



An International Pharmaceutical
Supply Chain Consortium

Planificación de contingencia de desastres naturales

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria, con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresa o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Rx-360 tampoco garantiza que el uso de esta información sea norma obligatoria.

Autores:

Rick Calabrese, Sartorius

Denise Pirko, Boehringer Ingelheim

Dee Ledwin, Daiichi Sankyo

Ken Crossley, Avantor

Norma Amilpa, Eli Lilly

Revisores:

Leigh Davidson, MilliporeSigma

Traducción al español:

Patricia Jiménez-García – ASQ FDC

TABLA DE CONTENIDOS

Sección 1: Introducción.....	4
Sección 2: Importancia del plan preestablecido.....	4
2.1 Minimizar el riesgo para el personal	5
2.2 Minimizar el riesgo para las instalaciones.....	5
2.3 Minimizar el riesgo para la cadena de suministro/la entrega de servicio.....	5
Sección 3: Evaluación del riesgo potencial.....	6
3.1 Riesgo del desastre.....	6
3.2 Riesgo para el negocio.....	7
Sección 4: Preparación del plan de respuesta al desastre	7
4.1 Implementación del centro de comando de desastres.....	8
4.2 Respuesta del personal al desastre	8
4.3 Respuesta de las instalaciones al desastre	11
4.4 Respuesta de los productos y servicios al desastre	12
Sección 5: Preparación del plan de continuidad del negocio	12
Sección 6: Ejecución de los planes preparados	15
6.1 Activación del equipo del centro de comando de desastres.....	15
6.2 Acceso al plan/ubicación del plan	15
6.3 Botiquín para la respuesta ante desastres	16
6.4 Comunicaciones	17
6.5 Lista de verificación del plan de desastres	17
6.6 Formación profesional	17
Sección 7: Ejecución del plan para la continuidad del negocio	18
Sección 8: Evaluación post Mortem	19
8.1 Reunión informativa del plan de recuperación.....	19
8.2 Encuesta al personal y a las partes interesadas en las acciones de respuesta	19
8.3 Evaluación	19
8.4 Documente todas las actividades y haga actualizaciones al plan de contingencia existente basado en comentarios.....	20
Sección 9: Conclusión	20
Apéndice 1: Recursos/enlaces	22
Apéndice 2: Lista de verificación de desastres 1	23
Apéndice 3: Lista de verificación de desastres 2	25

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Sección 1: Introducción

Cuando se produce un desastre natural, a menudo las empresas no están adecuadamente preparadas para gestionar de manera eficaz y expedita la situación a fin de minimizar el impacto al negocio, al cliente y/o al paciente. **Rx-360, un consorcio internacional de la cadena de suministro farmacéutico**, ha creado esta guía de planificación de contingencia a desastres naturales, en respuesta a los desastres naturales que experimentan nuestros miembros. Esta guía puede servir de base para ayudar a su organización a considerar de forma proactiva, cómo reaccionaría internamente en la lamentable circunstancia de que un desastre natural afecte a una de sus ubicaciones comerciales.

Esta guía abordará algunas de las consideraciones empresariales que su organización puede tener para tratar y gestionar desastres. Prepararse y planificar con anticipación le permitirá a su organización interactuar más rápidamente y dirigir a los expertos apropiados, internos y externos (policía, bomberos, respuesta ante desastres), que liderarán las actividades de mitigación de crisis más críticas de su negocio.

Esta guía de planificación de contingencia para desastres naturales puede ser utilizada en el caso de que su organización se vea afectada directamente por un desastre natural, como un tornado, huracán, tsunami, ventisca, tormenta de hielo, etc. Hay una amplia gama de desastres naturales que pueden suceder en todo el mundo, con diferentes niveles de riesgo, severidad e impacto potencial en su sitio. Esta guía no incluye todos los tipos de desastres naturales que pueden afectar a su organización, pero se proporciona con el fin de ayudarle a su organización a prepararse de forma proactiva para que se produzca una transición inmediata del impacto a la recuperación si ocurriera de tal evento. Además, esta guía también puede ser citada para el establecimiento de actividades de mitigación cuando se produzca un desastre natural en uno de sus proveedores globales.

Esta guía ayudará a las empresas a estar informadas sobre el impacto que un desastre natural podría tener en su personal, instalaciones y productos/servicios.

Sección 2: Importancia del plan preestablecido

Las empresas deben prepararse si existe el riesgo de que ocurra un desastre y esta guía explicará los pasos para la preparación de los planes de contingencia en su sitio. Las organizaciones deberían considerar la preparación proactiva de un plan de recuperación de negocio por fases, que se pueda ejecutar inmediatamente cuando se produzca un desastre. Se puede emplear un plan de recuperación de negocios por fases, que incluya un plan de respuesta a desastres y un

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

plan para la continuidad del negocio. La cantidad de pasos de preparación que se anticipen, depende del riesgo y la gravedad del evento que ocurra en su sitio, así como el tipo de industria. Dependiendo del tamaño y la complejidad de una organización, puede existir un plan a nivel global para un desastre, así como más planes específicos para un sitio, dependiendo de los desastres que puedan ocurrir en una región determinada y el tipo de actividad en cada sitio: como manufactura contra administrativo.

2.1 Minimizar el riesgo para el personal

El personal de una organización es el activo más importante. Si el personal no está disponible para trabajar, la organización no puede funcionar. Así, en primera instancia, la organización debe desarrollar un plan para evaluar la responsabilidad y seguridad del personal. Debe haber una lista completa de todo el personal que incluya diferentes maneras de contactarlos. En áreas donde el riesgo es alto en algún tipo de desastre, la lista de contactos debería incluir a familiares o amigos adicionales, en caso de que el personal no pueda ser localizado. Se deben hacer provisiones para ayudar al personal a garantizar que ellos y sus familiares inmediatos estén sanos y salvos. Esto permitirá que el personal pueda apoyar a la organización una vez estén libres de preocupaciones sobre su propia situación de desastre. Un ejemplo de esto sería utilizar un sistema de comunicación de texto de emergencia para contactar a todo el personal.

