GUÍA DE PRÁCTICAS RECOMENDADAS

posteriores a incidentes de agresores activos en el sector de fabricación crítica

JULIO DE 2024

Departamento de Seguridad Nacional de EE. UU. (U.S. Department of Homeland Security)
Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency)

ÍNDICE

DESCRIPCIÓN GENERAL

La Guía de prácticas recomendadas posteriores a incidentes de agresores activos en el sector de fabricación crítica (CM, por sus siglas en inglés) sirve como recurso para los esfuerzos de respuesta y recuperación posteriores a incidentes para el sector CM y sus socios. Planificar, preparar e implementar procesos esenciales de respuesta y recuperación son pasos cruciales ya que ayudan a todas las organizaciones de fabricación críticas y a sus filiales a permanecer resilientes ante cualquier incidente de agresor activo.

Un **agresor activo** es una persona que se dedica activamente a matar o intentar matar personas en un área poblada.[1] Estos agresores pueden atacar utilizando armas de fuego, tácticas de embestida con vehículos, bombas, dispositivos incendiarios, armas químicas, drones u otros métodos. Después de que una organización experimenta un incidente de agresor activo, debe tomar dos medidas igualmente importantes. La primera es la **respuesta inmediata**: las acciones iniciales tomadas por el personal después de un incidente para salvar vidas y minimizar los daños. Una vez tomadas estas medidas, comienza el siguiente paso, la **recuperación**, que incluye tanto la **recuperación a corto plazo**: restablecer la seguridad y mitigar las repercusiones físicas, psicológicas y emocionales en los días, las semanas y los meses posteriores al incidente, como la **recuperación a largo plazo**: ayudar a la organización a reanudar sus operaciones y ayudar a los afectados a volver a una sensación de normalidad en sus interacciones diarias y en su vida profesional; un proceso que probablemente llevará años. Tenga en cuenta que no existe una distinción clara entre estos pasos: la respuesta inmediata se extenderá a los días posteriores a un incidente, del mismo modo que la recuperación a corto plazo se extenderá a los meses siguientes.

Las medidas descritas en esta guía pueden variar drásticamente según el tipo de organización (p. ej., una oficina frente a una fábrica, un edificio de una sola empresa frente a una organización distribuida en varias ubicaciones o una empresa grande con recursos importantes frente a una empresa pequeña con personal limitado). El tamaño de una organización en particular incide en los esfuerzos de respuesta y recuperación después de un incidente. Por ejemplo, las pequeñas y medianas empresas pueden requerir que el equipo de liderazgo y un número limitado de empleados asuman múltiples funciones y responsabilidades con respecto a las que una organización más grande podría distribuir más ampliamente entre su personal. Las pequeñas y medianas empresas también carecen de los recursos de una organización más grande y es posible que deseen o necesiten externalizar algunos de los servicios mencionados en esta guía en lugar de depender de medidas y personal internos, desde servicios de tecnología de la información hasta responsabilidades legales. Para prepararse mejor para un incidente y garantizar la seguridad de la plantilla y la continuidad del negocio, una organización debe tener en cuenta los recursos disponibles, el personal, los edificios y la naturaleza de su operación.

Por encima de todo, una organización de fabricación crítica debe realizar estos preparativos mucho antes de que se produzca un incidente con un agresor activo. Sin una planificación adecuada, una correcta delegación de tareas, conexiones comunitarias y una comprensión de la amplia repercusión de un incidente con un agresor activo, es poco probable que la respuesta y la recuperación sean exitosas.

Descargo de responsabilidad: *La Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA, por sus siglas en inglés) no promociona a ninguna entidad comercial, producto, empresa o servicio, incluidas las entidades, los productos o los servicios vinculados en este documento. Cualquier referencia a entidades comerciales, productos, procesos o servicios específicos mediante marcas de servicio, marcas registradas, fabricantes, o de otro modo, no constituye ni implica la promoción, la recomendación ni la preferencia por parte de la CISA.*

1 Agencia de Seguridad de la Infraestructura y Ciberseguridad (CISA, por sus siglas en inglés), “Physical Security Performance Goals”, consultado el 12 de enero de 2024, https://www.cisa.gov/resources-tools/resources/physical-security-performance-goals-faith-based-communities.

PRIMERA PARTE: RESPUESTA INMEDIATA

La fase de **respuesta inmediata** se centra principalmente en las acciones inmediatas de una organización para salvar vidas, reducir los efectos en la salud física y mental, garantizar la seguridad pública y satisfacer las necesidades de las personas afectadas. Antes de empezar a pensar en recuperarse de un incidente, una empresa primero debe saber cómo responder de forma inicial al incidente en sí. Una respuesta eficaz, eficiente y oportuna depende de la adopción de medidas de preparación pensadas en los riesgos.

Los propietarios y operadores deben educar a la mayor cantidad posible de su personal sobre los procedimientos básicos para salvar vidas, como primeros auxilios y reanimación cardiopulmonar (CPR, por sus siglas en inglés), que pueden ser necesarios antes de que los servicios de emergencia lleguen al lugar de un incidente.[2] Sin embargo, navegar de forma eficaz por los pasos complejos y urgentes necesarios para una respuesta inmediata requiere un enfoque más organizado en toda la empresa, que incluya delinear y delegar las siguientes responsabilidades, comenzando desde la cima de la organización.

RESPONSABILIDADES DEL EQUIPO DIRECTIVO

El liderazgo de alto nivel, a menudo denominado ejecutivos del equipo directivo, desempeña un papel vital en el desarrollo, el compromiso y la interacción con las medidas de respuesta a incidentes de la organización. Ante una emergencia, los empleados buscan orientación en los líderes de la organización. Los ejecutivos deben participar y desempeñar un papel activo en la implementación de cualquier plan, curso de capacitación o medida de seguridad de la empresa. Deben liderar estos esfuerzos para el resto de su organización.

Si los ejecutivos no muestran interés o no están informados sobre los agresores activos u otros tipos de amenazas, será más probable que sus empleados adopten la misma mentalidad. Por el contrario, si los empleados observan que el equipo de liderazgo de alto nivel está comprometido a desarrollar e implementar un plan de acción de emergencia (EAP, por sus siglas en inglés) exhaustivo, es más probable que también se tomen en serio la amenaza. Si los líderes de la empresa entran en pánico o están indecisos ante un incidente, sus empleados pueden reaccionar de manera similar. Sin embargo, si el equipo de liderazgo muestra confianza, decisión, empatía y está informado durante un incidente y después de este, es más probable que sus empleados tomen la iniciativa y lleven a cabo medidas de respuesta a emergencias de manera eficiente.

El liderazgo de alto nivel debería participar de forma activa en la planificación y ejecución de estas medidas. Esta participación puede adoptar diversas formas, como dirigir o asignar cursos de capacitación periódicos sobre gestión de emergencias y primeros auxilios o compartir información de respuesta a incidentes a través de folletos, carteles u otras pautas accesibles dentro de sus instalaciones u oficinas.

RESPONSABILIDADES DE LA GESTIÓN DE EMERGENCIAS

El paso más importante que puede dar una organización para llevar a cabo una respuesta inmediata fluida, efectiva y eficiente es la creación de un EAP. Este debe ser un plan para toda la organización que involucre a todos los empleados (incluidos los ejecutivos del equipo directivo, como se señaló anteriormente). Ante un incidente con un agresor activo, todo el personal debe tener una función asignada que conozca y que pueda desempeñar con confianza para garantizar su propia seguridad y la del resto de la organización. Dependiendo del tamaño de la organización y sus recursos disponibles, este plan también involucrará servicios externos, como IT, Recursos Humanos (HR, por sus siglas en inglés) y personal de seguridad. Cada organización debe considerar su situación única al momento de elaborar el plan de respuesta inmediata.

Cada función y responsabilidad incluida en el EAP debe definirse claramente y delegarse a personas o equipos específicos entre el personal de la organización. Sin funciones claramente designadas, será poco probable o imposible que muchos empleados tomen las medidas adecuadas en caso de emergencia. Tenga en cuenta los diferentes horarios de los empleados, el acceso a diferentes pisos o áreas de las instalaciones y el dominio del inglés, oral y escrito, al asignar estas funciones. Si corresponde, involucre a los sindicatos de la organización al principio del proceso de planificación de emergencias; pueden ser recursos útiles para determinar planes específicos de las instalaciones, asignar funciones y garantizar que se atiendan las inquietudes del personal.[3]

---

2 Stop The Bleed®, "Get Trained!", consultado el 12 de julio de 2023, https://www.stopthebleed.org/training/; Agencia Federal para el Manejo de Emergencias (FEMA, por sus siglas en inglés), "You Are the Help Until Help Arrives", consultado el 12 de julio de 2023, https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US.

3 CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response*, 2019, https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide.

Al crear el EAP, los líderes de una organización, así como el director de Seguridad (o cualquier función equivalente que trate directamente con las autoridades y los servicios de emergencia), deben recibir capacitación en el Sistema Nacional de Gestión de Incidentes (NIMS, por sus siglas en inglés).[4] Otras herramientas federales para ayudar a las organizaciones a desarrollar planes integrales y personalizados de respuesta a la violencia incluyen el conjunto de herramientas de la Oficina para Víctimas de Delitos (Office for Victims of Crime),[5] la guía de preparación de la Agencia Federal para el Manejo de Emergencias (FEMA)[6] y la herramienta electrónica EAP de la Administración de Seguridad y Salud Ocupacional (OSHA, por sus siglas en inglés).[7] Los líderes de una organización deben conocer y dominar todos estos recursos. Deben revisar estos recursos de forma rutinaria (p. ej., anualmente) para revisar sus conocimientos y asegurarse de que su información esté actualizada.

Inmediatamente después de un incidente con un agresor activo, el EAP debe poner en marcha los siguientes procedimientos, que deben designarse, desarrollarse y ejercitarse con suficiente antelación a un incidente.

Sistema de notificación

La respuesta tras un incidente con un agresor activo debe comenzar con la notificación. El EAP debe establecer un sistema para notificar a todo el personal en el sitio sobre un incidente, incluido cuándo aconsejarles que evacuen el lugar o se refugien en algún sitio.[8] Las personas responsables de activar este sistema de notificación deben establecerse de antemano. La organización puede incluir mensajes predefinidos, que deben adaptarse a la situación en concreto.

Si corresponde, coordine con los sindicatos de la organización para garantizar que este sistema de notificación llegue a todos los empleados y que estos lo comprendan, incluidos aquellos con barreras lingüísticas o necesidades funcionales y de acceso, así como aquellos que se encuentren en zonas ruidosas, aisladas o cerradas de la instalación. También se debe enviar una notificación al personal que no está en el sitio (p. ej., trabajadores que están en una instalación diferente, que no están programados para trabajar ese día o que realizan algún trabajo fuera del sitio) para advertirles que eviten acercarse a la instalación debido a un incidente en curso.

