GUÍA DE LA ADL PARA PROTEGER SU INSTITUCIÓN COMUNITARIA O RELIGIOSA

GUÍA DE LA ADL PARA PROTEGER SU INSTITUCIÓN COMUNITARIA O RELIGIOSA

Liga Antidifamación

Marvin D. Nathan
Presidente Nacional

Jonathan A. Greenblatt
CEO

Kenneth Jacobson
Subdirector Nacional

Steven C. Sheinberg
Jefe de personal
Consejero General
Vicepresidente de Privacidad y Seguridad

Glen S. Lewy
Presidente, Fundación Liga Antidifamación

Deborah M. Lauter
Vicepresidente, Política y Programas

Steven M. Freeman
Subdirector, Política y Programas

Bonnie S. Michelman
Presidente, Seguridad Comunitaria

UNIDAD DE ORDEN PÚBLICO, EXTREMISMO Y SEGURIDAD COMUNITARIA

David C. Friedman
Vicepresidente, Orden Público, Extremismo y Seguridad Comunitaria

Kara K. Chisholm
Director Institucional, Orden Público, Extremismo y Seguridad Comunitaria

Oren Segal
Director, Centro sobre Extremismo

Elise M. Jarvis
Director Asociado de Compromiso con el Orden público y la Seguridad Comunitaria

Para recursos adicionales y actualizados, por favor visite: **www.adl.org**

CONTENIDO

AVISO: Esta guía pretende ayudar a las instituciones a ser conscientes de los temas básicos de seguridad. Esta guía no pretende ser y no constituye una asesoría legal o profesional. No pretende proporcionar asesoría exhaustiva ni específica para una institución en temas de seguridad, pero puede ser utilizada como referencia y guía general para diseñar políticas y procedimientos específicos que puedan ponerse en práctica. Para una asesoría completa y específica sobre seguridad para su institución, se debe consultar a un profesional de seguridad. La Liga Antidifamación no es responsable de ningún daño en que pueda incurrir su organización en relación al uso, no utilización, o uso erróneo de este manual o su contenido.

Nota: La guía ha sido desarrollada para grupos de todos los tamaños y tipos. Como tal, utiliza palabras como "institución", "organización" y "grupo" indistintamente. Igual sucede con palabras como "recinto" "propiedad" e "instalaciones".

INTRODUCCIÓN

La triste realidad es que cualquier institución religiosa o comunitaria puede convertirse en blanco potencial para los extremistas, acabando con su sentido de comodidad y seguridad. Las organizaciones tienen la responsabilidad de hacer todo posible para protegerse a sí mismas y a sus miembros contra potenciales amenazas. La Liga Antidifamación (ADL), una organización de derechos civiles fundada en 1913 para combatir el antisemitismo y todas las formas de odio, ha estado proporcionando asesoría sobre seguridad a las instituciones judías durante décadas. Este manual fue creado para compartir las mejores prácticas de seguridad con otras instituciones religiosas y comunitarias.

Además de la información proporcionada en este manual, la ADL puede ser un recurso para su institución, gracias a nuestra maestría y experiencia como la autoridad no gubernamental más importante de Estados Unidos sobre crímenes de odio, grupos de odio, extremismo, odio cibernético y terrorismo. La ADL trabaja más de cerca con las autoridades que cualquier otra organización privada en Estados Unidos, entrenando entre 10.000 y 15.000 agentes de seguridad federales, estatales y locales cada año en estos temas y áreas, entre otras. El Centro sobre Extremismo de la ADL supervisa y monitorea a los extremistas desde los supremacistas blancos hasta los ciudadanos extremistas islámicos proporcionando a las autoridades información crítica a diario. Con sede en Nueva York y 27 oficinas regionales en el país, la ADL está en condiciones de ayudarle a su institución a responder rápidamente y comunicarse con las autoridades apropiadas en caso de que su organización sea amenazada o atacada.

Ya sea que su organización no haya tenido que enfrentar una amenaza de seguridad significativa en el pasado o que necesite actualizar y ampliar las medidas de seguridad con que cuenta, esta guía le puede ser útil. Fue creada específicamente por los expertos de la ADL para ayudarle a analizar las consideraciones básicas que todas las instituciones deben tener en cuenta.

Esta guía fue escrita teniendo en mente a muchos tipos de organizaciones e instituciones diferentes. Usted puede encontrar que no todos los puntos son relevantes para usted, pero tal vez descubra que muchos de ellos siguen siendo útiles al desarrollar su propio plan de seguridad. Además, lo instamos a compartir esta guía con miembros escogidos de su personal y las directivas de su organización, así como con un profesional de seguridad que pueda evaluar directamente a su institución.

Capítulo 1

PLANIFICACIÓN DE SEGURIDAD

Si usted aún no tiene en marcha un plan general de seguridad, es probable que su organización haya enfrentado los incidentes a medida que se presentaban. Tal vez fue afortunado y la gente adecuada estaba en el lugar indicado para tomar la decisión apropiada y obtener un resultado positivo. Sin embargo, piense cuánto más seguro y más fácil habría sido si hubiese tenido un plan establecido.

Un buen plan de seguridad significa que una institución estará en mejores condiciones para frustrar y, en caso de necesidad, recuperarse de una violación a la seguridad, sea esta un incidente físico o digital.

La planificación de seguridad es un proceso a largo plazo que implica consultas con y entrenamiento de muchos miembros de la comunidad. Aunque ninguna guía puede ofrecer un plan de seguridad para cada institución, hay algunas consideraciones que todas las instituciones deben tener en cuenta. Le rogamos utilizar este documento como punto de partida para una conversación con miembros escogidos de su personal, directivas y un profesional de seguridad que pueda evaluar directamente a su institución.[1]

1 **Una nota importante:** Esta guía pretende ayudar a las instituciones a ser conscientes de los temas básicos de seguridad. No pretende proporcionar asesoría exhaustiva y específica para la institución o eventos en temas de seguridad, ni busca substituir la asesoría de un profesional de seguridad. Para una asesoría completa y específica sobre seguridad para la institución, se debe consultar a un profesional de seguridad. La ADL niega específicamente cualesquiera y toda responsabilidad, y no se hace responsable de ninguna pérdida o daños resultantes del uso, no utilización o uso erróneo de esta información. Además, es crítico el cumplimiento de todos los códigos de seguridad, incluyendo los protocolos contra incendio.