2.2 Minimizar el riesgo para las instalaciones

El siguiente activo más importante para una organización son las instalaciones donde se ejecutan las operaciones de la organización. Las instalaciones contienen todos los equipos de comunicación y operación, así como toda la documentación y los registros de la organización. Las instalaciones también pueden contener todos los materiales y herramientas utilizados diariamente en el negocio. Debido a esto, un plan de desastre debe prepararse antes de tiempo para proteger estos activos, ya que sin ellos la organización no puede funcionar. En las primeras etapas, se debería construir una instalación que resista los desastres con alto riesgo de ocurrir en la ubicación de las instalaciones. Los sistemas redundantes también deberían examinarse según lo justifique el plan de evaluación de riesgos.

2.3 Minimizar el riesgo para la cadena de suministro/la entrega de servicio

Un desastre puede afectar o incluso detener la capacidad de una organización para proporcionar bienes o servicios. Basándose en la evaluación del riesgo para la ubicación y el tipo de negocio, pudiera ser prudente desarrollar también un plan para la continuidad del negocio con el fin de minimizar cualquier interrupción del negocio debido a un desastre.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Esto puede incluir enviar el inventario a otra ubicación que no tenga el mismo riesgo de desastre, hacer arreglos para que otras ubicaciones proporcionen servicios y almacenar registros y documentos fuera del sitio. Tener un plan establecido puede minimizar los problemas y tratar de hacer frente a la situación para cada caso.

Cuanto más preparada esté una ubicación con un plan completo de desastre implementado antes de un desastre, más rápidamente podrá hacer la transición al plan completo de continuidad comercial, lo que permitirá la continuidad de productos y servicios para maximizar el retorno exitoso del negocio.

Sección 3: Evaluación del riesgo potencial

Hay dos tipos de evaluación de riesgos que deben realizar todas las empresas. El primer tipo evalúa el potencial de un desastre específico que se produzca. Esta información se utilizará para desarrollar el plan de respuesta ante desastres por parte de la organización.

El segundo tipo de evaluación de riesgos que se debería realizar es evaluar el riesgo en conjunto para el negocio una vez que un desastre golpea. Esto incluye el riesgo para la entrega de los productos o servicios de una organización en la cadena de suministro, así como el impacto en sus clientes y otras partes interesadas.

3.1 Riesgo del desastre

El riesgo de que ocurra un desastre debería ser evaluado por una organización para estar preparada en caso de que ocurran los desastres. La evaluación debería tener en cuenta la probabilidad del desastre, el potencial de ocurrencia y la gravedad de su impacto.

La evaluación del riesgo debería comenzar determinando la probabilidad de que ocurra un desastre en el sitio. Esto incluye identificar los tipos de desastres que el sitio puede encontrar con mayor probabilidad. Después de hacer una lista de todos los posibles desastres, el siguiente paso sería determinar el potencial para que ocurran.

Hay muchos recursos que pueden ayudar a identificar los tipos de desastres que pueden ocurrir, así como el potencial para que ocurran. Estos recursos incluyen sitios web nacionales y gubernamentales que publican el historial de diferentes tipos de desastres en todo el mundo. La aseguradora que cubre una organización para los daños a la propiedad también puede ser capaz de proporcionar algunas estadísticas útiles.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Otros factores que pueden jugar un papel en la evaluación del riesgo pueden incluir, pero no se limitan a, el diseño y la ubicación de la instalación y el tipo y la cantidad de materiales almacenados dentro de la misma. Aunque estos factores pueden no conducir a un desastre, pueden magnificar su efecto. Por ejemplo, si la organización tiene muchos materiales combustibles, puede intensificar los incendios. Además, el derrame de productos químicos peligrosos o biológicos puede crear riesgos adicionales para la contención.

Después de que se hayan identificado los tipos y el potencial de un desastre determinado, se puede desarrollar e implementar un plan de respuesta en caso de que ocurra un desastre natural.

3.2 Riesgo para el negocio

La siguiente evaluación de riesgos deberá consistir en valorar el efecto de disminuir el flujo de sus productos o servicios en el suministro a sus clientes u otras partes interesadas. Esta evaluación debería incluir, pero no se limita a, la evaluación de la comunicación, infraestructura, servicios públicos, problemas de transporte y el deterioro del producto. Otros riesgos potenciales que deberían evaluarse pueden incluir evaluar la capacidad de su proveedor para entregar materiales, así como la capacidad de proporcionar servicios para reparar las instalaciones dañadas. También puede existir riesgo financiero para el negocio debido a pérdidas de ingresos o pérdida de buena voluntad.

Otro riesgo que necesita ser evaluado consiste en valorar el riesgo para el cliente cuando hay una interrupción en la prestación de productos o servicios. La criticidad de los productos o servicios de una organización tendrá un impacto sustancial en la evaluación final del riesgo empresarial.

Las empresas multinacionales pueden optar por crear un programa estándar de evaluación de riesgos para simplificar la comprensión global de los diferentes riesgos que enfrentan en sus negocios.

Una vez realizadas las evaluaciones de riesgo de un desastre y el riesgo para el negocio, la organización puede desarrollar el plan de respuesta al desastre y el plan de contingencia del negocio para los riesgos potenciales asociados con los tipos de desastres para esa organización en particular. Cuanto más críticos sean los productos y servicios, será más necesario que se ponga en marcha una estrategia para mitigar el riesgo de mantener el negocio viable.

Sección 4: Preparación del plan de respuesta al desastre

Un plan preestablecido de respuesta ante desastres permitirá a su organización, y a los recursos internos y externos, enfocarse inmediatamente en el tratamiento de las secuelas del desastre. El

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

plan de desastre debería incluir garantizar la seguridad de su personal, garantizar que se sigan los procedimientos de evacuación, proporcionar los esfuerzos iniciales de respuesta al desastre, iniciar el control de daños requerido y preparar el centro de comando del plan de contingencia.