Rutas de evacuación

Los líderes de una organización (p. ej., gerentes de planta, ejecutivos o supervisores, según el edificio en cuestión y la familiaridad del personal con su diseño) deben trazar rutas de evacuación antes de un incidente y garantizar que todo el personal esté familiarizado con ellas. Las rutas deben ser físicamente accesibles para los ocupantes con necesidades funcionales y de acceso. Esto incluye a todos los potenciales visitantes del sitio, además del personal existente. La organización debe publicar un mapa de estas rutas de evacuación en todo el edificio, conservar una copia en el EAP y actualizarlo según sea necesario.

Este plan debe incluir al menos dos rutas de evacuación, y el personal debe ponerlo en práctica de manera rutinaria (p. ej., anualmente) para tener en cuenta cualquier bloqueo, peligro, camino obstruido u otras barreras que puedan surgir durante un incidente con un agresor activo o inmediatamente después. Dependiendo de la naturaleza del ataque, las rutas de simulacros de incendio ya practicadas pueden no ser seguras o incluso no ser posibles de seguir, por lo que las rutas de contingencia deben estar predeterminadas. Las salidas no tradicionales, como ventanas y tejados, se pueden utilizar como rutas de evacuación si es necesario. Asegúrese de que el personal tenga los medios (p. ej., llaves, herramientas para romper cristales) para acceder a ellas.

Las rutas de evacuación de las organizaciones de fabricación crítica dependerán de la ubicación del edificio, la distribución y la naturaleza de la operación de fabricación. Al planificar rutas de evacuación, se debe abordar una serie de preguntas, como las siguientes:

- ¿El personal está en un entorno de oficina o en una planta destinada a la fabricación?
- ¿La empresa tiene una única ubicación o el personal está repartido en varios edificios?

---

4 FEMA, “National Incident Management System”, consultado el 13 de julio de 2023, https://www.fema.gov/emergency-managers/nims.

5 Centro de Asistencia Técnica y Capacitación de la Oficina para Víctimas de Delitos, “Mass Violence and Terrorism”, consultado el 13 de julio de 2023, https://www.ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv.

6 FEMA, *Are You Ready?,* actualizado en abril de 2023, https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf.

7 Administración de Seguridad y Salud Ocupacional (OSHA), “Emergency Action Plan”, consultado el 13 de julio de 2023, https://www.osha.gov/etools/evacuation-plans-procedures/eap.

8 Agencia Federal para el Manejo de Emergencias (FEMA), *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101*, septiembre de 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.

- ¿El edificio tiene un sistema de seguridad que deba ser considerado?
- ¿Hay maquinaria que deba apagarse antes de la evacuación?
    - Si la maquinaria debe apagarse o desactivarse antes de la evacuación, asegúrese de que el personal (p. ej., trabajadores individuales de la fábrica, gerentes de planta u otro personal relevante, según el diseño de la organización) pueda hacerlo de manera rápida, eficiente y sin temor a repercusiones por operaciones interrumpidas. Sin embargo, asegúrese de que el personal comprenda que su seguridad es la principal prioridad de la organización; si el equipo de fabricación no puede desactivarse a tiempo, se debe proceder a la ruta de evacuación lo más rápido posible.

Si una organización no está segura de cómo planificar rutas de evacuación para su edificio, puede comunicarse con las autoridades locales, quienes podrían visitar las instalaciones y ayudar a planificar las mejores rutas.

Además de establecer rutas de evacuación, asegúrese de que el personal conozca las siguientes prácticas de evacuación recomendadas:

- Deje sus pertenencias.
- Levante las manos en el aire para indicar a las autoridades que está desarmado.
- Evite escaleras mecánicas y ascensores.
- Lleve a otros con usted, pero no se quede atrás porque otros se nieguen a irse.
- Llame al 911 tan pronto como sea seguro hacerlo.

Cuando llame al 911, proporcione la mayor cantidad posible de la siguiente información a los operadores:

- *Ubicación del incidente, incluida la dirección, el número del edificio, el piso y cualquier otra información necesaria (p. ej., Sala 123, muelle de carga 4).*
- *Ubicación de la persona que llama.*
- *Ubicación del agresor activo (y la cantidad, si es más de uno).*
- *Presencia de autoridades o personal de seguridad en el sitio, si lo sabe.*
- *Descripción física de los atacantes, si los conoce.*
- *Tipo y número de armas utilizadas por los atacantes, si lo sabe.*
- *Uso o amenaza de explosivos/dispositivos explosivos improvisados (IED, por sus siglas en inglés).*
- *Si el ataque continúa ocurriendo.*
- *Número de víctimas potenciales en el lugar.*

Cuando la evacuación no es posible debido a la ubicación del agresor o al daño resultante, el personal debe conocer las áreas de refugio seguras dentro de las instalaciones; lo ideal es que tengan una puerta con cerradura y que ofrezcan el mayor grado posible de ocultamiento y cobertura. El personal que se refugie en un área segura de las instalaciones debe permanecer en el lugar hasta que los servicios de emergencia les informen que es seguro moverse.

Grupos de control

Al evacuar, el objetivo más importante es que el personal salga lo más rápido posible. En la práctica, esto significa que muchas personas pueden salir del edificio por múltiples salidas, lo que dificulta la reunión después de una evacuación y la contabilización del personal desaparecido. El EAP debe designar cierto personal (p. ej., gerentes de planta, instalación o área) a un grupo de control para realizar un seguimiento del personal después de una evacuación. El control es el proceso mediante el cual una organización determina el estado y la ubicación del personal. Este proceso también incluye ayudar a las autoridades y a los servicios médicos de emergencia en la recuperación y facilitación posterior de las notificaciones a las familias.

El EAP debe indicar a todos los evacuados que busquen seguridad en lugares interiores cercanos, si es posible (p. ej., oficinas, hoteles o centros de conferencias), para adaptarse al clima impredecible. También debe instruir al personal para que evite permanecer en las áreas de estacionamiento adyacentes a la empresa, ya que los atacantes pueden haber dejado artefactos explosivos improvisados en los vehículos.

Cuando sea posible, elija una ubicación con suficiente espacio para acomodar a todo el personal del lugar, así como espacios específicos (p. ej., habitaciones, tiendas de campaña o edificios adyacentes) que el grupo de control pueda designar para los servicios de emergencia, la policía, los medios de comunicación, las familias y los seres queridos, y para aquellos que necesitan atención médica. En particular, los medios y la prensa deben ser dirigidos a una ubicación específica y separada para mantenerlos alejados de las familias y el personal afectados y fuera del camino de los servicios de emergencias. El grupo de control también debe considerar los requisitos potenciales de todo el personal una vez evacuado, incluida la accesibilidad física en sus ubicaciones y el acceso a recursos en otros idiomas.

El grupo de control debe tomar nota de todo el personal contabilizado, desaparecido y herido, y mantener sus listas actualizadas a medida que se desarrolle la situación. Este grupo debe estar al tanto de antemano de cualquier empleado que trabaje fuera del sitio o esté ausente de la organización, así como de todo el personal en el sitio (p. ej., empleados, patrocinadores, contratistas y proveedores). Sin embargo, un simple recuento puede no ser exacto o ni siquiera posible; los evacuados pueden no ser capaces de reunirse en un único lugar, y es posible que parte del personal no haya podido evacuar y siga refugiado en el interior del edificio o edificios. Por esta razón, el EAP puede considerar el uso de herramientas de control, como el registro mediante una aplicación.

El grupo también debe compartir esta información con los servicios de emergencia para facilitar la ayuda médica y los reencuentros con familias y contactos de emergencia. Tenga en cuenta que, si hay menores entre los evacuados, los organizadores deben extremar las precauciones para identificar adecuadamente a sus padres o tutores a fin de garantizar su bienestar.

Seguir estos pasos para predeterminar un plan de control adecuado fomentará el debate mientras se crea el EAP para identificar y planificar los esfuerzos de respuesta asociados, como la coordinación de recursos suficientes (p. ej., alimentos, bebidas, terapeutas, clérigos) que los evacuados y el personal de emergencias puedan necesitar.

Grupos de operaciones médicas

El grupo de operaciones médicas está formado por personal claramente designado para abordar las necesidades inmediatas y garantizar la seguridad física después del rescate (p. ej., primeros auxilios inmediatos, CPR, primeros auxilios diferidos, morgue). Es posible que algunas organizaciones más grandes ya cuenten con un grupo de operaciones médicas, aunque la mayoría de las pequeñas y medianas empresas deben asignar estas funciones a sus empleados como parte del plan de gestión de emergencias.

Siempre que sea posible, el grupo de operaciones médicas debe incluir personal capacitado en primeros auxilios y CPR. Esto puede requerir que la organización brinde capacitación en primeros auxilios o requiera una certificación de CPR para algunos o todos sus empleados. Los recursos existentes pueden ayudar a las organizaciones y a sus empleados a comprender lo que necesitan saber y pueden enseñarles primeros auxilios básicos y accesibles, así como cuándo usarlos y cómo coordinarse con los grupos de servicios de emergencia que responden; estos recursos incluyen la iniciativa Stop The Bleed® del Colegio Estadounidense de Cirujanos (American College of Surgeons)[9] y You Are the Help Until Help Arrives de la FEMA[10]. Con estos conocimientos, las responsabilidades del grupo de operaciones médicas incluyen ayudar a los sobrevivientes y evacuados a llegar a hospitales u otros lugares de reunión o reubicación y apoyar todos los esfuerzos para transportar a las víctimas que no pueden ser tratadas en el lugar a centros médicos.

El grupo de operaciones médicas debe poder proporcionar a todo el personal médico y de emergencias cualquier información necesaria sobre el incidente para ayudar en el tratamiento. Este esfuerzo requiere conocimiento de todas las instalaciones médicas cercanas y sus capacidades y niveles de atención de trauma.[11]

Tenga en cuenta que una preparación integral requiere algo más que conocer el hospital más cercano. Es posible que se requieran otras instalaciones dependiendo de las necesidades de atención especializada u otros factores (p. ej., bloqueos de carreteras después del incidente que hacen necesaria una ubicación secundaria o un plan de respaldo).

Dependiendo de sus recursos, algunas organizaciones más grandes pueden tener un director de Seguridad u otro directivo designado que ya tenga conocimiento de las instalaciones médicas de su área y sus capacidades, así como relaciones establecidas con esas instalaciones y con las autoridades estatales y locales. Una relación existente con estas instalaciones es fundamental para una comunicación eficiente durante un incidente con un agresor activo y después de este. Las organizaciones sin un director de Seguridad previamente establecido deben asegurarse de que el grupo de operaciones médicas se comunique con estos grupos para que estén familiarizados entre ellos y que la relación de trabajo sea positiva y fluida en caso de un incidente. Un hospital puede saturarse rápidamente después de un incidente si muchas personas resultan heridas. La capacidad de comunicarse lo antes posible con los hospitales puede ayudar a los servicios de emergencia a preparar y organizar la debida atención para las víctimas, aunque la llegada al hospital y la distribución de la atención aún puede ser un proceso caótico.[12]

---

9 Stop The Bleed®, “Get Trained!”, consultado el 12 de julio de 2023, https://www.stopthebleed.org/training/.

10 Agencia Federal para el Manejo de Emergencias (FEMA), “You Are the Help Until Help Arrives”, consultado el 12 de julio de 2023, https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US.

