilizar para capturar información sobre los procesos, matrices de tecnología y diagramas de flujo.
 - 2.2.5. Identificar otros documentos de apoyo según sea necesario.
 - 2.2.6. Asegurar que existen mecanismos incorporados para facilitar el mantenimiento, tales como el control de versiones.
- 2.3. Definir los requisitos de contenido para el plan, que pueden incluir, pero no se limitan a:
 - 2.3.1. Política y gobierno, tales como las políticas y procedimientos de continuidad de negocio, niveles de autorización, que se pueden encontrar en el gobierno corporativo, y una declaración de confidencialidad.
 - 2.3.2. El alcance y objetivos, que deben estar alineados con la misión, metas y objetivos de la entidad y las políticas de continuidad de negocio, e incluir la identificación de las operaciones sensibles en el tiempo y los recursos necesarios para soportarlas.
 - 2.3.3. Cualquier supuesto encontrado en el proceso de planeación.
 - 2.3.4. La estructura del personal involucrado en el proceso; incluyendo la descripción, la estructura organizativa y los roles y responsabilidades de cada equipo.
 - 2.3.5. Los procedimientos de activación del plan deben incluir la evaluación de incidentes, el escalamiento, el proceso de reporte, los procedimientos de declaración y los procedimientos de recuperación y restauración.
- 3. Coordinar el esfuerzo para documentar los planes de recuperación para las operaciones de la entidad y la infraestructura de apoyo, que puede incluir, pero no se limita a, los siguientes tipos de planes:
 - 3.1. Un plan de gestión de incidentes, que debe incluir lo siguiente:
 - 3.1.1. Procedimientos de seguridad de vida.
 - 3.1.2. Procedimientos de mando y control de incidentes.
 - 3.1.3. Roles y responsabilidades para el personal involucrado en la gestión de incidentes.
 - 3.1.4. La ubicación del centro de operaciones de emergencia (EOC) y los procedimientos de su activación.
 - 3.1.5. El proceso para la realización de una evaluación, que debe incluir la protección del sitio de una pérdida adicional; un análisis de costo / beneficio de la reparación frente a la sustitución de activos de la entidad (por ejemplo, equipos, tecnología, documentos, datos, mobiliario, instalaciones o la planta); el tiempo necesario estimado para reparar o reemplazar activos de la entidad; los métodos de restauración acordados para los activos de la entidad; el proceso de aprobación de las consideraciones de restauración y de seguros; y el proceso de rescate.

- 3.2. Un plan de gestión y comunicación de crisis¹², que debe incluir lo siguiente:
 - 3.2.1. Una lista de los individuos que serán parte del equipo de gestión de crisis.
 - 3.2.2. Un esquema de los procedimientos de transición de la respuesta de incidentes a la gestión de crisis y continuidad de negocio.
 - 3.2.3. Procedimientos de notificación para la comunicación a las partes interesadas durante el evento (tales como actualizaciones de estado, comunicados de prensa y otras comunicaciones dirigidas y diseñadas para las partes interesadas), que pueden incluir, pero no están limitados a, los medios de comunicación, los empleados y sus familias, los organismos reguladores, equipos de primera respuesta de emergencias, agencias, servicios especiales de materiales peligrosos, inversores, la junta de directores de gobierno u otra autoridad de liderazgo relevante, representantes de los trabajadores y otros grupos involucrados (tales como clientes, vendedores o proveedores).
- 3.3. Un plan de activación del sitio de recuperación, que debe incluir lo siguiente:
 - 3.3.1. Procedimientos de alerta.
 - 3.3.2. Procedimientos de declaración.
 - 3.3.3. Infraestructura de recuperación proporcionada, que puede incluir:
 - 3.3.3.1. Administración y logística
 - 3.3.3.2. Entrega de nuevo equipo de la forma “justo a tiempo” (*just-in-time*)
 - 3.3.3.3. Servicios y procedimientos técnicos, como las redes de comunicación (incluyendo voz, datos, e inalámbrico); preparación de datos; y soporte de aplicaciones.
 - 3.3.3.4. Enlace de usuario final
 - 3.3.3.5. Operaciones de negocio
 - 3.3.3.6. Logística y comunicaciones entre-sitios
 - 3.3.3.7. Proceso y procedimiento de recuperación de la producción
- 3.4. Plan de recuperación operacional, que debe incluir lo siguiente:
 - 3.4.1. Equipos de recuperación, incluyendo tanto los equipos primarios como los alternos.
 - 3.4.2. La logística involucrada en la organización para el viaje y alojamiento del personal de recuperación, el transporte de los datos necesarios para la recuperación y asegurando la obtención de recursos adicionales, según sea necesario.
 - 3.4.3. Documentación de recursos, incluyendo, pero no limitado a, los requisitos tecnológicos, los registros vitales, comunicaciones de voz y datos, contactos externos críticos y proveedores y los requerimientos de equipo.
- 3.5. Un plan de continuidad de negocio, que debe incluir lo siguiente:
 - 3.5.1. Equipos de recuperación, incluyendo tanto los miembros primarios como los alternos
 - 3.5.2. Formas alternativas de conducir el negocio cuando los recursos normales no están disponibles
 - 3.5.3. Procesos, procedimientos y comunicación de la continuidad de negocio
 - 3.5.4. La movilización de los recursos alternos
 - 3.5.5. La gestión de los recursos alternos
- 3.6. Un plan o planes de recuperación de tecnología, que debe incluir lo siguiente:
 - 3.6.1. Equipos de recuperación, incluyendo tanto los miembros primarios como los alternos