4.1 Implementación del centro de comando de desastres

Es importante para una organización establecer un Centro de Comando de Desastres (DCC, por sus siglas en inglés), el cual llevará a cabo los principios de preparación y gestión ante desastres, que funciona a un nivel estratégico durante un desastre y asegura la continuidad de las operaciones de la organización. El centro de comando de desastres debería estar localizado en las proximidades del desastre.

Un Centro de Comando de Emergencia (ECC, por sus siglas en inglés, *Emergency Command Center*) debería estar ubicado cerca de la organización y ser responsable de la dirección estratégica y las decisiones operativas. Normalmente no controla directamente los activos de campo, en lugar de eso, se encarga de las decisiones tácticas. Las funciones comunes de los ECC es coleccionar, recopilar y analizar los datos; tomar decisiones que protejan la vida y la propiedad, mantener la continuidad de la organización, dentro del ámbito de las leyes aplicables; y difundir esas decisiones a todos los organismos y particulares interesados.

4.2 Respuesta del personal al desastre

Seguridad y protección del personal

En el caso de un desastre, es importante que el personal en el sitio, ante todo, encuentre protección en un lugar seguro. El personal debería tener áreas designadas para protegerse dependiendo de dónde impacte el desastre natural al sitio y sus funciones asignadas. Una vez que el personal está protegido, el proceso de responsabilidad y comunicación puede llevarse a cabo.

Responsabilidad

La responsabilidad del personal es un esfuerzo de los brigadistas de desastres por mejorar la protección al personal, al hacer un seguimiento de sus ubicaciones y tareas cuando se opera en un sitio de incidentes. La implementación oportuna de los procesos de responsabilidad del personal no permite un “período independiente” cuando los brigadistas actúan independientemente de la supervisión. La responsabilidad del personal también facilita la rápida actuación de los brigadistas en la identificación y evacuación de personal lesionado o incapacitado en entornos peligrosos.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Atención médica

En caso de un desastre es importante proporcionar atención médica al personal que se ve afectado. Es imperativo disponer de los protocolos necesarios para garantizar una comunicación inmediata y adecuada que proporcione atención médica al personal. Las herramientas de respuesta ante desastres, que se abordan en la sección 6.3, contienen artículos que ayudarán a proporcionar atención médica al personal lesionado.

Necesidades básicas

Después de abordar las preocupaciones médicas y de protección, es importante atender las necesidades básicas del personal. Esto puede incluir ropa, refugio y comida. Cada sitio debería abordar cuáles podrían ser las necesidades básicas potenciales en caso de un desastre.

Plan de comunicación de crisis

Comunicación

Cuando ocurre un desastre, la necesidad de comunicarlo es inmediata y crítica. Dependiendo de la gravedad del desastre, una organización debe ser capaz de comunicarse con el personal, las familias, los clientes, la comunidad y los agentes reguladores. El personal y sus familias se preocuparán y querrán información. Si las operaciones de negocio se interrumpen, los clientes querrán saber cómo se verán afectados. Los vecinos que viven cerca de la instalación pueden necesitar información, especialmente si están amenazados por el desastre. Es posible que sea necesario notificar a los agentes reguladores, y los funcionarios del gobierno local querrán saber qué está sucediendo en su comunidad. Toda esta "audiencia" querrá información antes de que el negocio tenga la oportunidad de comenzar a comunicarse.

Un componente importante del programa de preparación es el plan de comunicación de crisis. Un negocio debe ser capaz de responder con prontitud, precisión y confianza durante un desastre en las horas y días siguientes. Se debe llegar a muchas audiencias diferentes con información específica de su interés y necesidad. La percepción pública de cómo una organización maneja un incidente puede impactar positiva o negativamente en la imagen del negocio. Por lo tanto, es importante tener un procedimiento en vigor con el que se pueda comunicar el estado de la instalación y el personal a estos públicos. El plan de comunicación de crisis detallará las comunicaciones entre el centro de comando de emergencia, el centro de comando de desastres, el personal local y el de emergencia.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Información de contacto

La información de contacto de cada audiencia debe compilarse antes de un desastre y ser inmediatamente accesible durante un incidente. La información existente para clientes, proveedores y personal puede ser exportable a partir de bases de datos existentes. Incluya tanta información para cada contacto como sea posible (por ejemplo, nombre de la organización, nombre del contacto, número de teléfono de la empresa, número celular, número de fax y dirección de correo electrónico).

Además de tener información del contacto, es importante tener métodos de comunicación en función de la gravedad del desastre. La información puede ser comunicada a estos públicos a través de un sistema telefónico satelital. En casos como este, debería haber una persona designada (equipo) encargada de las comunicaciones.

Administración

La administración siempre debería ser notificada sin importar la situación. Se deberían entender y documentar claramente los protocolos de cuándo se debe notificar a la gerencia.

Gobierno y respuesta ante desastres

Dependiendo de la gravedad del desastre, los protocolos deben estar implementados para comunicar el estado de los daños a los agentes reguladores. Se debería designar a una persona responsable por si surge el evento.

Personal, víctimas y sus familias

Recursos Humanos (RR. HH.) es responsable de las comunicaciones diarias con el personal con respecto a asuntos de empleo y administración de beneficios. La gestión de recursos humanos debería asumir un papel similar en el equipo de comunicación de crisis. RR. HH. debería coordinar las comunicaciones con la gerencia, los supervisores, el personal y las familias.

La comunidad

Si hay peligros en una instalación, que podrían afectar a la comunidad cercana, entonces la comunidad se convierte en una audiencia importante. Si es así, la información a la comunidad debería ser parte del plan de comunicaciones de crisis.