11 Administración de Recursos y Servicios de Salud (Health Resources and Services Administration), “Find a Health Center”, consultado el 13 de julio de 2023, https://findahealthcenter.hrsa.gov/.

12 Administración para la Preparación y Respuesta Estratégica (ASPR, por sus siglas en inglés), Centro de Recursos Técnicos, Asistencia e Intercambio de Información (TRACIE, por sus siglas en inglés), “A Day Like No Other—Case Study of the Las Vegas Mass Shooting”, 2018, https://asprtracie.hhs.gov/technical-resources/resource/6472/a-day-like-no-other-case-study-of-the-las-vegas-mass-shooting.

Grupos de seguridad de servicios públicos

Dependiendo de los motivos y métodos del agresor, este puede causar daños considerables a los activos físicos y cibernéticos de una organización, incluidos equipos de fabricación, computadoras y sistemas en línea, sistemas de seguridad y productos manufacturados. Se deben establecer grupos de seguridad de servicios públicos para garantizar la seguridad física y cibernética de estos activos y mitigar el riesgo de robo o vulnerabilidad de los datos después de un incidente.

Las organizaciones de fabricación crítica más grandes pueden tener personal u oficinas de seguridad física y cibernética que funcionen como grupos de seguridad de servicios públicos. Sin embargo, es probable que las pequeñas y medianas empresas necesiten establecer los suyos propios. Dependiendo del tamaño, el diseño y los recursos de la organización, su seguridad física y cibernética puede ser administrada por una empresa externa (p. ej., un proveedor de IT externo puede proporcionar servicios de ciberseguridad a la empresa). De ser así, se debe alertar a estas agencias externas lo antes posible en caso de un incidente de agresor activo y se debe mantenerlas al tanto de los acontecimientos para evitar violaciones de ciberseguridad o robo de datos. La organización debe garantizar una forma de comunicación de respaldo para contactar con esta empresa en caso de cortes de energía o cierres de sistemas (p. ej., correo electrónico, teléfonos celulares, líneas fijas).

Específicamente, los grupos de seguridad de servicios públicos deben ser administrados por el Departamento de IT (interno o externalizado, según la estructura de la organización) y un equipo de seguridad física, dirigido por un director de Seguridad Física. Esta persona es el líder de la organización en todos los asuntos de seguridad física y, en colaboración con el Departamento de IT, proporciona soporte y liderazgo unificados en la gestión de riesgos de seguridad en toda la organización. Si bien algunas organizaciones de fabricación crítica cuentan con un equipo de seguridad física establecido y un director, otras, especialmente aquellas con menos recursos, con instalaciones más pequeñas o con niveles de seguridad más bajos, no lo tienen. Estas organizaciones necesitan asignar estas responsabilidades por sí mismas, ya sea al personal existente (p. ej., supervisores, gerentes de planta, otro personal responsable y conocedor) o al jefe de seguridad del edificio, la instalación o el complejo de la organización. El personal de seguridad física y de IT debe tener una comunicación fluida entre sí y con el resto de la organización.

Los incidentes de agresores activos son aterradores e inesperados, y las personas, a menudo, se muestran reacias a actuar ante una amenaza, especialmente si son las primeras en su ubicación en iniciar protocolos de emergencia. Cuanto más familiarizados estén una organización y su personal con sus planes de gestión de emergencias, más confianza tendrán para llevarlos a cabo y más dispuestos y capaces estarán para ayudar a otros ocupantes de las instalaciones (sin importar si otros empleados o visitantes desconocen o no los planes de gestión de emergencias de la organización).

Para ser más efectivas, estas medidas de respuesta inmediata deben incluir todos los niveles de empleo, así como varios equipos establecidos antes del incidente, muchos de los cuales permanecerán activos más allá de los esfuerzos de respuesta de la organización y en su recuperación a corto y largo plazo. Además de los esfuerzos de gestión de emergencias anteriores, una organización debe establecer las siguientes responsabilidades.

RESPONSABILIDADES DE COMUNICACIONES

La comunicación precisa y oportuna durante la respuesta a incidentes es vital para que una organización reciba la ayuda adecuada de los servicios de emergencia y las autoridades. También se utiliza para proporcionar información valiosa y práctica, como hechos conocidos sobre el incidente, cierres de carreteras y recursos disponibles para los afectados. Además, se debe contactar y mantener informados a los familiares del personal. Las organizaciones deben planificar para garantizar que sus comunicaciones durante este momento difícil sean precisas, coherentes y útiles para todos los involucrados, incluidas las siguientes responsabilidades:

- Las personas asignadas por el EAP, así como cualquier personal de seguridad presente, deben comunicarse con los servicios de emergencia y las autoridades.
- HR, ya sea interno o externalizado, debe mantener informados al personal y sus familias.
- Los ejecutivos del equipo directivo de la organización, el equipo legal (interno o externalizado), el equipo de Asuntos Externos (EA, por sus siglas en inglés) (si existe) y el personal asignado a un equipo de comunicaciones de crisis deben comunicarse con los medios.

Si bien cada vía de comunicación será diferente, todos los esfuerzos de comunicación deben coordinarse en conjunto.

Respuesta ante emergencias

El personal de seguridad, o un empleado designado, de la organización debe coordinar las tareas con los servicios de emergencia y las autoridades para garantizar una respuesta de emergencia adecuada. El personal de seguridad debe elaborar un plan de comunicación predeterminado que esté disponible para todas las agencias que puedan responder a un incidente de agresor activo (p. ej., autoridades, servicios de emergencia). También deben estar preparados para comunicarse con la policía y los portavoces del personal de los servicios de emergencia a su llegada y ayudar a incorporar los procedimientos de estas organizaciones lo más rápido posible (p. ej., dónde deben estar, dónde pueden tratar a las víctimas y rutas preestablecidas para llegar y salir).

Este personal debe trabajar con las autoridades y el personal médico competente para identificar a cualquier empleado que no esté contabilizado en el área de reubicación, los hospitales o la morgue, y debe poder confirmar si algún empleado estuvo ausente, viajando, trabajando desde casa o desde otra instalación, etc. También se deben contabilizar las personas que no sean empleadas en el edificio (p. ej., invitados, clientes, proveedores, personal de mantenimiento, repartidores).

Facilitación de información

Después de un incidente, se debe proporcionar diferente información (y de diferentes maneras) al personal y sus familias, a los medios de comunicación y a las autoridades. Difundir la información correcta a los canales apropiados puede ser una tarea abrumadora y requerirá coordinación en toda la organización.

Las organizaciones deberían considerar el uso de tecnología de comunicación masiva a la hora de enviar alertas y actualizaciones a todo el personal para que puedan tomar medidas inmediatas. Este sistema debe establecerse y practicarse antes de un incidente, con personal específico autorizado responsable de iniciar estas notificaciones. Las personas responsables de esta comunicación deben crear mensajes predefinidos que puedan adaptarse y enviarse rápidamente en caso de una emergencia. También deben configurar estas alertas en múltiples canales (p. ej., por teléfono celular y correo electrónico) en caso de que algunos métodos de comunicación no estén disponibles temporalmente.

Más allá de la comunicación a nivel de toda la organización, el personal de HR debe comunicar información práctica a los empleados y sus familias, como hechos conocidos sobre el incidente, cierres de carreteras, resolución y estado de las instalaciones, y notificaciones de asistencia y control adecuadas. Si una organización no tiene personal de HR establecido, esta responsabilidad puede recaer en el equipo de liderazgo de las instalaciones o de la empresa, según la estructura de la organización. Nuevamente, deben estar preparados para comunicarse utilizando múltiples canales de comunicación si es necesario. Antes del incidente, HR debe crear y mantener una lista de verificación de la información necesaria y apropiada para distribuir y anunciar al personal y las familias. Esta lista de verificación, al igual que los mensajes predefinidos por la organización, debe actualizarse en consecuencia después del incidente.

Las autoridades suelen ser responsables de las notificaciones de defunción, pero todas las organizaciones involucradas deben comprender sus responsabilidades y cómo transmitir noticias de manera precisa y con empatía. El personal debe estar preparado para informar a los familiares directamente sobre el incidente, incluso sobre empleados potencialmente desaparecidos, heridos o fallecidos.[13] La información sobre empleados desaparecidos, heridos o fallecidos o noticias igualmente sensibles deben darse en un entorno cerrado y privado (p. ej., una habitación separada del centro de reubicación de la organización, si es posible). Es posible que se requiera que una organización se comunique con médicos forenses o capellanes en caso de muerte de un empleado.

Como se indicó, el personal de HR es responsable de facilitar información precisa y oportuna sobre un incidente. Sin embargo, la información errónea puede presentar obstáculos para un intercambio eficaz de información. La información errónea puede propagarse rápidamente y dar lugar a que los rumores socaven los hechos. El personal de HR debe contar con un plan sobre cuándo y cómo planean controlar los rumores que socavan los esfuerzos de la organización posteriores al incidente. Esto puede incluir la creación de una plantilla de declaración que resuma el rumor y proporcione una explicación que lo desacredite.

---

13 FBI, *Developing Emergency Operations Plans: A Guide for Businesses*, marzo de 2018, https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view; CISA ISC, *Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide*, mayo de 2021, https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide.

Medios de comunicación

Las organizaciones deben crear un equipo de comunicaciones de crisis para que coordinen actividades con los medios de comunicación. Este equipo debe incluir ejecutivos del equipo directivo, así como el equipo legal de la organización y el Departamento de EA, si corresponde. Este equipo desarrollará y divulgará información sobre el incidente a los medios de comunicación, al personal del incidente y a otras organizaciones, según corresponda. Se deben establecer contactos y relaciones de trabajo con los medios locales antes de un incidente. Además, la persona o el equipo debe desarrollar puntos de conversación estándar con anticipación para que los líderes de la organización los utilicen al interactuar con los medios, utilizando un lenguaje uniforme y sencillo. El personal legal y de EA deben trabajar juntos para garantizar que no se diga nada que pueda causar problemas a la empresa.

Dependiendo del tamaño y los recursos de la organización, puede tratarse de un equipo de comunicaciones internas o se puede contratar a un tercero. De todos modos, esta persona o equipo debe tener una línea directa con los ejecutivos del equipo directivo de la organización. Las empresas pueden decidir contratar o tener en nómina a una empresa de gestión de crisis que se especialice en el manejo de incidentes en términos de cuestiones legales y de comunicaciones.