Consideraciones básicas

- No todas las instituciones enfrentan el mismo riesgo, pero todas enfrentan algún riesgo.
- Hacer de la seguridad una prioridad debe ser parte de la cultura de todas nuestras instituciones.
- Al desarrollar un plan de seguridad, sus líderes y los profesionales que trabajan para la organización deben evaluar los riesgos para su organización y sus miembros, así como para las instalaciones físicas, el vecindario y la forma en que se maneja la información. En caso de necesidad, usted debe buscar asesoría profesional.
- Los líderes deben cerciorarse de que la seguridad sea parte de la cultura institucional. Cuando menos, usted debe buscar retroalimentación sobre seguridad de todo su personal, puesto que su participación es esencial para que un plan funcione adecuadamente. Ellos también son sus ojos y oídos fundamentales.
- El personal, los líderes y los miembros de la comunidad deben ser motivados y educados para entender la necesidad de crear y poner en marcha un plan de seguridad.
- Cuando planean o participan en eventos, cada uno —desde el Presidente de la Junta hasta el personal de apoyo— debe pensar en la seguridad.
- Los miembros de la comunidad juegan un importante papel en la seguridad de sus instituciones comunitarias. Los líderes deben ayudarles a entender la importancia del plan de seguridad y de su papel en el mismo. Los miembros de la comunidad deben:
  - — Estar alerta, listos y dispuestos a reportar cualquier actividad sospechosa.
  - — Ser conscientes de sus alrededores.
  - — Reportar cualquier cosa fuera de lugar, desaparecida o que no parece pertenecer al lugar.
  - — Cooperar activamente con las instrucciones, procedimientos y políticas de seguridad.
  - — Compartir ideas y sugerencias sobre seguridad.
  - — Trabajar activamente para crear una cultura que sea segura y acogedora.
  - — Apoyar a los líderes y al personal de la organización cuando tomen la difícil decisión de crear y poner en funcionamiento un plan de seguridad eficaz.

Es importante anotar que crear el plan es tan solo el comienzo del proceso. Una vez esté escrito el plan, es importante cerciorarse de que todos los líderes, empleados y miembros de su comunidad lo conocen y practican los pasos antes de que se presente un acontecimiento. Todos deben repasar el plan con regularidad y recordar ponerlo en práctica continuamente, sin excepción. El entrenamiento regular y la actualización del plan de seguridad son también pasos críticos para la seguridad de su institución.

Creación de un plan de seguridad

Crear un ambiente seguro es un proceso de tres pasos: **evaluación, planeación y puesta en práctica.** Usted puede consultar con la policía local o emplear una empresa profesional de seguridad para que le ayuden en este proceso.

Evaluación

Es de fundamental importancia evaluar la situación actual y entender las posibles amenazas para la organización. Primero, determine los riesgos actuales, luego identifique quién o qué necesita protección contra esos riesgos y, tercero, comience a trabajar con los profesionales para saber qué medidas deben tomarse.

- **Identifique las amenazas**. Primero, usted debe evaluar el peligro para su institución. Aquí presentamos algunas preguntas útiles para que usted pueda identificar las posibles amenazas:
  - ¿Qué le dicen las noticias sobre el ambiente nacional e internacional actual?
  - ¿Qué le dice la policía sobre el ambiente local?
  - ¿Qué dice la oficina regional de la ADL sobre la actividad extremista en su área? (La ADL monitorea y tienen información sobre todo tipo de crímenes por prejuicio y de odio, no solo los relacionados con la comunidad judía.)
- **Identifique qué o quiénes necesitan protección**. Identifique a quién y qué necesita proteger (ej. personas, la propiedad y la información) y entienda qué las hace vulnerables. Tenga presente que usted necesitará estrategias diferentes para proteger a los niños, los adultos, la propiedad y la información; su planeación debe tenerlos en cuenta a todos.

  Observe también que estos blancos a veces están relacionados y lo que afecta a uno también puede afectar a otro. Por ejemplo, una violación de la red que comprometa listas de miembros e información de pagos puede crearles problemas a sus miembros, pero también puede hacerle un gran daño a la reputación de su institución.
- **Relaciones con las autoridades.** Le instamos a reconocer la importancia de desarrollar y mantener una relación cercana con las autoridades locales, así como con otros servicios de emergencia en su área. Como verá en el siguiente capítulo, los profesionales locales pueden proporcionarle información útil y reveladora sobre cómo crear y poner en marcha su plan de seguridad. (Como mínimo, el departamento local de Policía puede tener un oficial de prevención de crímenes que haga una inspección de la seguridad y revise su plan.)

PLANEACIÓN

Reducción del riesgo. Una vez haya identificado las medidas más apropiadas para reducir su riesgo (reconociendo que usted nunca podrá eliminar todo riesgo), comience a poner en marcha el plan tan pronto como pueda. Por ejemplo, el primer paso para mejorar el control de acceso a su oficina o edificio podría ser substituir o cambiar las guardas de sus cerraduras.

Sus tres claves son mando, control y comunicación.

— Identifique un responsable con autoridad para actuar. Cerciórese de que los demás sepan y respeten que él o ella es el responsable.

— Asegúrese de que las decisiones se puedan comunicar eficazmente a quienes deben conocerlas.

— Planee para imprevistos, como en caso de que el responsable asignado no esté disponible durante una emergencia, ya sea porque está enfermo, de vacaciones, almorzando o fuera de la oficina a causa de una reunión. Desarrolle una lista de sucesión o cadena de mando para el caso de una ausencia, incluso si es temporal.

— Todos los presentes, así como las directivas de su organización, deben poder establecer quién es el responsable en un momento dado, ya sea el responsable asignado u otra persona en la cadena de mando.

— Cree un formato simple y de fácil uso para documentar nuevas amenazas. Incluya una lista de control que identifique el tipo de amenaza, la persona que hace esa amenaza y el método utilizado para transmitir la amenaza: teléfono, correo, visita al lugar u otros medios. Deje espacio para comentarios adicionales, tales como identificar características.

— Esta lista de control ayudará a sus empleados cuando hablen con las autoridades, si fuese necesaria una investigación. (Las clínicas para mujeres y las instalaciones en riesgo utilizan este sistema para documentar las amenazas en curso).

- **Planes para diversos usos.** Cree planes que respondan a los diferentes usos dados al edificio. Los días lectivos y acontecimientos de alto tráfico, tales como reuniones de la comunidad, y los días en que no se utilizan las instalaciones producen diferentes circunstancias de seguridad.

- **Recuperación.** Repase los planes y estrategias de recuperación del negocio y todos los seguros. Los planes de recuperación pueden incluir el almacenamiento de información fuera de las instalaciones, listas de proveedores y miembros, y planes para políticas de gobierno corporativo en caso de emergencia.