- Desarrolle una política de la organización en la que solo los portavoces autorizados puedan hablar con los medios de comunicación en nombre de la organización. Comunique la política regularmente a todo el personal, explicando que es una buena práctica comunicarse a través de una sola voz informada.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

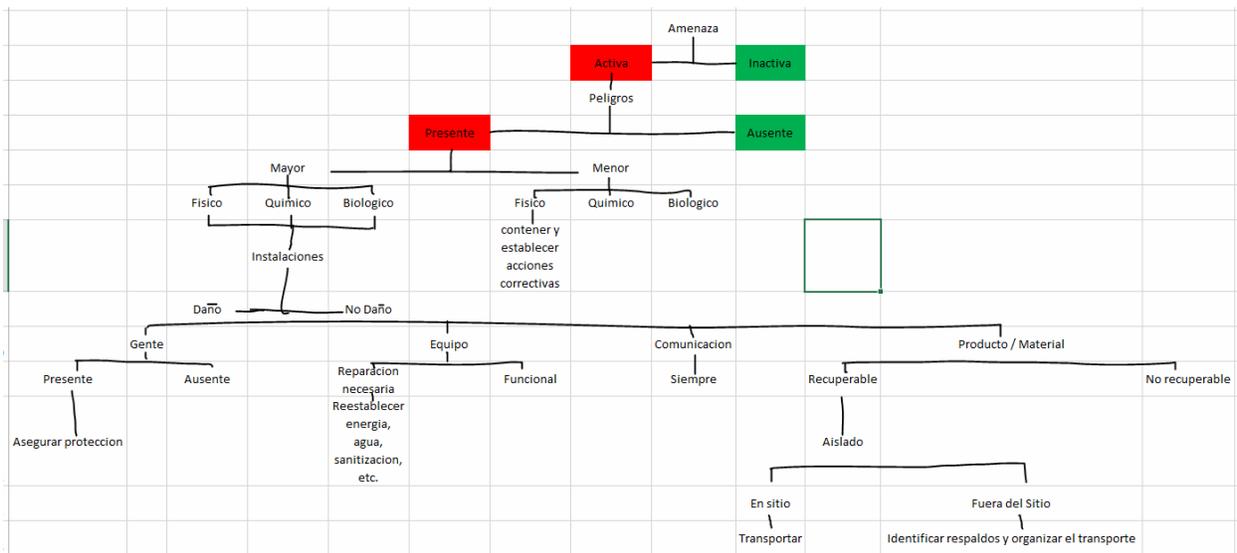
- Un elemento importante del plan de comunicación de crisis es la necesidad de coordinar la divulgación de información.
- Otro objetivo fundamental del plan de comunicaciones de crisis es pasar de reaccionar al incidente, a administrar una estrategia, y finalmente, a superar el incidente. La gerencia necesita desarrollar la estrategia y el equipo de comunicaciones de crisis necesita implementar esa estrategia, aliviando las preocupaciones de cada audiencia y posicionando a la organización para que emerja del incidente con su reputación intacta.

Contacto y centros de información

La comunicación antes, durante y después de un desastre es bidireccional. Las partes interesadas o el público harán preguntas y pedirán información. El negocio responderá preguntas y proporcionará información. Este flujo de información debería gestionarse a través de un centro de comunicaciones.

4.3 Respuesta de las instalaciones al desastre

El siguiente diagrama puede ser utilizado para evaluar las respuestas apropiadas cuando una instalación se ve afectada por un desastre natural. Estos factores deben evaluarse como parte del plan de respuesta ante desastres para garantizar la continuación de las operaciones.



La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

4.4 Respuesta de los productos y servicios al desastre

Los integrantes del equipo de planificación de contingencia de desastre evaluarán el impacto que tuvo el desastre en los productos o servicios en proceso y terminados. Se debe recopilar un inventario del producto y del estado del inventario. ¿El producto o los servicios se vieron afectados por daños? ¿Existen daños/riesgos potenciales adicionales? Si es así, ¿los planes y acciones deben iniciarse rápidamente para minimizar el posible daño/riesgo adicional? En esta fase temprana, puede ser prematuro evaluar con precisión la disposición futura del producto en distintas clasificaciones: producto no afectado, capacidad potencial de venta a través de esfuerzos de retrabajo y pérdida total del producto.

En los siguientes días, los esfuerzos y el personal pueden entonces pasar a la evaluación, inspección, segregación y reelaboración de cualquier producto afectado para la venta potencial. La urgencia de estas actividades dependerá de muchos factores, entre ellos el inventario de la cadena de suministro, la fuente del producto única o múltiple, la demanda por parte de los clientes y la infraestructura de la distribución.

Sección 5: Preparación del plan de continuidad del negocio

Un plan de continuidad del negocio garantiza la capacidad de una organización para continuar los procesos operativos críticos de negocio en el caso de una interrupción del negocio. La implementación efectiva del plan de continuidad del negocio es vital para proteger la marca y la reputación de la organización durante cualquier interrupción no planificada, proporcionando así un sentido de seguridad para sus clientes y otras partes interesadas.

Cuando se interrumpe el negocio, le puede costar ingresos y ventas a la organización. Un plan de continuidad del negocio es esencial. El desarrollo de un plan de continuidad del negocio incluye cuatro pasos:

Paso 1: Realizar un análisis de impacto empresarial para identificar funciones y procesos empresariales sensibles al tiempo o críticos y los recursos que los apoyan.

Paso 2: Identificar, documentar e implementar las funciones y procesos críticos del negocio.

Paso 3: Organizar un equipo de continuidad del negocio y compilar un plan para gestionar una interrupción del negocio.

Paso 4: Realizar capacitación para el equipo de continuidad del negocio, así como realizar pruebas y ejercicios para evaluar las estrategias de recuperación y el plan.

Paso 1: análisis de impacto empresarial

El análisis de impacto de continuidad del negocio identifica los efectos que resultan como consecuencia de la interrupción de las funciones y procesos del negocio. El análisis de impacto empresarial también utiliza información para tomar decisiones sobre la recuperación, las prioridades y las estrategias.

Esas funciones o procesos con el mayor potencial de impactos operacionales y financieros se convierten en prioridades para la restauración. El momento en que se debe recuperar una función o un proceso, antes de que se produzcan consecuencias inaceptables, a menudo se denomina "objetivo de tiempo de recuperación".

Paso 2: identificar las funciones críticas del negocio

Es importante identificar todas las funciones de negocio críticas que son necesarias para mantener la organización operativa. Esto incluye todas las operaciones que permiten la entrega continua de productos y servicios a clientes y otras partes interesadas, tales como, logística, cadena de suministro, recursos humanos, planificación y abastecimiento.