RESPONSABILIDADES DE IT

Adoptar un enfoque más proactivo al abordar los procedimientos de respuesta minimiza la confusión y los errores de juicio durante un incidente e inmediatamente después de este. Dependiendo de la gravedad del incidente, las torres de telefonía celular locales pueden verse saturadas por el volumen, lo que restringe las comunicaciones. Debido a esto, es posible que sea necesario utilizar diferentes canales temporalmente, como proporcionar actualizaciones en el sitio web de la organización o en las páginas de redes sociales o usar líneas de información automatizadas para informar a las personas que llaman para preguntar sobre la situación. Los profesionales de IT de la organización (ya sea en el propio Departamento de IT de la empresa o a través de un servicio de terceros) deben planificar el uso de estos canales de comunicación y prepararse para adaptarlos según sea necesario durante la respuesta a incidentes.

Quienes operan los canales de comunicación de la empresa deben tener en cuenta que, inmediatamente después de un incidente, una organización, sus empleados y la comunidad pueden ser blanco de intentos de estafa y robo de identidad. Estos delitos pueden presentarse en forma de sitios web, publicaciones en redes sociales, plataformas de financiación colectiva o solicitudes de estafadores que se hacen pasar por organizaciones benéficas. Los contratistas fraudulentos también pueden comunicarse con la organización o sus empleados en un intento de cometer fraude de seguros.[14] Las organizaciones deben realizar una investigación exhaustiva antes de firmar cualquier contrato, contratar ayuda externa o donar dinero, y animar a los empleados a hacer lo mismo; la base de datos de organizaciones benéficas del Servicio de Impuestos Internos (IRS, por sus siglas en inglés) de EE. UU. es un recurso útil.[15]

El Departamento de IT en coordinación con el equipo de EA, HR u otro departamento relevante, debe advertir al personal y al público sobre estos riesgos (p. ej., a través de publicaciones en las redes sociales, una advertencia en el sitio web de la empresa, notificaciones por correo electrónico a los empleados y socios de la empresa).

Concientice al personal sobre posibles estafas y fraudes:

- Las solicitudes fraudulentas de donaciones pueden provenir de solicitudes en persona, llamadas telefónicas, correos electrónicos o redes sociales.
- El IRS tiene una lista de organizaciones benéficas exentas de impuestos. Una organización benéfica que no aparece en esta lista puede ser fraudulenta.
- Algunos nombres de organizaciones benéficas fraudulentas pueden parecerse mucho a los de organizaciones benéficas reconocidas o pueden afirmar una afiliación con una organización benéfica existente.

Asegúrese de que los empleados reciban un enlace o una lista de organizaciones benéficas reconocidas a las que pueden donar de forma segura.

Reitere al personal la necesidad de verificar los sitios web y las direcciones de correo electrónico para detectar anomalías que puedan indicar fraude.

14 Oficina Federal de Investigaciones (Federal Bureau of Investigation), “Charity and Disaster Fraud”, consultado el 15 de agosto de 2023, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud.

15 Servicio de Impuestos Internos de EE. UU., “Tax Exempt Organization Search”, consultado el 18 de noviembre de 2023, https://www.irs.gov/charities-non-profits/tax-exempt-organization-search.

SEGUNDA PARTE: RECUPERACIÓN A CORTO PLAZO

Los esfuerzos de **recuperación a corto plazo** de una organización deben comenzar una vez que haya pasado la preocupación inmediata de muerte, lesiones y daños. La recuperación a corto plazo, que puede extenderse desde días hasta semanas o meses después del incidente, se ocupa principalmente de garantizar la salud y la seguridad de los empleados de la organización y la reanudación o continuación de las operaciones comerciales.

Después de un incidente con un agresor activo, la organización será irreconocible. Las operaciones no se reanudarán como de costumbre una vez que los servicios de emergencia y las autoridades hayan abandonado el lugar. Dependiendo de la gravedad del incidente, es posible que las operaciones no se reanuden (en parte o en su totalidad) durante semanas o incluso meses. Además, abordar los traumas físicos y mentales requerirá un gran esfuerzo, y una organización debe ser consciente de que no importa lo bien que responda a las necesidades de los empleados después de un incidente, es posible que aún así no quieran o no puedan regresar al trabajo.

Ayudar a una organización y a sus empleados a comenzar a recuperarse requerirá de muchos de los equipos y procesos creados durante la fase de respuesta inmediata, así como de nuevos equipos y esfuerzos realizados por otros miembros de la organización.

RESPONSABILIDADES DEL EQUIPO DIRECTIVO

Las responsabilidades de los ejecutivos del equipo directivo van mucho más allá de la respuesta inicial de su organización y se extienden a los esfuerzos de recuperación a corto y largo plazo. En los días y las semanas posteriores a un incidente, los empleados enfrentarán situaciones considerablemente perturbadoras tanto en su vida personal como profesional, y es vital que el equipo ejecutivo desempeñe un papel activo en los primeros pasos de la recuperación de su empresa.

Los ejecutivos del equipo directivo desempeñan un papel fundamental en la recuperación ante desastres y la continuidad del negocio. Deben tomar medidas proactivas, trabajar en estrecha coordinación entre ellos y con el resto de la organización y priorizar no solo la continuidad del negocio sino también la seguridad y la salud de los empleados. Además, los ejecutivos del equipo directivo son responsables de guiar eficazmente a los distintos departamentos que supervisan para minimizar los daños a la organización a corto y largo plazo durante una crisis. Todas las decisiones relacionadas con la información y comunicación sobre el incidente deben pasar por el líder del equipo de crisis o incidentes.

El equipo directivo también debe supervisar la devolución de las pertenencias de los empleados que quedaron en el lugar durante el proceso de evacuación. Deben informar a todo el personal que no podrán recuperar sus pertenencias hasta que se completen las investigaciones de la escena del crimen. En coordinación con las autoridades, el equipo directivo debe establecer un punto central para recolectar pertenencias personales y garantizar que los artículos (muchos de los cuales pueden ser costosos y ser objeto de robo, como teléfonos celulares, billeteras y computadoras) estén bien guardados y protegidos.

RESPONSABILIDADES DE COMUNICACIONES

Al igual que con el equipo directivo, las responsabilidades del equipo de comunicaciones van más allá de la etapa de respuesta inmediata a la crisis y se extienden hasta la recuperación a corto plazo. Este equipo debe continuar supervisando las actualizaciones necesarias del sitio web de la organización o los canales de redes sociales para garantizar que los clientes, las organizaciones asociadas y los seres queridos de los empleados estén informados sobre los actuales problemas de seguridad y continuidad del negocio.[16]

El equipo de comunicaciones debe establecer una estrategia de comunicación que proporcione información precisa y oportuna durante las primeras etapas del proceso de recuperación a corto plazo. No todas las organizaciones pueden ser lo bastante sólidas como para tener un equipo de gestión de crisis o incidentes completo, por lo que debe haber al menos una persona designada que pueda supervisar las responsabilidades de comunicación posteriores al incidente. La persona o el equipo de comunicaciones debe coordinar con la gerencia y el equipo directivo y de liderazgo para distribuir de forma adecuada contenidos y actualizaciones que destaquen los esfuerzos proactivos de la organización para manejar el incidente y, al mismo tiempo, mantener la imagen pública de la organización y el plan de continuidad del negocio.

El equipo de comunicaciones también debe garantizar que las familias de las víctimas no obtengan información sobre el incidente a través de canales públicos antes de que la organización se la comunique en privado. Además, la organización puede abrir una línea directa a la que el personal y sus seres queridos puedan llamar para recibir actualizaciones y acceder a recursos relevantes.

---

16 DHS, ready.gov, “Crisis Communications Plan”, consultado el 13 de julio de 2023, https://www.ready.gov/crisis-communications-plan.

RESPONSABILIDADES DE IT

El servicio de IT de la organización deberá determinar si los equipos de IT o telecomunicaciones de las instalaciones clave resultaron dañados o deshabilitados durante el incidente. Podrían pasar días o semanas para que este equipo sea reparado y vuelva a estar en pleno funcionamiento. Sin embargo, las organizaciones pueden garantizar que este aspecto de la recuperación a corto plazo se lleve a cabo de la manera más fluida y eficiente posible con la implementación de medidas exhaustivas de preparación contra riesgos (es decir, sistemas redundantes, archivos de recuperación externos, etc.) mucho antes de que se necesite el proceso de recuperación.

La función principal del servicio de IT de una organización es coordinar y proporcionar contexto e información relacionados con las repercusiones de IT asociadas con el evento inicial o las acciones de recuperación a corto plazo. El Departamento de IT debe utilizar esfuerzos de evaluación de riesgos poco después de que ocurra un incidente, incluida una caracterización completa del sistema, la identificación de amenazas y vulnerabilidades, el análisis de control y repercusiones y una determinación inmediata de riesgos para establecer mitigaciones de recuperación continuas a corto plazo.

RESPONSABILIDADES LEGALES

Se debe establecer un equipo para gestionar las responsabilidades legales de la organización después de un incidente con un agresor activo. Este equipo debe estar formado por el equipo legal existente de la organización (ya sea propio o externo) que supervisa sus asuntos legales. Para tratar de forma adecuada cualquier litigio que pueda surgir, es posible que la organización también necesite establecer asociaciones o conexiones con agencias u organizaciones legales externas antes de que ocurra un incidente.

Es probable que surjan litigios tras un incidente con un agresor activo, ya sean civiles (p. ej., demandas por negligencia o muerte por negligencia) o penales. Este equipo debe estar preparado para hablar en nombre de la organización durante el litigio, lo que incluye poder describir con precisión el incidente y sus resultados, comprender qué puede divulgarse públicamente y qué se debe mantener en privado y lidiar adecuadamente con la atención de los medios antes, durante y después del litigio.

El equipo legal y el de comunicaciones deben trabajar en estrecha coordinación para garantizar que cualquier información que transmitan públicamente sea legal, precisa y esté actualizada; que su descripción de la organización esté alineada con la imagen de la organización; y que su presencia en las redes sociales (tanto de la organización como de la persona) siga siendo apropiada y no revele ilegalmente información sobre el incidente que no debería hacerse pública.

Además, las víctimas que han sufrido un trauma pueden necesitar apoyo legal gratuito y competente para manejar posibles responsabilidades legales tras un incidente y durante la investigación en curso. La organización debe procurar tener un plan legal para víctimas desarrollado previamente en el que se aborden las necesidades legales de las víctimas.

RESPONSABILIDADES DE CONTINUIDAD DEL NEGOCIO

Continuar con las operaciones comerciales después de un incidente con un agresor activo será un desafío, e incluso imposible. Los obstáculos pueden incluir la pérdida temporal o permanente del acceso al lugar de trabajo; una fuerza laboral disminuida temporal o permanentemente debido a empleados fallecidos, heridos, afectados por el trauma o en proceso de duelo; pérdida de suministros o daños al equipo o la tecnología del lugar de trabajo, incluidos equipos de IT; e interrupción de la cadena de suministro (tanto ascendente como descendente). Es probable que la instalación permanezca como escena del crimen bajo investigación durante un período prolongado. Los líderes de la organización deben esperar que estas interrupciones sean igualmente expansivas y planificar en consecuencia.