¹² Ver también Prácticas Profesionales Cinco y Nueve.



Práctica Profesional Seis: Desarrollo e Implementación del Plan

- 3.6.2. Movilización de recursos
 - 3.6.2.1. La logística involucrada en la organización para el viaje y alojamiento del personal de recuperación, la adquisición de los datos necesarios para la recuperación y la obtención de recursos adicionales.
 - 3.6.2.2. Los recursos requeridos
 - 3.6.2.2.1. Los requisitos de almacenamiento, que pueden incluir, pero no están limitados a, dispositivos de almacenamiento en red y dispositivos de almacenamiento de datos.
 - 3.6.2.2.2. Hardware de comunicaciones de voz y datos, que puede incluir, pero no se limita a, conmutadores de red y equipos de interfaz.
 - 3.6.2.2.3. Requerimientos de hardware y software, que puede incluir, pero no se limita a, procesadores, las unidades de cinta/discos, biblioteca de cinta silo/virtual, software de aplicación, sistemas operativos, código fuente y dispositivos y software de seguridad.
 - 3.6.2.2.4. Requerimientos de infraestructura, que pueden incluir, pero no están limitadas a, las fuentes de alimentación y controladores eléctricos; calefacción, ventilación y aire acondicionado (HVAC); cableado; y la seguridad de acceso.
 - 3.6.2.2.5. Requerimientos de seguridad de la información, que pueden incluir, pero no están limitados a, firewalls, autenticación, virus o protección contra software espía, cifrado, contactos y proveedores clave, y las necesidades de equipo.
- 3.6.3. El plan de recuperación de la tecnología debe describir un procedimiento detallado para la recuperación del entorno de la tecnología, incluyendo los siguientes pasos:
 - 3.6.3.1. Identificar las dependencias de las aplicaciones.
 - 3.6.3.2. Crear un proceso para gestión de cambios.
 - 3.6.3.3. Crear un proceso para gestión de problemas.
 - 3.6.3.4. Un plan de pruebas, ejercicio y mantenimiento (incluidos los requisitos de ejercicio); alcance, los objetivos y el calendario; y un programa de mantenimiento del plan.
- 4. Publicar los documentos del plan.
 - 4.1. Proporcionar un borrador final a los equipos de desarrollo de plan y a los dueños de los procesos de negocio.
 - 4.2. Obtener las firmas autorizadas.
 - 4.3. Publicar y distribuir los planes o partes de los planes para cualquier persona con un rol documentado incluyendo la información necesaria para que los participantes ejecuten sus roles.
 - 4.4. Establecer procedimientos para la distribución y el control de los planes (como una lista de distribución), incluyendo cambios en el plan y actualizaciones.

Práctica Profesional Siete: Programas de Concientización y Entrenamiento

Objetivos

- Establecer y mantener programas de entrenamiento y concientización que tienen como resultado que el personal esté habilitado para responder a los incidentes de una manera tranquila y eficiente.