Medidas de seguridad inmediatas

Hay varias medidas básicas que se deben poner en funcionamiento enseguida, incluso antes de que se termine de desarrollar el plan de seguridad:

- **Examine con frecuencia su edificio.** Usted debe poder determinar rápidamente si algo no está como debe y ayudar a las autoridades si hay un problema.

- **Tenga siempre a disposición todos los teléfonos de emergencia.** Aunque usted siempre debe intentar comunicarse primero con el 911 en cualquier emergencia, también debe tener a la mano el número de teléfono de los servicios de emergencia locales. Además, tenga teléfonos móviles disponibles para llamar a los servicios de emergencia desde fuera de sus instalaciones. *Nota: No utilice teléfonos móviles o radioteléfonos durante una emergencia relacionada con una bomba pues cualquier aparato que usa ondas de radio puede hacer que un dispositivo estalle. (Utilice una línea telefónica fija.)*

- **Utilice los dispositivos de seguridad que ya tiene.** Asegúrese de que los dispositivos de seguridad están encendidos y funcionando, que la iluminación exterior funcione correctamente, que las ventanas y las cercas estén libres de arbustos, y que el acceso a su edificio sea adecuadamente limitado y cumpla con las regulaciones contra incendios.

- **Utilice los recursos disponibles para documentar cualquier comportamiento sospechoso.** Los teléfonos inteligentes, tabletas y otros dispositivos pueden ser extremadamente útiles para tomar fotografías o videos (cuando sea seguro hacerlo) que puede servir a la Policía en caso de individuos o coches sospechosos.

Implementar su plan de seguridad

Implementar un plan de seguridad exige **Responsabilidad, Actualización, Entrenamiento y Construcción de relaciones**.

Responsabilidad

— Asigne a un miembro del personal como encargado de la seguridad, responsable de poner en marcha, revisar y actualizar constantemente el plan de seguridad.

— Cerciórese de que todos están entrenados para poner en marcha el plan, especialmente quienes estarán en primera línea y quienes mejor conocen el edificio, incluyendo el personal de mantenimiento.

— Asegúrese de que el encargado de la seguridad sea un directivo responsable y organizado, que tenga suficiente tiempo para cumplir con sus responsabilidades de seguridad, especialmente al asumir el cargo. A menudo, el encargado de la seguridad no tiene ninguna experiencia en seguridad y tendrá que asumir un gran compromiso de aprendizaje y dedicación. Esta persona es responsable de entrenar continuamente y actualizar el plan.

- **Actualizar regularmente los planes y procedimientos.** Un plan de la seguridad debe ser evaluado y actualizado constantemente. Un plan obsoleto no es mejor que —y puede ser peor— no tener un plan.

- **Entrenamiento.** Realice con la comunidad y el personal ejercicios de entrenamiento, simulacros y juegos de rol. Los simulacros y juegos de rol garantizan que el plan sea aplicable, actualizado y esté fresco en la mente de la gente.

  — Los ejercicios basados en discusiones, incluyendo sesiones de orientación, talleres y simulacros conceptuales, familiarizan al personal y miembros de la comunidad con sus diversos procedimientos de seguridad. En los simulacros conceptuales, se presenta a los equipos involucrados un escenario de crisis. Los roles y responsabilidades específicas son revisados y una discusión en profundidad, constructiva, de resolución del problema lleva al equipo a través del escenario para poder identificar y resolver problemas potenciales.

  — Procedimientos o protocolos específicos de la práctica de simulacros de emergencia. El objetivo es garantizar que todos los posibles participantes sepan lo que deben hacer en una emergencia.

  — Los ejercicios funcionales simulan situaciones de emergencia. Son ejercicios que tienen en cuenta el factor tiempo, eventos interactivos en los cuales los participantes reciben instrucciones de un orientador y responden apropiadamente (como si realmente hubiese una situación de emergencia). Posteriormente, el ejercicio es analizado y se hacen recomendaciones para mejorar la seguridad y los procedimientos de respuesta.

- **Establecer relaciones**. Establezca relaciones con los servicios de emergencia locales en cada etapa de la planeación de seguridad. (Más sobre esto en el siguiente capítulo.)

Capítulo 2

ESTABLECER RELACIONES CON LOS SERVICIOS DE EMERGENCIA

Su organización puede tener ya un contacto en la Policía o el cuerpo de Bomberos, pero muchos grupos todavía no han construido una buena relación con las autoridades locales. Es importante pedirles ayuda a las autoridades y el personal de emergencia para la planeación e implementación de un plan de seguridad. Y tanto la Policía como los Bomberos saben que involucrarlos en su proceso de planeación también es una gran ventaja para ellos en caso de haber una emergencia que deben atender.

No hay exageración al decir que desarrollar relaciones con sus servicios locales de emergencia aumentará la seguridad de su institución. Este es un componente fundamental para cualquier programa de seguridad efectivo.

Las siguientes son sugerencias sobre cómo establecer relaciones con sus servicios locales de emergencia. En muchos casos, su oficina regional de la ADL puede facilitar dichas relaciones.

Conózcanse

La comunicación es la clave para una relación exitosa con las autoridades y trabajar con ellas realzará su capacidad de responder a sus necesidades. Es importante reconocer el extraordinario servicio que todos estos individuos prestan a nuestras comunidades y ser conscientes de su disponibilidad de tiempo y otros compromisos. Usted tiene que demostrar que no sólo está pidiendo ayuda sino que también apoya sus esfuerzos y es un participante activo en su propia seguridad.

- **Invite al personal de la policía, bomberos y otros servicios de emergencia a que visiten su edificio u oficina** y puedan familiarizarse con las instalaciones, el personal y las operaciones de rutina. Esto no sólo puede proporcionar información útil a todas las partes, sino que también ayudará a comenzar a construir una relación con quienes se ocuparían de un incidente en sus instalaciones. El peor momento para conocer a sus oficiales locales por primera vez, es durante una crisis.

- **Comparta los modelos y planos de su edificación** con todos los servicios de emergencia locales. Si están poco dispuestos o no pueden guardarlos en archivo, considere la opción de tenerlos almacenados en un lugar cercano y seguro para tener acceso a ellos rápidamente durante una emergencia.

- **Averigüe con los servicios de emergencia qué otra información podrían necesitar y dónde creen que debe almacenarse.**

- **Cree un plan "de ayuda" que provea a los servicios de emergencia la información que pueden necesitar.** Incluya otra copia de sus planos e información sobre dónde se encuentran los activos importantes.