Una organización debe establecer e implementar un plan exhaustivo de continuidad de las operaciones (CONOPS, por sus siglas en inglés) mucho antes de que ocurra un incidente para garantizar que las funciones comerciales esenciales se sigan llevando a cabo después del incidente.[17] Debido a que es posible que los empleados afectados por el trauma y lesionados no puedan reanudar su trabajo anterior durante mucho tiempo, si es que alguna vez lo hacen, las organizaciones necesitan un plan para que el personal capacitado pueda continuar operando las instalaciones, cuando sea posible.

---

17 Agencia Federal para el Manejo de Emergencias (FEMA), *Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101*, septiembre de 2021, https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf.

Las organizaciones deben desarrollar y poner en marcha un plan de transición para reanudar las operaciones normales de la forma más rápida y fluida posible, que puede incluir la transición a un espacio de trabajo temporal hasta que las oficinas normales o las plantas de la fábrica vuelvan a estar operativas o se reabran las carreteras que conducen al lugar de trabajo. Se debe asignar, entrenar y preparar personal capacitado para gestionar la reubicación o reorganización operativa, teniendo en cuenta que algunas instalaciones pueden ser inaccesibles mientras las autoridades completan su investigación. Las organizaciones también deben planificar la redundancia en las comunicaciones críticas, incluidos los servicios de IT, en sitios alternativos, utilizando potencialmente los canales de comunicación de las partes interesadas u otras organizaciones a lo largo de la cadena de suministro.[18]

Es fundamental garantizar que estas medidas de continuidad del negocio se comuniquen a toda la organización, de arriba abajo. Los empleados de todos los niveles de la organización deben participar para garantizar que estos procedimientos de recuperación a corto plazo sean integrales y eficientes.[19]

Seguridad física de personas, instalaciones y activos

La seguridad física es una parte vital de cualquier plan de seguridad. La seguridad física y la tecnología física de una organización desempeñan papeles particularmente importantes no solo en asegurar la protección del personal sino también en garantizar planes futuros de continuidad del negocio efectivos y eficientes. La tecnología física de una organización (desde computadoras y equipos de fabricación hasta sistemas de seguridad física existentes) puede ser atacada de forma intencional por un agresor, o dañarse o destruirse por accidente durante un ataque. Es fundamental que las organizaciones cuenten con directrices para abordar posibles daños, planificar el reemplazo o la reparación de los sistemas lo más rápido posible para garantizar la continuidad del negocio, mantener su marca y reputación y asegurar la protección de sus empleados, clientes y negocio.

RESPONSABILIDADES DE HR

Luego de un incidente de agresor activo, el personal experimentará una gran conmoción y angustia y necesitará todos los recursos disponibles para ellos y el apoyo de su organización durante la recuperación.[20] El Departamento de HR de una organización (ya sea interno o externalizado) puede desempeñar, o se le pueden asignar, múltiples funciones durante las etapas iniciales de la recuperación a corto plazo, como las siguientes, entre otras:

- Encargarse de todos los trámites relacionados con el fallecimiento de empleados y el pago del seguro a las familias.
- Reunir los artículos personales de los empleados fallecidos y asegurarse de que se devuelvan adecuadamente a sus familias.
- Gestionar las ausencias debido a lesiones o traumas emocionales.
- Conectar al personal con los servicios de salud mental a través de un programa de asistencia al empleado.
- Gestionar la nómina, las licencias por enfermedad y los beneficios médicos si los empleados no pueden regresar al trabajo durante un período prolongado o nunca pueden regresar al trabajo, etc.
- Gestionar el control del estrés de los empleados, por ejemplo, ofreciendo tiempo libre a los empleados que han estado supervisando los esfuerzos de gestión de crisis de la organización.
- Ocuparse de las velas conmemorativas u otros artículos dejados en el lugar para honrar a los fallecidos o heridos. También deberán ocuparse de estos objetos después del incidente, de modo que la tarea no recaiga en la población.
- Buscar organizaciones locales sin fines de lucro que puedan gestionar y distribuir las donaciones realizadas por la gente después de un incidente.
- El Departamento de HR, el equipo de comunicaciones y la gerencia del equipo directivo deben trabajar juntos para reconocer y abordar las inquietudes del personal después del incidente.

---

18 CISA, *Critical Manufacturing Sector Security Guide*, julio de 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

19 DHS, "Emergency Action Plan Guide: Active Shooter Preparedness", noviembre de 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite.

20 Administración de Servicios de Salud Mental y Abuso de Sustancias (Substance Abuse and Mental Health Services Administration), "Disaster Distress Helpline", consultado el 12 de julio de 2023, https://www.samhsa.gov/find-help/disaster-distress-helpline; VictimConnect, "VictimConnect Resource Center", consultado el 12 de julio de 2023, https:// victimconnect.org/; FBI, "FBI Victim Services", 2018, https://www.fbi.gov/file-repository/fbi-victim-services-brochure-2018.pdf/view.

PARTE TRES: RECUPERACIÓN A LARGO PLAZO

La fase de **recuperación a largo plazo** consta de actividades que continúan mucho más allá del período del incidente y se centra en restaurar, redesarrollar y revitalizar funciones organizativas y comunitarias críticas, y comenzar a gestionar los esfuerzos de estabilización y mitigación. Tenga en cuenta que el proceso de recuperación completo tardará años en completarse. Llevar a cabo una revisión integral posterior a la acción es fundamental para prepararse para futuros incidentes, ya sean causados por humanos o naturales. Esta revisión debe realizarse al mismo tiempo que los esfuerzos de recuperación a largo plazo y puede incorporarse a la revisión posterior a la acción y a la documentación de seguimiento.

Muchas de las medidas adoptadas en la primera y segunda parte deben continuar en el largo plazo, a menudo adaptándose y expandiéndose mucho más allá de las estructuras de equipo iniciales descritas anteriormente. También puede haber una superposición entre algunas actividades de recuperación a corto y largo plazo. Estos esfuerzos a largo plazo deben centrarse en asegurar la salud, la seguridad y la estabilidad del personal de una organización, así como en respaldar la continuidad del negocio, la posición de la organización ante los medios de comunicación y el público, y garantizar la seguridad física y cibernética a largo plazo de la organización.

RESPONSABILIDADES DE LA SALUD DEL PERSONAL

Tanto HR como los altos mandos directivos tendrán muchas responsabilidades continuas durante la recuperación a largo plazo de una organización. Es vital que la empresa continúe atendiendo y adaptándose a los cambiantes problemas de salud física y mental del personal, muchos de los cuales se extenderán a largo plazo.[21]

El trauma afecta a las personas de maneras diferentes y, a menudo, inesperadas. Los empleados pueden sentir ansiedad o inseguridad en ciertos escenarios, y la empresa debe estar preparada para adaptarse a estos cambios. Por ejemplo, los espacios pequeños y cerrados (como la puerta cerrada de una oficina) pueden provocar una sensación de miedo.

Es posible que la empresa necesite ampliar sus disposiciones de atención médica existentes para garantizar la salud física y la seguridad del personal. La empresa también puede asociarse con servicios de salud mental externos para satisfacer adecuadamente las necesidades de salud mental de los empleados. Esto podría incluir brindar acompañamiento durante el duelo para ayudar a los empleados a afrontar los efectos a largo plazo en su bienestar mental.

Además de respaldar los problemas de salud física y mental de los empleados, la organización deberá identificar y reconocer a los empleados que hayan sufrido daños o hayan fallecido. Es probable que las familias y los compañeros de trabajo quieran conmemorar el evento de alguna manera en las instalaciones, ya sea mediante una ceremonia, un monumento físico o ambos. La conmemoración también puede hacerse anualmente.

RESPONSABILIDADES DE CONTINUIDAD DEL NEGOCIO

Restaurar y mantener las operaciones comerciales seguirá siendo un desafío en los meses y años posteriores a un incidente.[22] Una organización debe considerar varios componentes al abordar posibles problemas de continuidad del negocio, como interrupciones a largo plazo en la cadena de suministro;[23] pérdida de empleo permanente o a largo plazo debido a lesiones, traumatismos o preocupaciones relativas a la seguridad al regresar a las instalaciones; y posibles repercusiones económicas y de marca para la organización. La organización debe revisar y evaluar todos los componentes dentro de su cadena de suministro para determinar cualquier factor que influya en su capacidad para restablecer el suministro en el mercado.

Como se señaló en la segunda parte, una organización enfrentará inevitablemente pérdidas en materia de empleo después de un incidente de agresor activo y, en muchos casos, esta disminución de la fuerza laboral se extenderá a largo plazo. Las organizaciones deben reconocer que es posible que algunos empleados nunca quieran volver al mismo entorno o reanudar sus operaciones, incluso en una ubicación diferente. El impacto

---

21 CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response*, 2019, https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide; DHS, *Active Shooter Recovery Guide*, agosto de 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.

22 DHS, *Active Shooter Recovery Guide*, agosto de 2017, https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide.

23 CISA, *Critical Manufacturing Sector Security Guide*, julio de 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

psicológico y físico de un incidente tan traumático es diferente para cada persona. Para mantener los niveles de empleo lo mejor posible y garantizar que los empleados existentes permanezcan en la empresa, la organización debe comprender y adaptarse a la variedad de razones por las que los trabajadores no pueden o no quieren volver al trabajo. Puede que algunos empleados hayan sufrido lesiones físicas que durarán a largo plazo. Es posible que otros aún no puedan trabajar debido a un trauma continuo, duelo o miedo a regresar a un entorno laboral inseguro.

Tenga en cuenta que las preocupaciones relativas a la seguridad, así como el estigma social y profesional que puede surgir en torno a la organización después de un incidente, pueden mantener alejados tanto a los empleados existentes como a los futuros. Para retener a los empleados existentes y atraer personal nuevo, la organización debe prepararse para adaptarse a sus necesidades. Por ejemplo, las organizaciones pueden mejorar y aumentar los sistemas de seguridad, los circuitos cerrados de televisión (CCTV) y los procedimientos de capacitación en seguridad para garantizar que el edificio sea seguro para todos los empleados existentes y futuros.

Las empresas deberán proporcionar y coordinar activamente un apoyo continuo para los empleados con traumas existentes y ofrecer servicios de salud mental para satisfacer adecuadamente las necesidades psicológicas de los empleados. Es posible que se requieran fondos adicionales para brindar servicios de asesoramiento y salud mental para los empleados de forma permanente.

Además, las organizaciones deberán revisar y analizar cualquier impacto económico a largo plazo posterior al incidente para garantizar la sostenibilidad económica de la empresa y mantener su marca y reputación dentro de la industria, la cadena de suministro y la comunidad. El daño a la reputación se puede evaluar examinando la participación de mercado y el precio de las acciones de la empresa. Como parte de su análisis económico, la empresa deberá considerar reclamaciones de compensación extendida y otros tipos de asistencia financiera para el personal, que pueden extenderse hasta el período de recuperación a largo plazo.