Rol del Profesional

1. Establecer los objetivos y componentes del programa de concientización y entrenamiento de continuidad de negocio.
2. Identificar los requerimientos de concientización y entrenamiento a través de las funciones de la entidad.
3. Priorizar los requerimientos de concientización y entrenamiento para el personal interno de la entidad.
4. Desarrollar la metodología para el programa de concientización y entrenamiento de la entidad.
5. Identificar, desarrollar o adquirir herramientas y recursos de concientización y entrenamiento necesarios para alcanzar los objetivos del programa.
6. Supervisar la ejecución de las actividades realizadas para cumplir con los objetivos del programa de concientización y entrenamiento.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Establecer los objetivos y componentes del programa de concientización y entrenamiento de continuidad de negocio.
 - 1.1. Definir el enfoque de la gestión del programa.
 - 1.2. Establecer plazos de implementación.
 - 1.3. Obtener el apoyo de los líderes para el programa.
 - 1.4. Obtener el compromiso del personal relevante.
2. Identificar los requerimientos de concientización y entrenamiento a través de las funciones de la entidad.
 - 2.1. Definir y documentar el nivel deseado de concientización en continuidad de negocio a través de la entidad.
 - 2.2. Definir y documentar los requerimientos de recursos para entrenamiento.
3. Priorizar los requerimientos de concientización y entrenamiento para el personal interno de la entidad.
 - 3.1. Al diseñar un programa de concientización, es importante considerar qué personal interno debe ser consciente de los componentes relevantes del programa BCM. Los temas requeridos de los cuales todos los empleados deben estar conscientes pueden incluir, pero no se limitan a:
 - Objetivos del programa de continuidad de negocio,
 - Notificación y expectativas de los eventos, y
 - Proceso de respuesta a incidentes.



Práctica Profesional Siete: Programas de Concientización y Entrenamiento

- 3.2. Al diseñar un programa de entrenamiento, es importante tener en cuenta cuál es el personal interno que se debe entrenar sobre los componentes relevantes del programa de continuidad de negocio.
 - 3.2.1. Los temas requeridos en los que todos los empleados deben ser entrenados, pueden incluir, pero no se limitan a:
 - Simulacros de evacuación, y
 - Tutoriales basados en escenarios.
 - 3.2.2. Los temas requeridos en los que la gerencia debe ser entrenada, pueden incluir, pero no se limitan a:
 - Simulacros de evacuación, y
 - Tutoriales basados en escenarios.
 - 3.2.3. Los temas requeridos en los que los miembros de los equipos en continuidad de negocio deben ser entrenados, pueden incluir, pero no se limitan a:
 - Simulacros de evacuación,
 - Tutoriales basados en escenarios, y
 - Ejercicios de la tecnología.
4. Desarrollar la metodología para el programa de concientización y entrenamiento de la entidad.
 - 4.1. Realizar una evaluación de las necesidades para el programa de concientización y entrenamiento, que puede incluir, pero no se limita a, los siguientes métodos:
 - Realizar una encuesta de las necesidades con el fin de evaluar el estado actual de concientización y preparación y para determinar si el estado actual está alineado con las expectativas de los líderes y de las mejores prácticas actuales. Los participantes de la encuesta podrían estar en diferentes niveles y pueden incluir diversas partes interesadas, tales como los gerentes funcionales, los participantes en el plan y la población más amplia de negocios.
 - Usar los datos recopilados para identificar tendencias y nuevos desarrollos.
 - Revisar resultados de pruebas y ejercicios previos y realizar un análisis de brechas con base en esos resultados.
 - 4.2. Realizar un estudio de mercado (*benchmark*) para definir el índice de referencia los niveles actuales de concientización y preparación dentro de la entidad contra el nivel deseado e iniciar el plan para abordar las oportunidades de concientización y entrenamiento.
 - 4.3. Diseñar el proceso de entrenamiento.
 - 4.3.1. Definir objetivos, identificar y seleccionar métodos de entrega, incluyendo, pero no limitados a, campañas de concientización, ejercicios, tutoriales basados en escenarios y boletines de noticias.
 - 4.3.2. Definir los roles y responsabilidades para el programa de concientización y entrenamiento.



Práctica Profesional Siete: Programas de Concientización y Entrenamiento

5. Identificar, desarrollar o adquirir herramientas y recursos de concientización y entrenamiento necesarios para alcanzar los objetivos del programa.
 - 5.1. Identificar los recursos internos y externos necesarios para dar soporte al programa, que pueden incluir, pero no se limitan a, cursos, un sitio web dedicado para continuidad de negocio, sitios web relevantes patrocinados por el gobierno, las herramientas de medios sociales sancionadas por la entidad, folletos y carteles de concientización.
 - 5.2. Identificar oportunidades internas y externas adicionales de concientización y entrenamiento, que pueden incluir, pero no se limitan a, conferencias, seminarios web, grupos de usuarios y asociaciones, documentos técnicos y otras publicaciones, organismos de certificación y programas de educación académicas relevantes.
6. Supervisar la ejecución de las actividades realizadas para cumplir con los objetivos del programa de concientización y entrenamiento.
 - 6.1. Calendarizar y realizar actividades de concientización.
 - 6.2. Calendarizar y entregar actividades de entrenamiento.
 - 6.3. Monitorear la efectividad de las actividades de concientización y entrenamiento a través de encuestas de seguimiento u otros métodos.
 - 6.4. Revisar los resultados de las actividades del programa de concientización y entrenamiento. Proporcionar un reporte a los líderes sobre los resultados del programa.