- **Si sus instalaciones cuentan con un gimnasio o un área similar de entretenimiento,** usted podría invitar a los oficiales de policía y bomberos a utilizarlo.
- **También puede invitar a los funcionarios locales de emergencias a que se reúnan con su personal para diversas actividades:** un servicio religioso semanal, festivales, celebraciones, acontecimientos especiales y reuniones de la comunidad.

Las autoridades

- **Invite a un representante del departamento de Policía a su reunión inicial de planeación de seguridad**. Comparta sus preocupaciones específicas y pida sugerencias sobre cómo comunicarse durante una emergencia, crear planes de evacuación, etc.
- **Para eventos especiales (incluyendo festividades religiosas), informe al departamento local de Policía sobre los horarios y naturaleza del acontecimiento.** También es útil avisarles los horarios en que la gente estará ingresando y saliendo a pie o en coche de su institución.
- **Si su departamento local tiene un equipo especial de armas y táctica (SWAT),** considere la posibilidad de que un oficial del SWAT mapee su institución y sus instalaciones para determinar qué información sería provechosa en caso de ser necesario desplegar un equipo SWAT.
- **Pida a un miembro de la brigada de explosivos que dé una charla a su personal.** Esta también sería una buena oportunidad para consultar con la brigada de explosivos qué información necesitan para ser eficaces. Es posible que necesite consultar con su departamento local de Policía para tener acceso a la brigada de explosivos.
- **Si es apropiado, considere la opción de ofrecer su sitio como espacio de entrenamiento para el SWAT o la brigada de explosivos.**

Tenga en cuenta que las funciones de los oficiales tienden a cambiar con cierta regularidad; cerciórese de estar informado de los cambios de personal y responsabilidades en las fuerzas del orden. Cuando haya cambios, comience a establecer relaciones tan pronto pueda y recuerde mantenerlas siempre frescas y vitales.

Cuerpo de Bomberos

- **Reúnase con los bomberos locales y con un miembro del equipo de incendios provocados.**

- **Pídales revisar sus instalaciones y sus planes contra incendio**. Una vez se aplique cualesquier sugerencia o revisión a sus planes, recuerde poner al día sus planes de ayuda y compartirlos con todos los servicios de emergencia.

- **Reúnase con su técnico local de emergencias médicas (EMT)** para que le ayude a crear un plan de emergencia médica. Además, tal vez quiera considerar la posibilidad de que su personal tenga entrenamiento en primeros auxilios y RCP. Como mínimo, deberá tener un kit de emergencias médicas (o varios) a la mano, así como un desfibrilador externo automatizado (AED, por sus siglas en inglés).

Capítulo 3

SECURIDAD FÍSICA

La seguridad física comienza con una premisa básica: quienes no pertenecen a la institución deben ser excluidos de ella. Hay tres maneras frecuentemente relacionadas con las cuales se implementa esta premisa básica:

1. Cuando quienes no pertenecen son identificados, detenidos y la admisión es negada por una persona.

2. Cuando quienes no pertenecen tienen la admisión negada por un dispositivo físico, tal como una puerta cerrada.

3. Cuando quienes no pertenecen son disuadidos de ingresar a sus premisas porque deciden que es demasiado difícil entrar y volver a salir voluntariamente.

Hay una serie de elementos relacionados con la seguridad física. Entre ellos:

Control del acceso

El control de acceso es esencial en sus planes de seguridad ya que significa que cuando las instalaciones u oficina están abiertas, ningún visitante, proveedor, personal de servicios o individuo desconocido puede ingresar sin ser directa o indirectamente observado y autorizado. Su plan de seguridad debe desarrollar y poner en práctica políticas para asegurarse de que la vigilancia es permanente, de manera que nadie ingrese al edificio sin ser detectado.

Es importante que estos sistemas formen parte de la cultura de su institución. Una cultura que promueve la conciencia de la seguridad permite al personal y visitantes entender que las pequeñas incomodidades puedan traducirse en importantes beneficios de seguridad.

Hay muchas maneras de realizar la vigilancia con recursos humanos, como porteros, voluntarios, personal pagado, guardias de seguridad empleados, etc., o dispositivos electrónicos. La instalación de circuitos cerrados de TV, intercomunicadores y puertas eléctricas puede ayudar significativamente al proceso de vigilancia y control.

Algunas tácticas clave para el control de acceso son:

- **Reduzca al mínimo el número de entradas abiertas a sus instalaciones** (sin infringir la reglamentación de incendios).

- **Vigile las entradas**. Es más fácil evitar la entrada de alguien a su edificio que lograr que alguien se vaya. Idealmente, una institución u oficina debe tener una sola entrada que sea vigilada por un empleado y que esté equipada con un intercomunicador para comunicarse con cualquier persona que se acerque a la puerta. También se puede considerar la posibilidad de colocar barreras externas y mantener la puerta siempre cerrada.
- **Tenga siempre un puesto de seguridad con personal.** Establezca un puesto protegido de seguridad en el vestíbulo principal de cada edificio u oficina con acceso abierto o una política de puertas abiertas. Utilice un libro de registro de entrada y salida, y que el vigilante verifique las credenciales de todo el que ingresa (véase abajo).
- **Verifique las credenciales.** Antes de permitir que los individuos ingresen a sus instalaciones u oficinas, compruebe que sus documentos de identificación u otras credenciales, incluyendo carnets de socio, sean válidos. Es perfectamente legítimo pedir un documento de identificación con foto. Algunas palabras de advertencia:

  — Los empleados no siempre pueden conocer la diferencia entre los documentos válidos y los falsificados. La Policía y la mayoría de los empleados de servicios públicos tienen credenciales, pero el personal puede no ser capaz de distinguir entre los documentos verdaderos y los falsos.

  — Comprar un uniforme o el equipo que distingue al personal de servicios públicos es muy fácil y le permite a un intruso fingir que tienen motivos legítimos para ingresar al lugar.

  — Vale la pena gastar unos minutos en comunicarse con la compañía o la organización apropiada para determinar la legitimidad de la persona que solicita autorización para entrar. Nunca se avergüence por pedir una mejor identificación o por pedirle a una persona que espere hasta que se compruebe su identidad. Cualquier individuo que se agite o enoje ante tal petición, debe ser considerado de cuestionable legitimidad.
- **Utilice identificaciones con fotografía.** Todos los empleados de la institución u organización deben tener un carnet de identificación que permita distinguir de inmediato a los no empleados y resolver dudas de identidad. Si es apropiado, usted puede emitir carnets de identificación con foto para los miembros de la organización.