Este proceso implica evaluar la sustentabilidad de su producto o servicio para sus clientes u otras partes interesadas. ¿Es éste el único sitio que fabrica un producto en particular o proporciona un servicio en particular? Esto desempeñará un papel importante en el desarrollo de su plan de continuidad del negocio.

Paso 3: organizar el equipo de continuidad del negocio

El primer paso para identificar quién debe hacer parte del equipo de continuidad del negocio es determinar qué eventos potenciales deberá planear para el equipo. Se debe desarrollar un equipo de continuidad del negocio consistente con representantes de diferentes departamentos que puedan formular, a corto y a largo plazo, estrategias para garantizar la continuidad del negocio. El equipo debe desarrollar procesos y una estructura de comunicación para ser utilizados en caso de una interrupción. El equipo también debe determinar las personas y los proveedores necesarios para administrar la recuperación técnica.

Los miembros de los equipos pueden incluir, pero no se limitan a:

- Patrocinador Ejecutivo.
- Comité Directivo de la Gestión de la Continuidad del Negocio.
- Gerente de continuidad del negocio.
- Proveedores clave y/o socios minoristas.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

- Equipos de recuperación específicos del Departamento:
 - Gestión de riesgos.
 - Servicio al cliente.
 - Gestión de instalaciones.
 - Comunicaciones internas/externas.
 - Fabricación/producción.
 - Tecnología de la información.
 - Recursos humanos.
 - Operaciones/logística.

Otras consideraciones para desarrollar una estrategia de recuperación deben incluir lo siguiente:

- Determinar la fuente para el respaldo de los recursos técnicos (PC, servidores, impresoras).
- Documentar los datos críticos que se restaurarán y hacer una copia de todos los datos fuera del sitio.
- Las herramientas esenciales para la gestión de continuidad virtual incluyen sistemas de notificación y comunicaciones inteligentes, además de una solución basada en la red para el seguimiento y la gestión de incidentes, que permita a todos los miembros del equipo tener una imagen operativa común del incidente a medida que se desarrolla y acceso a los archivos, planes y plantillas que necesiten para ejecutar sus tareas asignadas.

Paso 4: entrenamiento y evaluación de continuidad del negocio

La formación del personal es esencial para garantizar que todos sepan qué hacer cuando hay un desastre, o una interrupción en las operaciones comerciales. Todos necesitan capacitación para familiarizarse con las acciones seguras para la protección de la vida (por ejemplo, evacuación, refugio, amparo en el lugar y resguardo). Revise las acciones seguras para la protección de la vida y realice simulacros de evacuación ("simulacros de incendios") según lo requiera la normativa local. También deben llevarse a cabo simulacros de refugio y de resguardo. El personal debería recibir capacitación para familiarizarse con los programas de protección, seguridad de la construcción, seguridad de la información y otros programas de prevención de pérdidas.

Los miembros de los equipos de respuesta a desastres, continuidad de negocios y comunicaciones de crisis deben estar capacitados y familiarizados con su función y responsabilidades, tal como se definen en los planes. Los líderes de equipo deben recibir un nivel más alto de capacitación, incluyendo capacitación del sistema de comandos de incidentes, para que puedan liderar a sus equipos. Revise las regulaciones aplicables para determinar los

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

requisitos de capacitación. Se deberían mantener los registros del alcance de la capacitación, los participantes, el instructor y la duración.

Se deben realizar pruebas y ejercicios para evaluar la efectividad de su programa de preparación, asegurarse de que el personal sabe qué hacer y dónde encontrar las partes que faltan. Hay muchos beneficios en las pruebas y los ejercicios:

- Capacitar al personal; aclarar las funciones y responsabilidades.
- Reforzar el conocimiento de los procedimientos, instalaciones, sistemas y equipos.
- Mejorar el rendimiento individual, así como la coordinación organizacional y las comunicaciones.
- Evaluar políticas, planes, procedimientos y los conocimientos y habilidades de los miembros del equipo.
- Revelar debilidades y brechas de recursos.
- Cumplir con las leyes, códigos y regulaciones locales.
- Obtener reconocimiento por el programa de gestión de desastres y continuidad del negocio.

Sección 6: Ejecución de los planes preparados

Cuando el desastre afecta a su organización, el sitio debe activar inmediatamente los planes preparados preestablecidos y al equipo del centro de comando de desastre del sitio. Los esfuerzos de respuesta inmediatos, organizados y enfocados permitirán, al equipo de gestión del sitio y al personal, lidiar con situaciones peligrosas y minimizar el pánico y el trauma.

6.1 Activación del equipo del centro de comando de desastres

Inmediatamente después del inicio de una crisis, el equipo del centro de comando de desastres se activará para ejecutar el plan preparado establecido. El equipo de gestión de crisis será responsable de gestionar al personal para estar mejor equipados en tal situación.

6.2 Acceso al plan/ubicación del plan

Es fundamental tener varias copias impresas del plan de contingencia de desastre en varios lugares y con miembros del equipo de crisis en caso de que no se pueda acceder a los sistemas electrónicos. Parte del plan debería incluir la disponibilidad de listas de contactos para los recursos internos y externos. También se recomienda tener copias impresas de los

procedimientos organizacionales de recuperación de desastres del sitio a los que se pueda acceder.

6.3 Botiquín para la respuesta ante desastres

Las organizaciones deberían tener preparados varios botiquines de respuesta ante desastres que se puedan desplegar inmediatamente para administrar cuidado al personal impactado y/o miembros de la familia, como respuesta antes de que los servicios locales (médicos, bomberos, instituciones) puedan proporcionar asistencia a su sitio.

Las organizaciones deben evaluar las instalaciones circundantes, los usos y el diseño para detectar daños y riesgos. La principal prioridad es proteger a su personal ante situaciones peligrosas y potencialmente peligrosas (incendio, explosión, colapso, etc.). La construcción y las operaciones deberían ser contenidas y consideradas seguras antes de permitir la entrada rutinaria a las áreas. Una vez que la instalación y el área circundante estén estables, la organización debería asegurar el edificio, producto y/o servicios para limitar futuras pérdidas.