Práctica Profesional Ocho: Ejercicio, Evaluación y Mantenimiento del Plan de Continuidad del Negocio

Objetivos

- Establecer un programa de ejercicio, evaluación y mantenimiento para mantener un estado de preparación.

Rol del Profesional

1. Establecer un programa de ejercicio/prueba.
2. Establecer un programa de mantenimiento del plan.
3. Identificar la gobernanza apropiada.
4. Establecer un proceso de auditoría para el programa de continuidad de negocio.
5. Documentar y comunicar los resultados y las recomendaciones de los procesos de ejercicio/prueba y auditoría.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Establecer un programa de ejercicio/prueba.
 - 1.1. Desarrollar un programa de ejercicio/prueba que cumpla con el alcance y los objetivos del programa de continuidad de negocio de la entidad.
 - 1.1.1. Asegurar que el proceso de recuperación documentado es completo y de que no existan deficiencias.
 - 1.1.2. Identificar cualquier brecha en el proceso y oportunidades de mejora.
 - 1.2. Obtener el apoyo necesario para el desarrollo del programa de ejercicio/prueba.
 - 1.3. Desarrollar un programa efectivo para ejercicio/prueba.
 - 1.3.1. Documentar los criterios de ejercicio/prueba.
 - 1.3.2. Definir cualquier supuesto del programa de ejercicio/prueba.
 - 1.3.3. Con el fin de crear un programa integral, identificar los tipos de ejercicio/prueba que serán incluidos en el programa de ejercicios/prueba. Estos pueden incluir, pero no se limitan a, los siguientes: seguridad de la vida; ensayar el plan paso a paso; prueba de escritorio basada en un escenario; notificación; sitio alternativo; plataforma, infraestructura, o aplicación independiente; proceso funcional; prueba completa de extremo a extremo de una operación o de la tecnología; ejercicio/prueba integral de todos los recursos internos requeridos para recuperar la entidad; y un ejercicio/prueba totalmente integrada tanto con dependencias internas como externas.
 - 1.3.4. Identificar los participantes y sus roles y responsabilidades en el programa de ejercicio/prueba, que puede incluir, pero no se limita a, los equipos de recuperación,

observadores y generadores de reportes, cronometradores, auditores y revisores, facilitadores, proveedores y proveedores de servicios tercerizados.

- 1.4. Definir los objetivos y el alcance del programa de ejercicio/prueba para seleccionar escenarios apropiados.
 - 1.4.1. Crear escenarios realistas basados en la evaluación del riesgo tal como se describe en la Práctica Profesional Dos. Incluir actividades que puedan invocar diversas facetas de las estrategias de recuperación, incluyendo, pero no limitado a, escenarios técnicos definidos como las capacidades operativas; escenarios de procedimiento definidos como la exactitud de los procedimientos; escenarios de logística definidos como la capacidad de acceder al lugar de recuperación y ejecutar sus procedimientos de recuperación; y los escenarios de línea de tiempo definidos como la capacidad de lograr objetivos dentro de los plazos establecidos.
 - 1.4.2. Determinar los requerimientos de ejercicio/prueba y elaborar un plan detallado de actividades.
 - 1.4.2.1. Definir y documentar objetivos para el ejercicio/prueba.
 - 1.4.2.2. Definir y documentar el alcance del ejercicio/prueba. Asegurar que hayan parámetros claros para diferenciar las actividades dentro y fuera del alcance.
 - 1.4.2.3. Definir un proceso de notificación del ejercicio, que puede incluir cualquiera de los ejercicios planeados y anunciados o ejercicios sorpresa sin previo aviso.
 - 1.4.2.4. Calendarice el plazo de tiempo para el ejercicio. Desarrollar un horario específico para el ejercicio/prueba para que sea realizado sobre una base anual o tan a menudo como sea necesario para garantizar la competencia y para cumplir con los requisitos regulatorios. Desarrollar un calendario de ejercicio/prueba progresivo de varios años que incorpore las lecciones aprendidas de ejercicios anteriores.
 - 1.4.2.5. Definir y documentar criterios de evaluación tanto cuantitativos como cualitativos alineados con los objetivos y el alcance del ejercicio/prueba.
 - 1.4.2.6. Identificar las actividades que deben ocurrir antes del ejercicio, que pueden incluir, pero no se limitan a, las siguientes:
 - 1.4.2.6.1. Identificar los recursos requeridos para realizar el ejercicio/prueba.
 - 1.4.2.6.2. Identificar los participantes necesarios para realizar el ejercicio/prueba.
 - 1.4.2.6.3. Distribuir comunicaciones que expliquen los objetivos del ejercicio y los roles de todos los participantes.
 - 1.4.2.6.4. Proporcionar una lista del hardware, software, suministros físicos, equipo y otros artículos requeridos para el ejercicio/prueba.
 - 1.4.2.6.5. Documentar y comunicar las especificaciones del ambiente que será necesario para realizar el ejercicio.
 - 1.4.2.6.6. Especificar si el ejercicio/prueba usará un ambiente de producción o fuera de producción.
 - 1.4.2.6.7. Especificar la hora y fecha del ejercicio/prueba.
 - 1.4.2.6.8. Proporcionar un calendario de eventos y distribuirlo a todos los participantes.
 - 1.4.2.6.9. Establecer plan de cancelación “back-out” (vuelta atrás) para el ejercicio/prueba.
 - 1.4.3. Realizar el ejercicio/prueba como fue planeado.
 - 1.4.3.1. En caso de producirse un incidente real durante un ejercicio/prueba, debe haber un mecanismo predeterminado para cancelar el ejercicio/prueba e invocar el proceso real de continuidad. Esto puede diferir del plan de “back-out” en 1.4.2.6.9.