  — Se debe exigir a todos los empleados usar su documento de identificación con foto en lugar visible mientras se encuentren en el edificio y, para su propia seguridad, guardarlo cuando estén fuera del edificio. Eso con el fin de prevenir hurtos. Además, no hay razón para que cualquier persona en la calle o transporte público pueda identificar quién es alguien y dónde trabaja.

  — El carnet de identificación no debe ser entregado sin el acompañamiento de información sobre su cuidado, incluyendo los procedimientos a seguir si se pierde y la forma en que los empleados deben acercarse a individuos desconocidos.

  — El uso de carnets de identificación exige cuidado. Deben tener fotografías claras, junto al nombre del empleado. Cada institución debe decidir si su nombre se incluye en el carnet.

— Los carnets perdidos deben reportarse inmediatamente.

- **Supervise a los visitantes después de que ingresan**. Nunca se debe permitir a los visitantes vagar libremente por las instalaciones. Deben ir acompañados o ser observados. Se debe tener especial cuidado con los individuos que trabajan en los sistemas más sensibles de la organización, tales como alarmas contra robo, alarmas de incendio, sistemas de comunicación o computadoras. En instituciones más grandes, ciertas áreas deben ser restringidas a todos a excepción del personal autorizado.
- **Identifique claramente las zonas de libre acceso.** Los centros comunitarios para jóvenes y ancianos, las instalaciones con gimnasios y otras instituciones similares buscan mantener el libre acceso a esas áreas. Pero, permitir a los visitantes el acceso libre a esa zona de sus instalaciones no significa que puedan andar por dondequiera. El final de las áreas de libre acceso debe estar debidamente señalizado, al igual que las áreas restringidas o las oficinas. Los visitantes deben percibir que el personal de la institución está pendiente de ellos y sus acciones.
- **Evite los rezagados.** Los procedimientos de cierre al final del día deben incluir una revisión visual de todas las áreas de la institución para evitar ladrones rezagados u otros dispuestos a hacer daño de alguna manera.

Control de las llaves

La frase control de las llaves se refiere a todos los tipos de acceso a edificios, oficinas y espacios individuales (cerraduras específicas, accesos con tarjeta y conocimiento de los códigos de las alarmas). Una política de control de llaves es esencial para un buen programa de seguridad. No hacer un seguimiento constante a quienes tienen la posibilidad de acceder a las áreas restringidas por sí mismos puede convertirse en un problema y convertir un sistema de seguridad en un fracaso. Recuerde que los ex empleados o voluntarios contrariados pueden meterse a un edificio para robar o dañar de otra manera a su organización.

- **Lleve un registro.** Se debe establecer un registro central de control de llaves para todas las llaves y combinaciones. Los empleados y líderes de la organización deben firmarlo. Devolver las llaves debe ser parte de la entrega de un cargo.
- **Tenga un proceso de aprobación para ello.** La aprobación de un supervisor debe ser requisito para la entrega de llaves y candados. Las llaves y candados de repuesto se deben mantener en un gabinete cerrado y centralizado, supervisado por un empleado. Las llaves maestras deben entregarse a un número restringido de empleados y se deben revisar por lo menos dos veces cada una.
- **Considere la posibilidad de cambiar las guardas.** Cuando el acceso a llaves, a tarjetas, etc. no es

correctamente controlado o se pierden llaves y tarjetas, cambiar las cerraduras de la institución o los lectores de acceso pueden ser una buena medida.

- **Cambie las combinaciones y los códigos de las cerraduras regularmente.** Cuando se utilizan cerraduras o candados con clave, las combinaciones y claves se deben cambiar por lo menos cada seis meses o cuando se retiran empleados o directivos. Las claves deben ser estrictamente controladas por la administración.
- **Utilice cerraduras cuyas llaves no puedan ser duplicadas fácilmente.** Es una buena política utilizar cerraduras que requieran special key blanks para hacer llaves adicionales.
- **Evalúe la posibilidad de instalar lectores de tarjetas.** Aunque son costosos, los lectores de tarjetas facilitan el control de acceso y son casi automáticos. Las instituciones grandes, o aquellas con activos valiosos, pueden encontrar justificada la inversión porque pueden controlar y hacer seguimiento a quién entra y sale de cuartos específicos en cualquier momento.

Cerraduras

Unas cerraduras durables son esenciales para la seguridad del edificio. Recomendamos consultar con un cerrajero experimentado que pueda determinar las circunstancias de su institución y ofrecer recomendaciones específicas. La siguiente información puede servir para comenzar la discusión con un profesional:

- **Las cerraduras de seguridad son más confiables.** Deben entrar por lo menos una pulgada en el marco de la puerta y ser apropiadas para el tipo de marco (madera vs. metal).
- **Los candados** deben ser de un material de alta calidad, diseñado para resistir el abuso y los intentos para forzarlos.
- **Los cilindros de las cerraduras y candados** deben ser altamente resistentes.
- **El sistema de cierre de las puertas debe cumplir con los códigos de seguridad e incendio para permitir la evacuación de emergencia sin ser impedimento.** Es importante mantenerse al corriente de cualquier cambio en las leyes locales.
- **La jamba de la puerta** debe ser suficientemente fuerte, puesto que una cerradura fuerte penetrando en una jamba débil no serviría de nada.
- **Los cilindros de las cerraduras de las puertas exteriores deben estar protegidos con placas de metal o armored rings para evitar que sean retirados.** Las placas protectoras de metal deben estar aseguradas con tornillos de seguridad de cabeza redonda. Algunos cilindros muy resistentes a ataques tienen una platina de metal a su alrededor.
- **Las cerraduras con cilindros individuales y interior thumb turns instaladas en puertas con paneles de vidrio deben colocarse a más de 36 pulgadas del panel de vidrio más cercano.**

- **Cierres automáticos**. Las puertas que se cierran con sistemas de aire, hidráulicos o resortes deben ser revisadas periódicamente para asegurarse de que vuelven a la posición completamente cerrada o bloqueada.
- **La administración de las cerraduras es de fundamental importancia.** El encargado de seguridad de la institución o un empleado asignado y entrenado debe:
  - Revisar y reportar regularmente todas las cerraduras dañadas y asegurarse de que sean reparadas rápidamente.
  - Establecer una cadena de responsabilidad para todas las cerraduras de puertas y ventanas para asegurar que estén cerradas. Esta responsabilidad debe incluir informar sobre todos los casos en que no se cumpla la norma.
  - Asegurarse de que las llaves no sean descuidadas.
  - Recomendar la instalación de cerraduras adicionales cuando sea necesario.
  - Incluir el programa de control de llaves en la auditoría de seguridad periódica. Recuerde examinar todas las cerraduras. Además de las cerraduras exteriores en las instalaciones, debe haber cerraduras en puertas, ventanas, oficinas, archivos y armarios interiores.