RESPONSABILIDADES DE DIVULGACIÓN PÚBLICA

Las responsabilidades de comunicación de la organización también continuarán a largo plazo. Los esfuerzos del equipo de comunicaciones, el equipo legal, los ejecutivos del equipo directivo y otros deberán manejar las interacciones continuas con las autoridades, los servicios de emergencia y cualquier procedimiento legal que pueda surgir. También se les puede asignar la tarea de mantener actualizado el sitio web de la organización y la presencia en las redes sociales para transmitir información sobre el proceso de recuperación. Esto puede incluir detalles sobre nuevas medidas de seguridad, condolencias por los heridos y fallecidos en el incidente y actualizaciones de continuidad del negocio. Además, es fundamental que la organización mantenga un canal de comunicación exclusivo para los empleados que se vieron directamente afectados por el incidente y sus seres queridos. Esto garantiza que reciban el apoyo y la información necesarios durante el proceso de recuperación a largo plazo.

Además, la organización deberá planificar eventos conmemorativos y memoriales anuales. Estas son oportunidades para revaluar las necesidades de planificación y seguridad de la organización y determinar la salud, la seguridad y la estabilidad del personal, también para reconocer el impacto que ha tenido un incidente en una empresa, el personal, las familias y la comunidad. Dependiendo de la magnitud del incidente, estos eventos conmemorativos también pueden requerir la coordinación de un comunicado o una conferencia de prensa, además de hacer una declaración en el sitio web y las páginas de redes sociales de la organización.

RESPONSABILIDADES DE SEGURIDAD FÍSICA Y CIBERNÉTICA

Restaurar la seguridad de una organización después de un incidente (incluida tanto la seguridad del personal como la seguridad física y cibernética de sus activos) es una pieza vital de la recuperación a largo plazo que puede tardar meses o incluso años en conseguirse. Hay varios factores que una organización debe considerar como parte de sus responsabilidades de seguridad física y cibernética. La organización debe analizar todos los daños físicos y cibernéticos causados por el incidente,[24] que incluyen posibilidades de amenazas internas, artículos personales robados o dañados, sistemas de seguridad física o cibernética comprometidos y activos físicos y electrónicos destruidos o comprometidos. Esto también incluye cualquier daño o cambio en la reputación de la organización dentro de la industria, la cadena de suministro y la comunidad.

Abordar estos daños es esencial no solo para salvaguardar la continuidad del negocio y la seguridad financiera de la organización, sino también para mejorar la sensación de seguridad de los empleados dentro de la organización. Muchos trabajadores se sentirán inseguros al regresar a una ubicación que

24 CISA, *Critical Manufacturing Sector Security Guide*, julio de 2020, https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf.

estuvo comprometida en el pasado (incluso después de que hayan pasado meses o años) y necesitarán ver cambios tangibles y significativos en las medidas de seguridad de la organización. Involucrar al personal en el análisis de las mejoras necesarias, así como solicitar su opinión sobre lo que vieron durante el incidente y que podría haberse evitado o mitigado, puede ser un paso valioso en la implementación de estos cambios. Estos cambios pueden incluir la instalación de un sistema de seguridad integral y actualizado en todas las entradas y salidas del edificio, autenticación multifactor para todos los datos de la empresa y capacitación obligatoria sobre agresores activos para todo el personal, que cubra temas como prevención, mitigación, respuesta y recuperación.[25] Si la organización ya contaba con capacitación antes del incidente, es posible que sea necesaria una evaluación del programa para asegurarse de que esté actualizado. Debido a que la tecnología avanza a un ritmo tan rápido, es posible que sea necesario actualizar incluso un nuevo programa de capacitación para tener en cuenta los cambios en las amenazas a la ciberseguridad y las formas en que los sistemas de seguridad, la maquinaria y los datos pueden verse comprometidos.

Tenga en cuenta que para algunos empleados que han experimentado un trauma previo ciertos planes y ejercicios de capacitación pueden resultar difíciles o imposibles debido a la angustia emocional causada por el contenido de la capacitación. Sea comprensivo y compasivo con estos empleados y busque formas alternativas (p. ej., diferentes programas de capacitación, instrucciones escritas en lugar de videos) para mantenerlos actualizados sobre las medidas de seguridad y los procedimientos de emergencia de la organización.

Existen muchos recursos federales para informar y capacitar a las organizaciones y a sus empleados sobre la detección, la prevención y la mitigación de amenazas físicas y cibernéticas. Estos incluyen el conjunto de recursos de mitigación de amenazas internas de la CISA[26] y su Evaluación del Programa de Mitigación de Riesgos Internos (IRMPE, por sus siglas en inglés), que se puede utilizar para medir la preparación de una organización para un incidente de agresor activo.[27] Otros cursos de capacitación en línea, como los diversos cursos de preparación para desastres de la FEMA, deben ser de carácter obligatorio para que el personal fortalezca sus habilidades de preparación para emergencias.[28] Estas medidas deben tomarse periódicamente para garantizar la protección y la seguridad ciberfísica de una organización.

CONCLUSIÓN

La Guía de prácticas recomendadas posteriores a incidentes de agresores activos en el sector de fabricación crítica sirve como recurso para organizaciones de todos los tamaños. Todas las organizaciones de fabricación crítica y sus filiales pueden utilizar esta Guía al planificar sus esfuerzos de respuesta y recuperación posteriores al incidente.

Incluso si una organización toma todas las medidas que figuran en esta guía cuando ocurre un incidente, es poco probable que los empleados vuelvan alguna vez a los niveles de comodidad y seguridad que tenían antes del incidente dentro de la organización. De manera similar, la organización puede sobresalir en sus esfuerzos de continuidad del negocio y, aun así, nunca alcanzar los niveles operativos previos al incidente.

Recuerde que la recuperación no es un proceso lineal, y es posible que la organización afectada nunca vuelva a la normalidad que tenía antes del incidente. Sin embargo, al utilizar estas medidas como guía para la respuesta inmediata y la recuperación a corto plazo y a largo plazo, **la organización puede lograr una nueva línea de base para garantizar la seguridad del personal y la continuidad de sus operaciones.**

Para obtener más información o buscar ayuda adicional, contáctenos en CriticalManufacturingSector@cisa.dhs.gov.

---

25 CISA ISC, *Violence in the Federal Workplace: A Guide for Prevention and Response*, 2019, https://www.cisa.gov/resources-tools/ resources/isc-violence-federal-workplace-guide.

26 CISA, "Insider Threat Mitigation", consultado el 13 de julio de 2023, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation.

27 CISA, "Insider Risk Mitigation Program Evaluation (IRMPE)", consultado el 12 de julio de 2023, https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe.

28 FEMA, Instituto de Manejo de Emergencias (Emergency Management Institute), "ISP Courses", consultado el 13 de julio de 2023, https://training.fema.gov/is/crslist.aspx?lang=en.

ANEXO A: HOJAS SEPARADAS

Este anexo proporciona una serie de listas de verificación para que las organizaciones de fabricación crítica y sus filiales preparen sus planes de respuesta inmediata, recuperación a corto plazo y recuperación a largo plazo tras un incidente de agresor activo. Estas listas de verificación están diseñadas para que puedan separarse de la Guía de prácticas recomendadas, imprimirse y ser distribuidas según sea necesario entre los ejecutivos del equipo directivo, el personal de Recursos Humanos (HR) y todos los demás empleados involucrados en la creación y ejecución del Plan de Acción de Emergencia (EAP) de la empresa.

Las organizaciones deben adaptar estas listas a sus circunstancias y recursos específicos, utilizarlas durante la capacitación sobre incidentes de agresores activos, mantenerlas a mano cuando sea posible durante la respuesta y recuperación del incidente y actualizarlas según sea necesario después de un incidente o cada vez que se produzca un cambio en la estructura de la empresa o el EAP.

Antes de que ocurra un incidente

Utilice esta lista para asegurarse de que el EAP de su empresa sea completo, esté actualizado y se adapte a los edificios, la estructura laboral y la ubicación de la organización. Modifique los títulos y las categorías de empleo según sea necesario e indique los puestos que deberán externalizarse, así como las personas designadas dentro de su empresa responsables de contactar y mantener una conexión con estos grupos externalizados antes del incidente.

Contabilización inmediata del grupo

Utilice estas listas de verificación para garantizar que los empleados designados mantengan un registro preciso y completo de todo el personal de la organización y su estado durante y después de una evacuación. Si es necesario, agregue más filas a la tabla e incluya columnas separadas para otras ubicaciones específicas del EAP.

Respuesta inmediata

Esta lista describe las responsabilidades básicas de varios puestos dentro de una organización, incluido el equipo directivo, el director de Seguridad, el Departamento de HR y el equipo legal, para llevar a cabo un esfuerzo de respuesta inmediata optimizado y seguro. Ajuste estos puestos según sea necesario para que concuerden con la estructura de la organización y adapte las responsabilidades individuales para que se ajusten al EAP de la organización.

Recuperación a corto plazo

Al igual que el punto anterior, utilice esta lista de verificación para cubrir los conceptos básicos del plan de recuperación a corto plazo de su organización, ajustando funciones y responsabilidades según sea necesario para adaptarse a la estructura y situación de la empresa. Tenga en cuenta los procedimientos que deberán externalizarse, así como los medios para contactar y mantener una relación laboral con estos servicios y las personas dentro de la empresa responsables de contactarlos y trabajar con ellos después del incidente.

Recuperación a largo plazo

Utilice esta lista, al igual que la anterior, para describir los esfuerzos de recuperación a largo plazo de la empresa. Consulte esta lista periódicamente durante los meses y años de su recuperación a largo plazo, actualícela y ajústela según sea necesario para que refleje cualquier cambio en las circunstancias o nuevas áreas de enfoque (p. ej., avances en litigios, cambios en la salud o el estado laboral del personal, fluctuaciones en la situación financiera de la empresa).