Práctica Profesional Ocho: Ejercicio, Evaluación y Mantenimiento del Plan de Continuidad del Negocio

- 1.4.3.2. Registrar los eventos del ejercicio/prueba.
- 1.4.3.3. Documentar los resultados del ejercicio/prueba.
- 1.4.3.4. Declarar el final del ejercicio/prueba.
- 1.4.3.5. Realizar los procedimientos de apagado (*shut-down*) durante la conclusión del ejercicio/prueba.
- 1.4.3.6. Realizar cualquier actividad de limpieza (*cleanup*) necesaria.
- 1.4.4. Identificar las actividades que deben ser completadas después del ejercicio/prueba.
 - 1.4.4.1. Llevar a cabo sesiones de interrogación para revisar los resultados del ejercicio/prueba. Identificar las lecciones aprendidas y acciones de mejora.
 - 1.4.4.2. Reportar los resultados del ejercicio/prueba. Proporcionar un resumen exhaustivo con recomendaciones.
 - 1.4.4.3. Documentar un plan de acción para las recomendaciones que resultaron del ejercicio/prueba.
 - 1.4.4.4. Identificar las cuestiones sobresalientes identificadas como resultado del ejercicio/prueba o que existían antes del ejercicio/prueba.
 - 1.4.4.5. Identificar los elementos de acción incluyendo las responsabilidades asignadas a participantes específicos y los plazos de tiempo para la solución.
 - 1.4.4.6. Monitorear el progreso para completar los elementos de acción identificados. Escalar cuando sea necesario de acuerdo con los requerimientos de comunicación de la entidad.
 - 1.4.4.7. Documentar las lecciones aprendidas del ejercicio/prueba incluyendo resultados esperados contra los resultados reales y los no esperados.
 - 1.4.4.8. Comunicar los resultados del ejercicio/prueba a las partes organizacionales relevantes.
- 2. Establecer un programa de mantenimiento del plan.
 - 2.1. Definir el método y el calendario para el programa de mantenimiento del plan.
 - 2.1.1. Definir los dueños de los datos del plan. Identificar personal específico.
 - 2.1.2. Preparar calendarios de mantenimiento y revisión de procedimientos.
 - 2.1.3. Seleccionar herramientas de mantenimiento.
 - 2.1.4. Monitorear las actividades de mantenimiento.
 - 2.1.5. Establecer un proceso de actualización para el plan.
 - 2.1.6. Asegurar que el calendario de mantenimiento del plan aborda todas las recomendaciones documentados que resultaron del ejercicio/prueba.
 - 2.1.7. Reportar sobre las actividades de mantenimiento a las partes organizacionales relevantes.
 - 2.2. Definir un proceso de gestión del cambio para el programa de mantenimiento del plan.
 - 2.2.1. Analizar los cambios en la entidad que darían lugar a cambios en el programa de continuidad de negocio y en el proceso de planificación.
 - 2.2.2. Desarrollar procedimientos de control del cambio para monitorear los cambios. Integrar los procedimientos con los procesos de control de cambios existentes en toda la entidad.
 - 2.2.3. Crear un adecuado control de versiones. Desarrollar procedimientos para la re-edición, distribución y circulación del plan a las partes relevantes.
 - 2.2.4. Identificar listas de distribución del plan para su circulación.
 - 2.2.5. Desarrollar un proceso para actualizar los planes con base en la respuesta a los hallazgos de auditoría.
 - 2.2.6. Crear procedimientos para facilitar el mantenimiento del plan.
 - 2.2.7. Implementar el proceso de control de cambios.