Dispositivos, alarmas y tecnología de seguridad

Los dispositivos protectores son una consideración importante para fortalecer la seguridad. Incluyen detección de intrusos y fuego y sistemas de alarma, así como cámaras conectadas a un circuito cerrado de TV (CCTV, por sus siglas en inglés). Pueden ser costosos y hay una amplia variedad de modelos, fabricantes y características para elegir, por ello la selección, especificaciones e instalación requieren asesoría profesional.

Usted deseará comenzar por comunicarse con las autoridades y pedirles ayuda de la unidad que se especializa en la prevención de crímenes/robos, ya que sus oficiales están especialmente entrenados y pueden darle una asesoría experta. Además, los administradores de las instalaciones, miembros del comité de construcción del edificio, arquitectos e ingenieros licenciados, así como respetados e, idealmente, certificados consultores de seguridad pueden ayudarle en la selección de una tecnología apropiada y dispositivos protectores. En última instancia, el administrador de las instalaciones debe entender cómo utilizar y mantener el sistema y asegurarse de que cualquiera que sea la tecnología cumpla con las tareas necesarias para mantener segura la propiedad.

Presentamos algunas pautas que pueden resultar provechosas para fomentar la discusión con los expertos que consulte o para renovar el equipo existente:

Sistemas de alarma

Como las cerraduras, los sistemas de alarma requieren asesoría de un profesional. El tamaño, la ubicación y el tipo de institución determinarán el tipo de sistema requerido, pero aquí presentamos algunas pautas iniciales para instalar y mantener las alarmas:

- Asegúrese de que el sistema de alarma cumple los requisitos legales locales.
- Determine si la ciudad permite la marcación directa a la Policía cuando una alarma se activa.
- Asegúrese de que todos los sistemas de alarma tengan fuentes de energía de reserva para emergencias.
- Esconda la caja de control de la alarma y límite el acceso a ella.
- Seleccione un sistema con un circuito electrónico de retraso de 30 segundos.
- Asegúrese de que la alarma se escucha en toda la propiedad.
- Contrate una compañía de monitoreo de alarmas centrales.
- Proteja todos los cables, componentes y sirenas contra cualquier manipulación.
- Pruebe el sistema de alarma con frecuencia para garantizar su eficacia.
- Fije en las ventanas y entradas y salidas etiquetas adhesivas anunciando la existencia de la alarma.
- Enseñe al personal y líderes de la organización cómo utilizar el equipo y trabajar con la compañía de monitoreo.
- Considere la opción de agregar botones de pánico al sistema, de manera que sea posible activar la alarma desde lugares diferentes al panel principal de la misma. Colóquelos en oficinas clave, espacios utilizados durante las horas libres y en sitios en donde sea más factible encontrar intrusos, como por ejemplo las áreas de la recepción.
- Evalúe también la conveniencia de usar alarmas personales o portátiles. Estas emiten un fuerte sonido de advertencia que alerta a otras personas y las guía al lugar donde es necesaria la ayuda.
- Los detectores de movimiento o sensores automáticos que responden al sonido son excelentes dispositivos de seguridad, usados solos o conjuntamente con su sistema de iluminación. Estos detectores y sensores son económicos y se pueden utilizar dentro o fuera del edificio.
- Las alarmas que usan contactos magnéticos y cables trampa también son eficaces y económicas, pero las alarmas con detectores de movimiento, sonido o luz son generalmente más confiables. El costo de invertir en un sistema de alarma confiable es generalmente menor que el de los daños causados por un intruso.

Sistemas de CCTV (circuito cerrado de TV)

Las cámaras de vigilancia pueden documentar los actos criminales que ocurren en su propiedad y posteriormente pueden utilizarse para identificar y procesar a los responsables. También pueden servir para disuadir a los potenciales intrusos. Aunque los costos iniciales suelen ser altos, a largo plazo, las cámaras y el equipo de grabación son económicos si se los compara con los costos de posibles pérdidas o daños al personal y miembros del grupo.

- Para ser eficaces, los sistemas de CCTV deben ser correctamente mantenidos y supervisados. La gente responsable de supervisar o repasar el vídeo debe estar bien entrenada y concentrarse. Las distracciones se deben reducir al mínimo o eliminarse totalmente si es posible.
- La mayoría de las instituciones probablemente no tienen los recursos para una supervisión continua, pero la mayoría de los sistemas hoy día tienen la capacidad de almacenar video lo cual permite a las instituciones revisar y repasarlos después de los hechos.
- Utilice lentes gran angular para vigilar las entradas.
- Utilice cámaras con iluminación infrarroja para mejorar los vídeos nocturnos.
- Junte las cámaras con una grabadora de intervalos de tiempo para los expedientes permanentes.
- Cerciórese de que las cámaras registran la hora y fecha.
- Compare el costo de color contra blanco y negro, y determine la relación costo/beneficio basado en las necesidades de seguridad de su organización.
- Archive la grabación durante mínimo 72 horas si se observa algún comportamiento sospechoso. Con frecuencia vale la pena archivar la grabación indefinidamente en caso de que la Policía o los juzgados la necesiten como evidencia.
- Sopese la conveniencia de cambiar las cámaras más viejas por modelos más nuevos de alta-definición.