ANTES DE QUE OCURRA UN INCIDENTE

Director de Seguridad/director de la instalación

- ☐ Elaborar e implementar un Plan de Acción de Emergencia (EAP). Consultar www.ready.gov para obtener ideas y plantillas, así como también el paquete de planificación de la continuidad empresarial.
- ☐ Coordinar con el personal de emergencias local (policía y bomberos) para definir un proceso para controlar al personal, métodos para proteger las áreas de la empresa, qué esperar durante un incidente y después de este, y cómo y cuándo devolver las pertenencias personales a los empleados.
  - Bolsos, identificaciones, computadoras, teléfonos, automóviles, etc., probablemente quedarán atrás durante la evacuación y deberán ser asegurados y custodiados antes de que los empleados o el pariente más cercano los recojan ordenadamente.
- ☐ Coordinar con los bomberos y el personal de emergencias médicas todo lo necesario con respecto al triaje. Identificar y hacer un mapa de los centros médicos y de traumatología de la zona.
- ☐ Capacitar al personal en procedimientos de evacuación.
  - Asegurarse de que los procedimientos de evacuación sean prácticos para cualquier miembro del personal con necesidades funcionales y de acceso o que no domine el inglés.
- ☐ Crear un sistema de notificación a los empleados multicanal (p. ej., teléfono, correo electrónico, etc.) y asignar la responsabilidad de su activación.
  - Realizar pruebas periódicas de este sistema de notificación, para asegurarse de que llegue a todo el personal independientemente de cualquier discapacidad, barreras idiomáticas o áreas de trabajo con altos niveles de ruido.
- ☐ Proporcionar o utilizar capacitación en el Sistema Nacional de Gestión de Incidentes (NIMS).
- ☐ Utilizar recursos federales, como el conjunto de herramientas de la Oficina para Víctimas de Delitos, la guía de preparación de la Agencia Federal para el Manejo de Emergencias (FEMA) y la herramienta electrónica del Plan de Acción de Emergencia de la Administración de Seguridad y Salud Ocupacional (OSHA).
- ☐ Establecer un grupo de control y predeterminar métodos para contabilizar al personal (p. ej., verificación a través de una aplicación).
- ☐ Designar empleados calificados para un grupo de operaciones médicas, si es posible.
- ☐ Establecer un grupo de seguridad de servicios públicos, si es necesario.
- ☐ Implementar y poner en práctica un plan integral de continuidad de las operaciones (CONOPS).
- ☐ Animar al personal a recibir capacitación en primeros auxilios y CPR.
- ☐ Designar responsables principales para cada piso, instalación y ubicación para supervisar e informar la contabilización de empleados.

Departamento de Recursos Humanos (HR)

- ☐ Trabajar con el director de Seguridad o de la instalación para saber dónde están ubicados los centros médicos y de traumatología. Asegurarse de que todos los puntos de contacto (POC, por sus siglas en inglés) en las ubicaciones estén actualizados y que se hayan realizado las presentaciones (p. ej., personal de comunicaciones del hospital, etc.).
- ☐ Trabajar con el equipo legal, Asuntos Externos (EA), el equipo directivo y otras partes relevantes para identificar y organizar áreas de reunión y reubicación y asegurar la contratación de los servicios necesarios (hoteles, centros de conferencias, etc.) que se implementarán según corresponda.
  - Asegurarse de que estas partes están al tanto de los POC actuales y de cualquier actualización del EAP.
- ☐ Determinar los requisitos y beneficios del personal en caso de tales incidentes, incluidas las responsabilidades de la empresa.
- ☐ Si existe un sindicato en la instalación, trabajar con los representantes sindicales y el personal para identificar y abordar cualquier problema sindical que deba considerarse.
- ☐ Elaborar una lista de verificación de información esencial que se comunicará al personal y sus familias en caso de un incidente.

Empleados

- ☐ Completar la capacitación sobre agresores activos proporcionada por la empresa.
- ☐ Participar en simulacros de agresores activos organizados por la empresa.
- ☐ Participar en las pruebas del sistema de notificación de empleados y proporcionar comentarios.
- ☐ Asegurarse de que toda la información de los POC, familiares cercanos, etc., esté actualizada.
- ☐ Asegurarse de que toda la información sobre beneficiarios del seguro, prestaciones médicas y de otra índole esté actualizada.
- ☐ Asegurarse de que los miembros de la familia tengan acceso a copias de toda la información médica y del seguro en un lugar de fácil acceso en caso de emergencia.

Departamento Legal

- ☐ Trabajar con el equipo directivo, HR, el director de Seguridad y otras partes relevantes para abordar cuestiones legales relacionadas con posibles incidentes.
- ☐ Colaborar con EA y el equipo directivo para desarrollar puntos clave para los medios en caso de un incidente, asegurándose de que no se hagan declaraciones que puedan representar problemas para la empresa.

Departamento de Asuntos Externos/Comunicaciones

- ☐ Colaborar con el equipo directivo, HR, el director de Seguridad, etc., en la redacción de mensajes para enviar a las familias y los empleados afectados.
- ☐ Elaborar plantillas de divulgación para medios sociales y convencionales para facilitar la presentación de informes. Anticiparse al problema puede evitar que la información errónea ocupe un lugar central en los medios o en línea.
- ☐ Establecer un equipo de comunicaciones de crisis para manejar las relaciones con los medios, difundiendo información relacionada con el incidente a todas las partes relevantes según sea necesario.
- ☐ Construir conexiones y cultivar relaciones de trabajo con los medios de comunicación locales.
- ☐ Trabajar con el equipo directivo, HR, el director de seguridad, IT y cualquier otro grupo relevante para establecer plantillas de mensajes sobre posibles sitios web, solicitudes, etc., de donaciones fraudulentas. Prepararse para combatir dichas actividades publicando o anunciando periódicamente información precisa sobre donaciones.

Departamento de Tecnologías de la Información/grupo de red

- ☐ Trabajar con el director de Seguridad para salvaguardar la ciberseguridad y los activos cibernéticos de la empresa durante incidentes físicos.
- ☐ Mantener la integridad continua de la red.
- ☐ Si es necesario, ayudar a establecer un sistema de notificación al personal.
- ☐ Planificar el uso de canales de comunicación alternativos, como redes sociales y sitios web de la empresa, para la comunicación y prepararse para adaptarlos según sea necesario durante la respuesta al incidente.
- ☐ Establecer planes para situaciones en las que los posibles agentes de amenazas intentan aprovechar un sistema de red degradado durante un incidente.

Departamentos de Finanzas/Contratación/Proveedores

- ☐ Incorporar cláusulas contractuales para abordar incidentes causados por humanos.
- ☐ Dar seguimiento a proveedores y clientes para evaluar compras o pedidos pendientes.

CONTABILIZACIÓN INMEDIATA DEL GRUPO

- **Tome nota y clasifique a los empleados lesionados para el personal de emergencias médicas.**
- **Si corresponde, utilice métodos preestablecidos para transportar al personal a un lugar seguro.**

Después de una evacuación, los miembros del grupo de control designado deben contabilizar al personal, incluido el número total de personas en cada categoría, así como sus nombres y ubicación (si se conocen).

Grupo de control

Gerentes de piso/instalación/área u otros empleados previamente designados para contabilizar al personal (incluidos los heridos, sanos, desaparecidos, de viaje/ fuera de la ciudad/de licencia) después de la evacuación.

Contabilizado, fuera del sitio *(de viaje, fuera de la ciudad, de vacaciones, etc.)*	**En buen estado**	**Desaparecido/ desconocido**	**Herido** *(incluya hospital o estado, si se conoce)*
CANT. TOTAL:	CANT. TOTAL:	CANT. TOTAL:	CANT. TOTAL:

RESPUESTA INMEDIATA

Director de Seguridad/director de la instalación

- ☐ Coordinar con el personal de emergencias local.
- ☐ Garantizar que el equipo directivo, HR y el equipo de Asuntos Externos (EA)/Comunicaciones estén informados sobre las instalaciones médicas a las que han sido trasladados los empleados.

Equipo directivo

- ☐ Si la instalación aún está operativa, analizar cuándo y en qué medida se pueden reanudar las operaciones después de las investigaciones.
- ☐ Contactarse con los empleados, las familias, los clientes y los accionistas afectados por el incidente.
- ☐ Trabajar con EA/Comunicaciones para manejar la cobertura mediática del incidente.

Equipo de Recursos Humanos

- ☐ Trabajar con el director de Seguridad o de la instalación para identificar las instalaciones médicas donde los empleados han sido llevados.
- ☐ Trabajar con su equipo legal, EA, equipo directivo y otras partes relevantes para organizar las áreas de reubicación (hoteles, centros de conferencias, etc.).
- ☐ Mantener informados al personal y sus familias sobre el estado del incidente y el paradero de los empleados.
- ☐ Tramitar cualquier documentación requerida para los empleados afectados que no puedan trabajar debido a lesiones o para las familias de los empleados fallecidos.
- ☐ Trabajar con representantes sindicales, si corresponde, para garantizar que la organización cumpla con los requisitos sindicales y para abordar cualquier posible problema relacionado con el sindicato debido al incidente.
- ☐ Trabajar con profesionales de la salud mental para crear planes de apoyo inmediato y a largo plazo para el trauma, incluido el tratamiento del estrés postraumático.
- ☐ Comunicar la información necesaria al personal y sus familias, como detalles confirmados sobre el incidente, cierres de carreteras, actualizaciones del estado de las instalaciones (incluida la recolección de pertenencias personales) y notificaciones de asistencia y responsabilidad adecuadas.
- ☐ Actualizar de forma precisa, compasiva y privada a los miembros de la familia directamente sobre el incidente, incluidos los empleados potencialmente desaparecidos, lesionados o fallecidos.

Equipo legal

- ☐ Trabajar con el equipo directivo, HR, el director de Seguridad y cualquier otro grupo relevante para prepararse para cualquier problema legal que pueda surgir del incidente.

Equipo de IT/grupo de red

- ☐ Trabajar con el director de Seguridad para salvaguardar los activos cibernéticos de la empresa de cualquier repercusión potencial debido a un incidente físico.
- ☐ Mantener la integridad de la red.

Equipo de Asuntos Externos/Comunicaciones

- ☐ Trabajar con el equipo directivo, HR, el director de Seguridad y otros grupos relevantes para redactar mensajes para las familias y los empleados que se han visto afectados por el incidente. Esto puede incluir elaborar mensajes predefinidos para ayudar con la comunicación inmediatamente después de un incidente.
- ☐ Continuar supervisando la relación con los medios de comunicación hasta la total resolución de la incidencia.
- ☐ Enviar mensajes a organizaciones benéficas legítimas para solicitar donaciones. Aconsejar a las personas que estén atentas a las organizaciones benéficas fraudulentas y que las denuncien de manera adecuada.

RECUPERACIÓN A CORTO PLAZO

Director de Seguridad/director de la instalación

- ☐ Identificar las lecciones aprendidas de los éxitos y fracasos en materia de seguridad.
- ☐ Incorporar lecciones aprendidas y actualizar el Plan de Acción de Emergencia (EAP) de la organización.

Equipo directivo

- ☐ Reparar los daños sufridos por las instalaciones durante el incidente.
- ☐ Garantizar que las instalaciones sean seguras para que los empleados regresen al trabajo.
- ☐ Proporcionar tranquilidad a los accionistas en caso de una caída del mercado.

Equipo de Recursos Humanos

- ☐ Desarrollar un plan para facilitar la transición de los empleados de regreso al trabajo.
- ☐ Contemplar el impacto potencial del trauma en la capacidad de los empleados para regresar al trabajo.
- ☐ Determinar cómo manejar adecuadamente los artículos que se dejan en las instalaciones, tanto si se devuelven a los empleados, a los familiares o si se utilizan como parte de un acto conmemorativo.
- ☐ Decidir si la empresa organizará servicios conmemorativos en el aniversario del incidente.