Práctica Profesional Ocho: Ejercicio, Evaluación y Mantenimiento del Plan de Continuidad del Negocio

3. Identificar la gobernanza apropiada.
 - 3.1. Revisar las expectativas de las partes organizacionales relevantes. Las expectativas pueden ser motivadas por los requerimientos de la industria, las necesidades internas de la entidad, y los acuerdos de nivel de servicio.
 - 3.2. Identificar los procesos globales de la entidad, incluyendo una revisión periódica, la mejora, y el proceso de mejora continua.
 - 3.3. Identificar los modelos de gobierno apropiados basados en la industria, nacionales o los estándares internacionales.
 - 3.4. Definir la frecuencia y alcance del ejercicio/prueba que cumpla con las necesidades de la entidad.
 - 3.5. Asegurar la aprobación por las partes organizacionales relevantes.
4. Establecer un proceso de auditoría para el programa de continuidad de negocio.
 - 4.1. Determinar un calendario para realizar una auditoría de auto-evaluación.
 - 4.2. Prepararse para apoyar otras auditorías que pueden ocurrir, que pueden incluir, pero no se limitan a, auditoría interna, auditoría externa o auditoría de tercera parte, auditoría de un ente regulador o una auditoría de segunda parte.
 - 4.3. Documentar cualquier requerimiento de auditoría.
 - 4.4. Seleccionar o desarrollar herramientas que puedan ser necesarias para realizar la auditoría.
 - 4.5. Establecer el calendario de auditoría.
 - 4.6. Llevar a cabo las actividades de auditoría y monitorear el proceso.

La auditoría de las estructuras del plan, contenidos y secciones de acción, puede incluir, pero no se limita a, los requisitos del programa, documentos y estándares; plantillas y planes; requisitos y resultados de ejercicios/pruebas; el repositorio para el plan y los resultados de los ejercicios/pruebas; los procedimientos de control de documentación del plan; el proceso de control de versiones y la documentación; y las listas de distribución y procesos asociados.
 - 4.7. Auditar el proceso de control de cambios para la documentación del plan y el programa de continuidad de negocio.
 - 4.8. Revisar la respuesta a los hallazgos de auditoría.
 - 4.9. Confirmar que las respuestas se presenten y que se documenten los planes de acción. Verificar que todas las acciones realizadas son capturadas en la documentación del plan y la documentación de apoyo.
5. Documentar y comunicar los resultados y las recomendaciones de los procesos de ejercicio/prueba y auditoría.
 - 5.1. Identificar las partes organizacionales relevantes, que pueden incluir, pero no se limitan a, los dueños de procesos, coordinadores de gobierno, comités de supervisión y los líderes de la organización.
 - 5.2. Seleccionar los métodos de comunicación apropiados, incluyendo el nivel de detalle de reportes apropiado y utilizarlos de manera oportuna. Cuando sea apropiado, tener en cuenta las representaciones gráficas o reportes de comparación, dirigidos a audiencias específicas.
 - 5.3. Establecer un proceso de retroalimentación y un ciclo de validación para confirmar que las medidas adecuadas se han tomado como consecuencia de los resultados de los hallazgos de auditoría. Este proceso debe incluir el seguimiento de problemas, la fecha de apertura para asunto a tratar, el propietario del asunto y la fecha de cierre para el asunto.

Práctica Profesional Nueve: Comunicación de Crisis

Objetivos

- Proveer un marco de trabajo para el desarrollo de un plan de comunicación de crisis.
- Asegurar que el plan de comunicación de crisis proporcionará comunicación oportuna y efectiva con las partes internas y externas.