Al renovar, actualizar o modificar las instalaciones existentes (y especialmente al diseñar nuevas instalaciones), se debe consultar a un arquitecto y un ingeniero licenciados para los temas de seguridad. Usted querrá que los profesionales recomienden los materiales apropiados, específicos, que cumplan las normas (de seguridad local, construcción e incendios) para las ventanas, puertas, verjas, claraboyas y otros materiales de construcción. Las mejores prácticas para las mejoras físicas de este tipo son:

Puertas

- Todas las puertas exteriores, puertas principales del edificio y puertas de vestíbulos que conducen a pasillos comunes deben cumplir varios criterios importantes.
  - Las puertas sólidas, de madera o metal, son aceptables, dependiendo de los requisitos del código.
  - Las puertas de paneles de vidrio o los paneles laterales de vidrio deben estar reforzados con metal o acero o ser substituidos por vidrio inastillable.
- Se deben instalar cerca a las puertas y ventanas de vidrio sensores que detecten el rompimiento del mismo.
- Es conveniente que programe una prueba anual de los sensores con su proveedor de alarmas.
- Los marcos de las puertas deben ser fuertes y apropiados para el tipo de puerta. Los marcos débiles deben ser substituidos o reconstruidos.
- Las cerraduras de las puertas exteriores deben cumplir las pautas mencionadas en la sección sobre cerraduras.
- Las puertas interiores o de las oficinas deben estar equipadas con cerrojos resistentes, escopleados, y de alta seguridad.
- Las puertas con bisagras externas o a la vista pueden ser víctimas de la remoción del perno central. El perno de la bisagra debe fijarse con soldadura de punto u otros medios, o las bisagras deben ser selladas para prevenir la separación. Tales salidas deben tener alarma y utilizarse solamente en casos de emergencia.
- El personal no debe salir por las puertas traseras que conducen a callejones o a calles poco transitadas.
- Las puertas de los armarios de servicios públicos deben tener cerraduras de seguridad y permanecer siempre cerradas. Si no es así, tales armarios pueden convertirse en escondites para criminales rezagados o dispositivos explosivos.
- Todas las puertas exteriores sin paneles de vidrio deben tener una mirilla (u ojo mágico) ubicado a una altura accesible para los individuos altos y bajos.
- Las puertas interiores en las escaleras y pasillos deben tener visibilidad de dos vías. Debe haber una vista clara del interior de las habitaciones desde el umbral.
- El acceso a las oficinas y cocinas, así como a cuartos eléctricos, mecánicos y de almacenaje, debe estar limitado al personal apropiado y deben permanecer cerrados si no están en uso.

Ventanas

Las ventanas deben proporcionar luz, ventilación y visibilidad, pero no fácil acceso para los intrusos.

- Los bloques de vidrio ofrecen una continua fuente de luz a la vez que aumentan la seguridad (aunque la visibilidad y ventilación disminuyen).
- Las rejas y las pantallas expandidas de acero son poco atractivas pero proporcionan un alto grado de seguridad. Se deben consultar los códigos locales de construcción con respecto a la colocación de bloques o pantallas en los pasillos clasificados como resistentes al fuego, en vías de salida o restricciones de ocupación del edificio para garantizar el cumplimiento de las clasificaciones aplicables de incendio.
- Las claraboyas, el acceso a la azotea, los ventiladores y los grandes travesaños de las puertas pueden facilitar el acceso a los intrusos a menos que estén adecuadamente protegidos. Si no es posible sellarlos permanente, puede ser necesario recurrir a varillas de acero o pantallas expandidas de acero, si la reglamentación de incendios las permiten.
- Una nota crucial sobre el vidrio: en una explosión, el vidrio que vuela puede ser tan peligroso como la explosión misma. Considere substituir el vidrio tradicional por vidrios de seguridad o vidrio inastillable, o utilizar una película protectora transparente para asegurar el vidrio al marco.

Elementos del diseño ambiental (CPTED, por sus siglas en inglés)

Los principios de planeación de la prevención del crimen a través del diseño ambiental (CPTED) incluyen el uso de cercas, características naturales del sitio e iluminación del perímetro, por ser formas relativamente baratas y poco sofisticadas de reducir los problemas y mejorar la seguridad.

Todas las barreras físicas utilizadas en una institución deben ser compatibles con la estética del vecindario o el ambiente circundante. Usted debe esforzarse por evitar enajenar a los vecinos, que pueden ser parte de un sistema de vigilancia de la vecindad y proporcionan ojos y oídos adicionales al programa general de seguridad.

Además, al igual que con muchas de las otras medidas de seguridad mencionadas en este libro, usted debe consultar con un profesional de seguridad, arquitecto licenciado o un ingeniero al instalar elementos de CPTED.

Cercas y paredes de seguridad

Una cerca dificulta al intruso el ingreso y da la sensación de una institución segura. Como cuando evalúa cualquier elemento protector, antes de planear, diseñar y construir, usted debe consultar los códigos de construcción y zonificación locales con respecto a la instalación de cercas. En general:

- Las cercas ornamentales abiertas, a diferencia de las paredes, no bloquean la visibilidad, son menos susceptibles a los grafiti y más difíciles de escalar.
- Las cercas deben tener por lo menos seis pies de alto. Aproveche cualquier pendiente o colina al decidir dónde construir la cerca.
- Las cercas se deben diseñar para evitar que una persona meta la mano o un alambre para abrir la puerta desde el exterior.
- Si se requiere una barra anti-pánico para la salida de emergencia, se debe utilizar un protector sólido de metal o plástico en la parte interior de la puerta de la cerca.
- En lugar de cercas, se deben construir paredes allí donde hay una necesidad de privacidad y control del ruido.

Paisajismo

El paisajismo y la basura a lo largo de las cercas, los costados del edificio o cerca a los sitios de entrada podrían ocultar la actividad criminal o, incluso, ayudar a un intruso.

- Mantenga los arbustos bajos (menos de 36 pulgadas) o elimínelos totalmente.
- Despeje los árboles y enredaderas que podrían ayudar a alguien a trepar.

Nota: Crear una barrera física impenetrable, incluso una protegida por personal de seguridad, es difícil; cuando la gente está fatigada, distraída o aburrida puede cometer errores.

Iluminación de seguridad

Una iluminación adecuada es una rentable forma de prevenir crímenes. Es sabio incluir en sus discusiones de planeación a un consultor en iluminación para determinar las ubicaciones y el mejor tipo de luces para cada sitio.

- Todas las entradas y cercas deben estar bien iluminadas.
- La iluminación debe ser constante y uniforme para reducir el contraste entre las sombras y las áreas iluminadas, especialmente en las calzadas, entradas, salidas y zonas de estacionamiento.
- Las luces deben estar dirigidas hacia abajo, no al edificio o área que se busca proteger y lejos del personal de seguridad que vigila el recinto.
- El nivel recomendado de luz es uno que sea igual a la luz del día.
- Al mismo tiempo, es importante ser considerado con la gente que está alrededor de su institución. Se puede tener una iluminación interior y exterior adecuada sin ser invasivo con los vecinos.
- Los accesorios de la iluminación deben ser resistentes al vandalismo. Repare y substituya inmediatamente los bombillos defectuosos o gastados.
- Cuando utilice cercas, la iluminación debe estar adentro y sobre la cerca para iluminarla tanto como sea posible. Asegúrese también de que los árboles y arbustos no estén bloqueando los accesorios de la iluminación.
- Las luces perimetrales deben ser instaladas de manera que los conos de iluminación se sobrepongan, eliminando las áreas de oscuridad total si alguna lámpara no se enciende.
- Los temporizadores y las celdas fotoeléctricas automáticas protegen contra los errores humanos y garantizan el funcionamiento durante un clima inclemente, aun cuando el edificio esté desocupado.