Dado que las organizaciones no saben cuándo ocurrirá un desastre o el impacto que un desastre puede tener en un sitio, se recomienda que las mismas tengan varios botiquines de respuesta ante desastres colocados estratégicamente en varios lugares a lo largo de la instalación en caso de que cualquiera de los botiquines de respuesta a desastres no esté accesible durante el desastre. Asegúrese de que todo el personal conozca la ubicación de los botiquines de respuesta ante desastres.

Los siguientes son elementos que deberían considerarse como parte de los botiquines de respuesta ante desastres de su sitio:

Agua embotellada estéril	Guantes sin látex	Radios de dos vías	Gafas / lentes de seguridad
Linternas y baterías	Bolsas para desechos infecciosos	Teléfonos celulares satelitales con Wi-Fi	Hacha
Kit de limpieza de derrames	Botiquín de primeros auxilios que incluye desfibrilador, vendas, apósitos de compresión, cinta adhesiva, ungüentos tópicos, compresas de gasa y rollos, parches oculares, tijeras	Cinta adhesiva	Kits de herramientas
Compresas de hielo	Mantas solares	Bengalas	Cinta de precaución
Desinfectante de manos	Toallitas desinfectantes	Radio solar	Cuchillos utilitarios

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

A lo largo del año, revise el contenido del botiquín de respuesta ante desastres y reemplace los elementos caducados según sea necesario. También se recomienda volver a evaluar el contenido del botiquín de respuesta ante desastres después de cada simulacro planeado en su sitio.

6.4 Comunicaciones

Las organizaciones deberían tener un plan preestablecido sobre cómo informar al personal y cómo proporcionar actualizaciones y comunicados. Este es un componente del plan de comunicación de crisis. Los objetivos durante un desastre son informar, proteger y asegurarse de que el personal se mantenga informado para que la organización pueda sobrevivir. Es mejor comunicar más que permitir que el pánico, el miedo y los rumores llenen el vacío de comunicaciones inapropiadas y menos frecuentes.

El punto de comunicación local debería coordinarse a través del equipo de gestión de crisis en el sitio de comando local. El equipo debería predefinir quién estará proporcionando las comunicaciones al personal, la frecuencia en la que se van a recibir y en el caso de que los modos de comunicación tradicionales no estén disponibles, ¿cuál es el plan para obtener comunicaciones periódicas con el personal?

6.5 Lista de verificación del plan de desastres

Una copia de la lista de personal del sitio debe ser parte del kit de respuesta a desastres. Dicha lista debe incluir números de teléfono celular, direcciones e información de contacto de un miembro de la familia. El equipo de gestión de crisis debe gestionar la responsabilidad de todos los miembros del personal.

Como parte del plan de contingencia por desastre, los sitios pueden desarrollar una lista de verificación predefinida para cosas como la seguridad de las instalaciones, el acceso a las provisiones básicas, las utilidades/infraestructura, la cadena de suministro, los sistemas informáticos, la lista de contacto ante un desastre (interna y externa).

Una parte del plan para desastres puede considerar cómo su personal obtendrá acceso y transporte al sitio en caso de un desastre catastrófico que incluya el uso compartido del automóvil, la guardería en el lugar, el horario flexible, etc. Evalúe la posibilidad del trabajo de forma remota si el edificio/transporte no está disponible.

6.6 Formación profesional

La realización de capacitaciones sobre el plan de contingencia de desastre antes de un evento es un componente crítico para que todos los planes ejecutados sean eficientes. Asegurarse de que las personas sean conscientes de sus roles y responsabilidades en el sitio es importante para permitir el despliegue inmediato de su equipo de crisis. Se sugiere realizar una capacitación

regular en gestión de crisis para el Equipo de Gestión de Crisis, que incluya llevar a cabo simulacros anuales de crisis y de práctica del procedimiento de evacuación.

Como parte del plan de contingencia ante desastres, los sitios pueden desarrollar una lista de verificación predefinida para aspectos como la seguridad de las instalaciones, el acceso a las disposiciones de necesidades básicas, servicios públicos/infraestructura, cadena de suministro, sistemas de información, lista de contactos ante un desastre (internos y externos). La capacitación en recuperación ante desastres debe ser parte de la capacitación de ingreso de cada nuevo personal.

Sección 7: Ejecución del plan para la continuidad del negocio (PCN)

Una vez que un desastre impacta a una organización, la principal prioridad es promulgar el plan de respuesta ante desastres para la seguridad del personal y las instalaciones donde ocurrió el desastre. Es igualmente importante iniciar el plan de continuidad comercial para minimizar la interrupción de productos o servicios para sus clientes y otras partes interesadas.

Existen varias acciones relacionadas con la ejecución del plan para la continuidad del negocio

- Asegurarse de que la alta gerencia y los dueños corporativos del PCN sean notificados del desastre tan pronto como sea posible.
- Garantizar que se haya iniciado el plan de respuesta ante desastres para la instalación afectada.
- Comunicar a todos los miembros del equipo del PCN que ha acontecido un desastre y que se debe iniciar el PCN.
- Asegurarse de que el equipo del PCN está informado del progreso de las medidas de respuesta ante el desastre para la toma de decisiones relacionadas con el PCN.
- Una vez iniciado el PCN, crear comunicaciones internas y externas para informar al personal, los clientes y otras partes interesadas.
- Finalmente, es importante recopilar sistemáticamente información crítica para la implementación del PCN y ajustar la respuesta según sea necesario para minimizar el impacto en las operaciones empresariales.

Los equipos paralelos o separados también deben centrarse en el reinicio de las operaciones para ofrecer productos y servicios a sus clientes u otras partes interesadas. Este equipo creará la lista de reparaciones, actividades, etc. que deben completarse antes de que la organización pueda regresar a la operación completa. Estos pasos también deben considerar cualquier impacto o necesidad de recalificación y/o actividades de validación y el impacto en los plazos de operación.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.