Rol del Profesional

1. Diseñar, desarrollar e implementar un plan de comunicación de crisis.
2. Comunicar y entrenar a los miembros del equipo de comunicación de crisis en sus roles y responsabilidades.
3. Ejercitar/probar el plan de comunicación de crisis.
4. Actualizar el plan de comunicación de crisis.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Diseñar, desarrollar e implementar un plan de comunicación de crisis.
 - 1.1. Revisar el plan de comunicación de crisis existente, identificar y documentar las brechas, según sea necesario. Si no existe un plan, crear el plan.
 - 1.2. Aprovechar los resultados de la evaluación del riesgo tal como se indica en la Práctica Profesional Dos con el fin de identificar eventos potenciales para los cuales se deberían planificar las comunicaciones.
 - 1.3. Definir los objetivos, el alcance y la estructura del plan.
 - 1.4. Establecer la ubicación, roles y responsabilidades para el equipo de comunicación de crisis responsable del plan.
 - 1.4.1. Identificar y documentar la ubicación principal para las operaciones del equipo de comunicación de crisis. Puede ser una ubicación física o virtual.
 - 1.4.2. Identificar la estructura de gobierno para el desarrollo de la mensajería interna.
 - 1.4.3. Identificar la función de los medios de comunicación interna que servirá como el contacto principal para las comunicaciones salientes a los medios.
 - 1.5. Identificar las partes interesadas internas y externas para las comunicaciones de crisis. Ellos pueden incluir, pero no están limitados a, los empleados y sus familias, inversores, clientes, vendedores y proveedores, actividades subcontratadas, aseguradoras, líderes comunitarios, autoridades locales de respuesta, entidades de gobierno, reguladores, organizaciones de trabajadores, competidores, medios de comunicación, *bloggers* de la industria y publicaciones comerciales, y otras partes interesadas o involucradas. Asegurar la alineación del portavoz de la comunicación de crisis con el público para el mensaje.



Práctica Profesional Nueve: Comunicación de Crisis

- 1.6. Desarrollar y documentar el proceso de notificación a las partes interesadas.
 - 1.6.1. Determinar la frecuencia de las comunicaciones antes, durante y después de un evento.
 - 1.6.2. Identificar métodos de comunicación, que pueden incluir, pero no se limitan a, sistemas de notificación de incidentes, correo electrónico y listas de grupos de distribución, llamadas en conferencia, sistemas de intranet, ruedas de prensa, líneas de información de eventos, medios de comunicación (como la prensa escrita, radio, televisión), el Internet, las plataformas de redes sociales y los blogs.
- 1.7. Establecer directrices para identificar el evento y sus posibles impactos.
- 1.8. Establecer directrices para las comunicaciones iniciales después de un evento.
- 1.9. Identificar y asignar los miembros del equipo de comunicación de crisis.
- 1.10. Desarrollar directrices para las comunicaciones con las operaciones de respuesta al incidente.
- 1.11. Documentar muestras de comunicaciones que puedan ser usadas como plantillas durante un evento.
2. Comunicar y entrenar a los miembros del equipo de comunicación de crisis en sus roles y responsabilidades.
 - 2.1. Distribuir el plan de comunicación de crisis a los que se les ha asignado roles y responsabilidades
 - 2.2. Proporcionar entrenamiento a aquellos que se les han asignado roles y responsabilidades. El entrenamiento puede incluir, pero no se limita a, la determinación de los disparadores para iniciar el proceso de comunicación de crisis, los procedimientos de notificación y respuesta, y el protocolo adecuado para la emisión de comunicaciones
3. Ejercitar/probar el plan de comunicación de crisis.
 - 3.1. Establecer un calendario de ejercicios/pruebas para el plan de comunicación de crisis que sea consistente con las directrices que se describen en la Práctica Profesional Ocho.
 - 3.2. Determinar la metodología para los ejercicios/pruebas del plan de comunicación de crisis.
 - 3.3. Desarrollar el escenario, alcance y objetivos para cada ejercicio/prueba.
 - 3.4. Realizar una sesión para determinar las lecciones aprendidas después del ejercicio/prueba. Documentar los asuntos de acciones correctivas.
4. Actualizar el plan de comunicación de crisis.
 - 4.1. Actualizar el plan en base a los resultados de los ejercicios/pruebas realizadas y de acuerdo con el calendario de mantenimiento del plan establecido en la Práctica Profesional Ocho.

Práctica Profesional Diez: Coordinación con Dependencias Externas

Objetivos

- Establecer políticas y procedimientos para coordinar las actividades de respuesta a incidentes con las entidades públicas.

Rol del Profesional

1. Identificar y establecer procedimientos de respuesta a incidentes de acuerdo con la Práctica Profesional Cinco.
2. Identificar las directrices aplicables de preparación para emergencias y respuesta a incidentes y los organismos que tienen jurisdicción sobre las instalaciones y actividades de la entidad.
3. Coordinar procedimientos de respuesta a incidentes con entidades externas.