Equipo legal

- ☐ Gestionar demandas de empleados lesionados o familiares de los empleados fallecidos.
- ☐ Gestionar cualquier procedimiento legal relacionado con los sospechosos.
- ☐ Prepararse para representar a la organización durante el litigio, incluida la descripción precisa del incidente y los resultados, la gestión de divulgaciones públicas y el manejo de los medios durante todo el proceso legal.
- ☐ Analizar la posibilidad de contar con un plan de apoyo legal preestablecido para abordar las necesidades de las víctimas.

Equipo de IT

- ☐ Determinar si algún equipo de IT o de telecomunicaciones ha sufrido daños o averías debido al incidente.
- ☐ Realizar evaluaciones de riesgos cibernéticos o de IT poco después de que suceda el incidente.

Equipo de Asuntos Externos/Comunicaciones

- ☐ Continuar comunicándose con el personal y gestionar cualquier solicitud de los medios.
- ☐ Ofrecer información precisa y oportuna durante las fases iniciales de recuperación a corto plazo.
- ☐ Coordinar con el liderazgo del equipo directivo para compartir actualizaciones sobre la gestión proactiva de incidentes y preservar a la vez la imagen pública y el plan de continuidad del negocio.
- ☐ Establecer una línea directa a la que el personal y sus seres queridos puedan llamar para recibir actualizaciones o acceder a recursos relevantes.
- ☐ Trabajar con HR para identificar y proporcionar recursos que el personal y los familiares más cercanos puedan utilizar si es necesario (médicos, psicológicos, etc.).

Equipo de Finanzas/Contratación/Proveedores

- ☐ Dar seguimiento a proveedores y clientes para evaluar las repercusiones en compras o pedidos pendientes.
- ☐ Trabajar para obtener costos para la recuperación a corto y largo plazo, incluida la limpieza y reparación de las instalaciones, la incorporación de nuevas medidas de seguridad basadas en las lecciones aprendidas, atención médica ampliada u otros beneficios para el personal, etc.

RECUPERACIÓN A LARGO PLAZO

Director de Seguridad/director de la instalación

- ☐ Incorporar las lecciones aprendidas en la capacitación y los ejercicios sobre incidentes.
  - Implementar programas nuevos de capacitación sobre agresores activos para empleados o evaluar los existentes, que se llevarán a cabo y actualizarán periódicamente (p. ej., anualmente).
- ☐ Actualizar el Plan de Acción de Emergencia (EAP) existente de la organización.
- ☐ Implementar nuevos protocolos y tecnología de seguridad basados en las lecciones aprendidas.
- ☐ Evaluar todos los daños físicos posteriores al incidente, incluidos los artículos robados o dañados, los sistemas de seguridad comprometidos y los activos afectados.

Equipo directivo

- ☐ Trabajar para restablecer la reputación de la empresa en los medios, la industria y su cadena de suministro.
- ☐ Mantener contacto con el personal para asegurarles el compromiso de la empresa con la rehabilitación.
- ☐ Evaluar las preocupaciones sobre la continuidad del negocio, incluidas las interrupciones prolongadas de la cadena de suministro, los desafíos sostenidos del empleo debido a lesiones o traumatismos y los posibles impactos económicos.

Equipo de Recursos Humanos

- ☐ Proporcionar recursos de apoyo a la salud mental a largo plazo para empleados que sufrieron traumas.
- ☐ Ampliar la atención médica del personal para abordar los problemas de salud posteriores al incidente, según sea necesario.
- ☐ Administrar y efectuar pagos de seguros a las familias de los empleados fallecidos.
- ☐ Adaptarse para ajustarse a las necesidades cambiantes de salud física y mental de los empleados.

Equipo legal

- ☐ Atender acciones legales iniciadas por las familias de empleados lesionados o fallecidos.
- ☐ Gestionar cualquier acción legal relacionada con los sospechosos.

Equipo de IT

- ☐ Actualizar los sistemas comprometidos según sea necesario.
- ☐ Evaluar todos los daños cibernéticos y de ciberseguridad, incluidos los sistemas comprometidos y la pérdida de activos electrónicos.

Equipo de Asuntos Externos/Comunicaciones

- ☐ Actualizar el sitio web y las redes sociales de la organización con información sobre la recuperación, las medidas de seguridad, las condolencias e información de continuidad del negocio.
- ☐ Organizar eventos conmemorativos en las semanas, meses y años posteriores al incidente, lo que podría incluir la coordinación de un comunicado o conferencia para los medios de comunicación, el personal y los seres queridos de las personas fallecidas.

Equipo de Finanzas/Contratación/Proveedores

- ☐ Dar seguimiento a proveedores y clientes para evaluar las repercusiones en compras o pedidos pendientes (a largo plazo).
- ☐ Trabajar para actualizar todos los contratos, etc., según lo desarrollado en el plan e incorporar las lecciones aprendidas, etc.

ANEXO B: RECURSOS

GUÍA SOBRE AMENAZA DE AGRESOR ACTIVO

Active Shooter Emergency Action Plan Product Suite (CISA): https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

Shields Up! Cyberattack Resources (CISA): https://www.cisa.gov/shields-up

Active Shooter Attacks – Action Guide (CISA): https://www.cisa.gov/resources-tools/resources/active-shooter-attacks-action-guide

Vehicle Ramming – Action Guide (CISA): https://www.cisa.gov/resources-tools/resources/vehicle-ramming-action-guide

Fire as a Weapon – Action Guide (CISA): https://www.cisa.gov/resources-tools/resources/fire-weapon-action-guide

Chemical Attacks – Action Guide (CISA): https://www.cisa.gov/sites/default/files/2022-11/Chemical%20Attacks%20-%20Security%20Awareness%20for%20ST-CP.PDF

Complex Coordinated Attacks – Action Guide (CISA): https://www.cisa.gov/resources-tools/resources/complex-coordinated-attacks-action-guide

Protecting Against the Threat of Unmanned Aircraft Systems (UAS) (CISA Interagency Security Committee [ISC]): https://www.cisa.gov/resources-tools/resources/isc-best-practices-protecting-against-uas-threat

Counter-IED Resources Guide (CISA, Office for Bombing Prevention): https://www.cisa.gov/sites/default/files/publications/obp-counter-ied-resources-guide.pdf

What to Do – Bomb Threat (CISA): https://www.cisa.gov/news-events/news/what-do-bomb-threat

Insider Threat Mitigation (CISA): https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

GUÍAS PARA PLANES DE CONTINUIDAD DEL NEGOCIO

Business Continuity Plan (DHS): https://www.ready.gov/business-continuity-plan

Business Continuity Planning Suite (DHS): https://www.ready.gov/business-continuity-planning-suite

Crisis Communication Plan (DHS): https://www.ready.gov/crisis-communications-plan

RECURSOS DEL PLAN DE ACCIÓN DE EMERGENCIA

Developing Emergency Operations Plans: A Guide for Businesses (FBI): https://www.fbi.gov/file-repository/active-shooter-guide-for-businesses-march-2018.pdf/view

Emergency Action Plan Guide: Active Shooter Preparedness (DHS): https://www.cisa.gov/resources-tools/resources/active-shooter-emergency-action-plan-product-suite

Are You Ready? Basic Preparedness (FEMA): https://www.fema.gov/pdf/areyouready/basic_preparedness.pdf

Evacuation Plans and Procedures eTool (OSHA): https://www.osha.gov/etools/evacuation-plans-procedures/eap

Emergency Response Plan (DHS): https://www.ready.gov/business/implementation/emergency

Incident Management (DHS): https://www.ready.gov/incident-management

ASISTENCIA DE EMERGENCIA Y APOYO A LAS VÍCTIMAS

FBI Victim Services (FBI): https://www.fbi.gov/file-repository/fbi-victim-services-brochure-2018.pdf/view

VictimConnect Resource Services (VictimConnect): https://victimconnect.org/

Disaster Distress Helpline (Substance Abuse and Mental Health Services Administration [SAMHSA]): https://www.samhsa.gov/find-help/disaster-distress-helpline

Antiterrorism and Emergency Assistance Program (OVC): https://ovc.ojp.gov/program/antiterrorism-and-emergency-assistance-program-aeap/overview

National Mass Violence Victimization Resource Center (NMVVRC): https://www.nmvvrc.org/

Technical Resources, Assistance Center, and Information Exchange (TRACIE) (U.S. Department of Health and Human Services [HHS]): https://asprtracie.hhs.gov/technical-resources

Find Treatment (SAMHSA): https://findtreatment.gov/

Find a Health Center (HHS, Health Resources and Services Administration): https://findahealthcenter.hrsa.gov/

Charity and Disaster Fraud (FBI): https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud

RECURSOS DE PREPARACIÓN PERSONAL

Stop The Bleed® (American College of Surgeons): https://www.stopthebleed.org/training/

You Are the Help Until Help Arrives (FEMA): https://community.fema.gov/PreparednessCommunity/s/until-help-arrives?language=en_US

On-Site Group Training for Teams and Employees (American Red Cross): https://www.redcross.org/take-a-class/train-my-employees

Online Safety Training Courses (American Red Cross): https://www.redcross.org/take-a-class/online-safety-classes/all-online-classes

Attacks in Crowded and Public Spaces (DHS): https://www.ready.gov/public-spaces

GUÍAS DE PLANIFICACIÓN DE RESPUESTA Y RECUPERACIÓN

Active Shooter Recovery Guide (DHS): https://www.cisa.gov/resources-tools/resources/active-shooter-recovery-guide

Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide (CISA ISC): https://www.cisa.gov/resources-tools/resources/isc-planning-and-response-active-shooter-guide

Developing and Maintaining Emergency Operations Plans: Comprehensive Preparedness Guide (CPG) 101 (FEMA): https://www.fema.gov/sites/default/files/documents/fema_cpg-101-v3-developing-maintaining-eops.pdf

Physical Security: Insider Threat Mitigation (CISA): https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Violence in the Federal Workplace: A Guide for Prevention and Response (CISA ISC): https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide

Mass Violence and Terrorism Resources (Office for Victims of Crime & Training & Technical Assistance Center): https://www.ovcttac.gov/massviolence/?nm=sfa&ns=mvt&nt=hvmv

Workplace Violence (OSHA): https://www.osha.gov/workplace-violence/enforcement

RECURSOS DEL SECTOR DE SEGURIDAD

Critical Manufacturing Sector Security Guide (CISA): https://www.cisa.gov/sites/default/files/publications/Critical_Manufacturing_Sector_Security_Guide_07012020.pdf

CAPACITACIÓN Y EVALUACIONES DE SEGURIDAD

National Incident Management System (NIMS) (FEMA): https://www.fema.gov/emergency-managers/nims

Independent Study Program (ISP) Course List (FEMA): https://training.fema.gov/is/crslistaspx?lang=en

Insider Risk Mitigation Program Evaluation (IRMPE) (CISA): https://www.cisa.gov/resources-tools/resources/insider-risk-mitigation-program-evaluation-irmpe

Vehicle Ramming Self-Assessment Tool (CISA): https://www.cisa.gov/vehicle-ramming-self-assessment-tool