Sección 8: Evaluación post mortem

8.1 Reunión informativa del plan de recuperación

Evalúe los eventos que se llevaron a cabo, incluidos los planes de mitigación y la acción por parte del personal, para determinar si se implementaron los planes y procedimientos apropiados, y si se siguieron, qué tan efectivos fueron en la mitigación del incidente.

8.2 Encuesta al personal y a las partes interesadas en las acciones de respuesta

Comenzar con la detección del incidente; se debe obtener de múltiples fuentes la mayor cantidad de información posible sobre el incidente. Una lista de verificación de la información que se recopilará y revisará de cada participante ayuda al proceso.

8.3 Evaluación

Aspectos a considerar durante la evaluación:

- ¿Se siguió la respuesta planeada ante el desastre?
- ¿Fue lo suficientemente flexible para hacer frente a eventos inesperados?
- ¿La respuesta fue efectiva y rápida?
- Revisar los resultados de la encuesta, identificar las fortalezas en cada área, evaluar los recursos movilizados, la planificación de recursos empresariales (ERP, por sus siglas en inglés, *Enterprise Resource Planning*) y los procedimientos relacionados, incluidos los procedimientos de capacitación.

8.4 Documentación de todas las actividades y actualizaciones al plan de contingencia existente basado en comentarios *

Se deben documentar los siguientes elementos:

- Basándose en la evaluación, documente todas las actividades y considere la actualización del plan de contingencia existente.
- ¿Qué cambios habrían sido útiles?
- Fortalezas identificadas, áreas que necesitan mejoras y recomendaciones para cumplir mejor los objetivos del plan.

- Realice un seguimiento de los cambios en el plan de contingencia e incluya la justificación de esos cambios.

* Tenga en cuenta que esto no es todo, le corresponde al personal en el sitio desarrollar una lista completa y comprensiva de preguntas y evaluaciones.

Sección 9: Conclusión

En nuestra vida cotidiana nadie espera que ocurra un accidente, pero tomamos medidas para minimizarlos. Ir a un chequeo médico, inspeccionar su auto o hacer una prueba de burbuja en los tanques de propano de su parrilla de barbacoa son ejemplos de pasos para minimizar la ocurrencia de un evento negativo. En las operaciones comerciales, y especialmente en la industria de productos y servicios médicos, la preparación para un evento potencialmente negativo puede ser fundamental, no solo para la empresa, sino también para el usuario final que también puede ser un paciente.

El primer paso para estar preparado es comprender los desastres que pueden afectar a una organización. El siguiente paso sería entender completamente cómo esto puede afectar el negocio. Después de comprender los riesgos relacionados, la organización puede preparar tanto su plan de respuesta ante desastres como su plan de continuidad comercial.

El propósito de un Plan de Respuesta ante Desastres es establecer una estructura organizativa y acciones para responder ante desastres. Así mismo, asignar los roles y responsabilidades para la implementación del plan durante un desastre.

Si bien el plan de continuidad comercial está directamente relacionado con el plan de respuesta a desastres, un plan de continuidad empresarial es un plan para ayudar a garantizar que los procesos comerciales puedan continuar durante un desastre. Esto incluye ser capaz de entregar productos y servicios que pueden ser críticos para sus clientes.

La evaluación de riesgos y el desarrollo de planes de continuidad de negocios y desastres son solo los primeros pasos. Los planes de preparación deben implementarse en su totalidad con los suministros, materiales o ajustes necesarios o cambios en los procesos o instalaciones existentes. El personal debe recibir capacitación sobre los planes para que pueda ejecutarse de manera efectiva en tiempos de crisis. Esto debería incluir la auditoría de los planes de efectividad y relevancia.



Al igual que con cualquier proyecto, debería existir una evaluación de las lecciones aprendidas y cómo se puede mejorar el programa. Un plan de recuperación de desastres adecuado debe ayudar a garantizar las siguientes consideraciones críticas para el negocio:

- Seguridad, protección y bienestar de las personas.
- Seguridad del producto.
- Suministro de productos.
- Capacidades de infraestructura crítica.
- Responsabilidades financieras/de la tesorería.
- Cumplimiento/Protección de la Propiedad Intelectual.

Finalmente, ninguna organización quiere ser víctima de un desastre, sin embargo, la cantidad de recursos utilizados para preparar y armar un plan de respuesta ante desastres puede ahorrar gastos innecesarios si la organización está adecuadamente preparada para ello.

Apéndice 1: Recursos/enlaces

Sitio	Enlaces
<p><i>Business Continuity Overview for the Biotechnology, Pharmaceutical and Life Sciences Cluster</i></p> <p>Generalidades de la continuidad del negocio para el grupo de biotecnología, farmacéuticas y ciencias de la vida</p>	<p>https://www.eda.gov/files/about/disaster-recovery/biotechnology-pharm-life-sciences.pdf</p>
<p><i>Business as Usual. No Matter What.</i></p> <p>El negocio como siempre. Sin importar nada.</p>	<p>http://www.preparemybusiness.org/</p>
<p><i>SBA Disaster Planning</i></p> <p>Administración de Pequeños Negocios: Planeación para desastres</p>	<p>http://www.sba.gov/content/disaster-planning</p>
<p><i>Federal Disaster Management Agency (FEMA)</i></p> <p>Agencia Federal para la Gestión de Emergencias</p>	<p>http://www.ready.gov/business</p>
<p><i>American Red Cross</i></p> <p>Cruz Roja de EE. UU.</p>	<p>http://www.readyrating.org/</p>
<p><i>Institute for Business and Home Security</i></p> <p>Instituto para la Seguridad Empresarial y del Hogar</p>	<p>http://www.ibhs.org/</p>
<p><i>Ready: Risk Assessment</i></p> <p>Evaluación del riesgo</p>	<p>https://www.ready.gov/risk-assessment</p>
<p><i>Federal Disaster Management Agency (FEMA)</i></p> <p>Agencia Federal para la Gestión de Emergencias</p>	<p>“Every Business should have a plan” (PDF)</p>
<p><i>Readiness Best Practices: Assembling Your Business Continuity Team</i></p> <p>Mejores prácticas de preparación: conformación del equipo de continuidad de su negocio.</p>	<p>https://www.missionmode.com/readiness-best-practices-assembling-business-continuity-team/</p>
<p><i>Business Continuity Template</i></p> <p>Plantilla de continuidad del negocio</p>	<p> BCP Template 2012(1).docx</p>
<p><i>Center for Disease Control (CDC)</i></p> <p>Centro para el control de enfermedades</p>	<p> Emergency Action Plan Template.doc</p>
<p><i>Ready: Crisis Communications Plan</i></p> <p>Plan de Comunicaciones de Crisis</p>	<p>https://www.ready.gov/business/implementation/crisis</p>

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.