Actividades

El profesional en continuidad de negocio demostrará su conocimiento al realizar las siguientes actividades:

1. Identificar y establecer procedimientos de respuesta a incidentes de acuerdo con la Práctica Profesional Cinco.
2. Identificar las directrices aplicables de preparación para emergencias y respuesta a incidentes y los organismos que tienen jurisdicción sobre las instalaciones y actividades de la entidad.
 - 2.1. Identificar los organismos reguladores con jurisdicción sobre las instalaciones y operaciones de la entidad. Los organismos pueden incluir, pero no están limitados a, los oficiales de las instalaciones, jefes de bomberos, policía, organismos reguladores y otras organizaciones gubernamentales.
 - 2.2. Identificar los requisitos para la presentación de información acerca de la instalación (por ejemplo, una descripción de su ocupación, los peligros, los sistemas de protección y procedimientos de respuesta) para las organizaciones apropiadas, incluidas las indicadas en el apartado 2.1.
 - 2.3. Identificar los requerimientos sobre inspecciones periódicas de las instalaciones, incluyendo la frecuencia de ejercicios/pruebas y las actividades de entrenamiento.
 - 2.4. Identificar los requerimientos y plazos para la notificación obligatoria de incidentes, incluyendo, pero no limitado a, las deficiencias de los sistemas de protección, incendios, lesiones, muertes, derrames o liberación de materiales peligrosos y otros incidentes.
 - 2.5. Desarrollar o actualizar los procedimientos de preparación para emergencias y respuesta a incidentes para cumplir con las leyes, ordenanzas, regulaciones y otras directivas obligatorias.
 - 2.6. Reportar información a los organismos reguladores según sea apropiado.



Práctica Profesional Diez: Coordinación con Dependencias Externas

3. Coordinar procedimientos de respuesta a incidentes con entidades externas.
 - 3.1. Identificar la entidad externa que actuará como el primer nivel de respuesta en las instalaciones de la entidad en el caso de un incidente.
 - 3.2. Desarrollar y documentar los procedimientos de alerta de emergencia (por ejemplo, alertas automáticas a través de alarma contra incendios, o alertas manuales a través de protocolos de telefonía y notificación) y los requerimientos (como la notificación obligatoria de los derrames, lesiones y otros incidentes).
 - 3.3. Identificar los representantes de las entidades de primera respuesta y establecer relaciones de enlace con el personal relevante de las entidades.
 - 3.4. Invite personal de entidades de primera respuesta para visitar las instalaciones de la entidad y solicitarles proporcionar recomendaciones para mejorar los planes de respuesta a incidentes.
 - 3.5. Identificar y documentar las funciones y responsabilidades de respuesta a incidentes para los tipos de incidentes y escenarios descritos en la Práctica Profesional Cinco.
 - 3.6. Coordinar, conducir y participar en el entrenamiento, simulacros y ejercicios con las agencias externas y de primera respuesta para aumentar la conciencia y el cumplimiento de las regulaciones.
 - 3.7. Llevar a cabo una reunión informativa después de cualquier entrenamiento, simulacro y ejercicios. Documentar las acciones que se deben tomar con el fin de mejorar las capacidades de respuesta a incidentes.
 - 3.8. Documentar los resultados del ejercicio y las lecciones aprendidas. Proporcionar copias a los líderes y otras partes organizacionales relevantes. Actualizar el plan de respuesta a incidentes utilizando las lecciones aprendidas y la retroalimentación de los ejercicios/entrenamiento de acuerdo con el calendario establecido en la Práctica Profesional Ocho.

Aviso Legal

Estos materiales se presentan únicamente con fines informativos. El DRI Internacional, sus funcionarios, directores, empleados, afiliados y voluntarios ("DRI Internacional") no están ofreciendo esto como asesoramiento legal u otros servicios profesionales. Si bien los mejores esfuerzos se han utilizado en la preparación de estos materiales, el DRI Internacional no hace representaciones o garantías de ningún tipo y no asume responsabilidad de ningún tipo con respecto a la exactitud o integridad de los contenidos y se exime de cualquier garantía implícita de comerciabilidad o aptitud de uso para un propósito particular. El DRI Internacional no se hace sujeto o responsable hacia ninguna persona o entidad con respecto a cualquier pérdida o daño incidental o daños causados consecuentemente, directa o indirectamente, por la información contenida en el presente documento. Cada organización es diferente y las definiciones contenidas en el presente documento pueden no ser adecuadas para su situación. Usted debe buscar los servicios de un profesional competente antes de iniciar cualquier programa de mejora.

Comité

Chair, Raymond Seid, MBCP, CBCLA, ARMP
DRI Coordinator, Al Berman, CBCP, CBCV, MBCP, CBCLA
Harley Lemons, MBCP
Michele Turner, MBCP

Comité de Revisión

Mike Morganti, MBCP, CBCLA
Harvey Betan, CBCP, CBCV, MBCP, CBCLA
Don Schmidt, CBCP, CBCLA

Editores

Chloe Demrovsky, CBCV
Buffy Rojas Leach

Traductor a español

Karol Cordero, CBCP

Reconocimientos

Gary Villeneuve, MBCP, CBCLA, CPSCP, ARMP
Bobby Williams, CBCP, MBCP