Apéndice 2: Lista de verificación de desastres 1

Riesgo	Acción protectora potencial
Denegación de acceso a las instalaciones	<ul style="list-style-type: none">• Actualice continuamente el estado de los sitios en redes sociales, el sitio web y la prensa para que los clientes y el personal conozcan el estado actual y los planes para escapar o encontrar espacio temporal si es necesario.• Trabaje con la administración local de desastres para participar en cualquier programa de reingreso disponible.
Pérdida crítica de capacidad del proveedor para completar pedidos	<ul style="list-style-type: none">• Conforme listas electrónicas y de copia impresa de contactos de proveedores alternativos (y competidores).• Establezca contratos de contingencia con proveedores alternativos en lugares separados.
Denegación de acceso a los sistemas de información clave (p. ej. sistemas informáticos, bases de datos)	<ul style="list-style-type: none">• Disponga un respaldo robusto de los datos de los sistemas de información clave y las bases de datos fuera del sitio.• Adquiera métodos de comunicación alternativos para respaldar los requisitos tecnológicos y de transacción.• Integre el acceso remoto en las operaciones siempre que sea posible. La capacidad del personal para trabajar desde casa podría disminuir los problemas de personal durante/después de un desastre.• Utilice la tecnología de la nube para almacenar datos críticos de forma remota.
Ausencia de comunicación para proveedores y suministradores	<ul style="list-style-type: none">• Mantenga actualizado el estado de las empresas en las redes sociales y en el sitio web del negocio; informe a los proveedores y clientes que el negocio sobrevivió al evento. Comuníquese vía correo electrónico.• Contacte a los clientes actuales a través de ráfagas de correo electrónico y llamadas de cortesía (si es posible). Si la



	<p>ubicación ya no es accesible, busque una ubicación temporal cercana y publique la nueva dirección.</p> <ul style="list-style-type: none">• Considere el uso de más de un proveedor de telefonía, en ubicaciones separadas• Los servicios redundantes múltiples y especialmente la proximidad de los proveedores al área son críticos para este grupo.
Vandalismo y/o robo	<ul style="list-style-type: none">• Desarrolle planes con las autoridades locales y la gestión de desastres para mantener la seguridad durante una ausencia prolongada.• Invierta en equipos de seguridad y vigilancia de acceso remoto.
Daño físico	<ul style="list-style-type: none">• Desarrolle listas de contactos de contratistas de construcción, techadores, plomeros, propietarios, administradores de edificios, etc. que puedan responder de manera confiable a daños físicos.
Interrupción de las operaciones de los clientes.	<ul style="list-style-type: none">• Desarrolle listas de contactos de contratistas de construcción, techadores, plomeros, propietarios, administradores de edificios, etc. que puedan responder de manera confiable a daños físicos.

Apéndice 3: Lista de verificación de desastres 2

1. Confirme los roles y las responsabilidades de todos.
El equipo de crisis determina si se añaden más o nuevos especialistas internos o externos
2. ¿Qué ha pasado y que hechos han sido confirmados?
Recopile los hechos confirmados acerca de la situación. Los hechos ayudan a decidir qué curso tomar.
3. ¿Qué suposiciones pueden hacerse en relación con el incidente o la situación?
Recopile las suposiciones hechas hasta ahora en relación a la situación. Asegúrese que estas suposiciones sean examinadas (¡punto de acción!) y puedan ser descartadas o sean el hecho del caso.
4. Prepare el peor escenario y el más probable (individualmente) y asegúrese de no olvidar nada.
Maneje estos escenarios en una junta informativa y repítase esta pregunta ¿Qué puntos de acción se tienen que observar si el escenario sucede?
5. Establezca las prioridades (Incluyendo las necesidades del equipo local de manejo de crisis para la información e instrucciones necesarias y/o tareas para otros empleados).
Considere qué información es necesaria para tomar acciones. Considere si otras medidas son necesarias, las cuales tienen que ser tomadas ahora.
6. Considere la disponibilidad y opciones posibles. ¿Qué tiene que hacerse ahora y qué puede esperar?
Considere opciones de gestión de incidentes y escoja la mejor opción.
7. Establezca objetivos (ejemplo: regresar al negocio de manera usual).
Determine los indicadores que serán capaces de establecer si el resultado de lo seleccionado es exitoso.
8. Identifique a las partes interesadas involucradas y priorice de acuerdo a los intereses e influencia que pudieran tener.
Ejecute un análisis profundo de las partes interesadas y priorice de acuerdo con el interés e influencia de cada una de ellas.
9. Establezca si las partes interesadas deben ser informadas y determine la notificación adecuada.
Establezca declaraciones para las partes interesadas, incluyendo los métodos y tiempos de comunicación.
10. Revise este protocolo cada hora.
Determine el tiempo y la localización de la siguiente reunión. Revise todos los pasos sucedidos con base en cualquier información nueva que esté disponible.

Documento publicado en su versión original en inglés en octubre del 2018.

La información contenida en este documento se proporciona como un servicio a los miembros de Rx-360 y representantes de la industria con el entendimiento de que Rx-360 no hace ninguna garantía, ya sea expresada o implícita, con respecto a la exactitud, integridad, confiabilidad, o idoneidad de la información. Tampoco Rx-360 garantiza el uso de esta información como norma obligatoria.