Capítulo 4

DETECTAR LA VIGILANCIA

Muchas organizaciones o terroristas individuales que buscan hacer daño a alguien o a un grupo se dedican primero a vigilar a sus víctimas potenciales. Es importante mantenerse alerta y prestar atención a cualquier persona que intente tomar fotografías, grabar videos o estudiar sus instalaciones especialmente en los días y semanas antes de un evento especial.

A quién observar

Sea cauteloso con cualquiera que:

- Tome datos sobre su institución ya sea dibujando, tomando notas, grabando o tomando fotografías.
- Permanezca sentado en un vehículo por un período extendido, incluso después de las horas de oficina.
- Holgazanee cerca de su recinto o en el vestíbulo del edificio u oficina.
- Llegue a sus instalaciones y se presente como obrero sin notificación previa (pueden asegurar que son contratistas o técnicos del servicio, etc.).
- Exija entregar paquetes u otros artículos a una oficina o persona específica.
- Procure evitar su seguridad, incluso accidentalmente (pasar de largo frente a la recepción o recepcionista).
- Parezca medir distancias o trazar un plano de su edificio.
- Se rehúse a cooperar o tenga una actitud desdeñosa.
- Finja no entender lo que usted le dice cuando lo cuestiona sobre su presencia en las instalaciones.

Cuando alguien es señalado como sospechoso

Si usted detecta a alguien que parece estar vigilando su organización, preste atención a los detalles. Lo que para usted puede parecer de poca importancia, puede ser importante para las autoridades o su empresa de seguridad.

Llame a la Policía inmediatamente

Es crucial que el operador del 911 reciba *toda* la información disponible.

- Proporcione su dirección y la localización exacta del incidente que le preocupa (área de recepción, oficinas de la dirección, gimnasio, etc.).
- Otra información importante que debe reportar es una descripción del individuo sospechoso:
  - Género
  - Altura y peso aproximados
  - Vestimenta
  - Tipo de coche y placas, si se ven
  - Cualquier característica inusual que haga a la persona o personas más fáciles de identificar
- Este es uno de esos casos en los cuales tener buenas relaciones con la Policía puede ser de gran ayuda. Además de llamar al 911, intente hablar con uno de sus contactos.
- Si un operador del 911 no considera que su situación es una emergencia, infórmele si se siente amenazado y requiere ayuda inmediata. Si el oficial que responde se rehúsa a tomar un informe, llame a la ADL.

Reúna pruebas de sus sospechas

Teniendo en cuenta su seguridad y nivel personal de comodidad:

- Considere la opción de fotografiar a la persona que lo vigila. Anime al personal a tomar fotos o vídeos del individuo con una cámara fotográfica o un teléfono inteligente, siempre y cuando hacerlo no los coloque en una posición incómoda o peligrosa.
- Si su institución tiene un sistema de vigilancia que pueda ser supervisado o revisado, cerciórese de que la persona responsable de esa función sepa qué buscar y consiga la grabación del incidente.
- Si la persona sospechosa decide irse antes de que llegue la Policía, usted puede elegir acercarse al individuo y averiguar por qué está tomando fotografías del recinto, anotando medidas o actuando de otra manera que usted encuentra sospechosa.
- Aunque la persona puede desdeñar su pregunta (No es su problema o Puedo tomar fotos de lo que me

provoque [2], por ejemplo) usted le habrá dejado claro que sus acciones no pasaron desapercibidas.

- Aunque la persona se vaya, la Policía debe recibir un informe completo. Asegúrese de que sus líderes y empleados conozcan todos los detalles relevantes sobre el incidente, para que puedan identificar a el/los sospechoso si regresa.

2 Esto aplica, a menos que la persona esté violando la propiedad.

Capítulo 5

CORRESPONDENCIA Y PROTOCOLOS DE ENTREGA

La seguridad del correo y los paquetes también es esencial, sin importar el tamaño de su organización o institución. Es fundamental que tenga dispositivos de seguridad para prevenir o manejar con éxito el correo y los paquetes sospechosos. Al igual que con otras medidas de seguridad, su primer paso es desarrollar un plan de respuesta ante correo peligroso .

La clave es pasar todo el correo y paquetes por un proceso de revisión, sin importar cómo fueron entregados. Su objetivo es asegurarse de que toda carta y paquete se someta a un escrutinio formal. Esto incluye todo lo recibido del servicio postal, servicios de mensajería e individuos no reconocidos por quien recibe un paquete.

Desarrolle un sistema

1. **Realice una evaluación de vulnerabilidad para determinar si su organización o un empleado en particular es un blanco potencial.** Recuerde que siempre es mejor pecar por exceso de precaución.
2. **Desarrolle procedimientos específicos de revisión e inspección para todo el correo entrante o paquetes recibidos.** Como mínimo, asegúrese de que todo el correo y paquetes sean examinados por alguien entrenado para evaluarlos.
3. **Designe un coordinador de seguridad para el área de correspondencia y alguien que lo respalde.** Ellos serán responsables de implementar el plan y asegurarse de que todos los empleados lo cumplan.
4. **Establezca líneas directas de notificación y comunicación entre el coordinador de seguridad del área de correspondencia, la gerencia y su oficina general de seguridad si la tiene.**
5. **Realice sesiones de entrenamiento:**

   - Para el área de correspondencia y personal de seguridad y administrativo, para asegurarse de que todas las fases de un programa de detección de explosivos en el correo funcionen correctamente. •
   - Para que todos los empleados y voluntarios estén alerta ante el correo y paquetes sospechosos.

En qué fijarse

- Exceso de franqueo o cinta adhesiva.
- Palabras mal escritas o con mala ortografía.
- Destinatarios inusuales, tales como el uso del cargo sin un nombre (ej. Presidente) o el uso incorrecto de los cargos.
- Ausencia de dirección del remitente o una dirección sospechosa.

- Empaque rígido, voluminoso o desequilibrado.
- Manchas de grasa en el empaque o un olor extraño.
- Cables que sobresalen.
  Polvo no reconocible o substancias sospechosas.

Qué hacer si encuentra algo sospechoso

Desarrolle técnicas y procedimientos específicos para el manejo de la correspondencia identificada como sospechosa y peligrosa.

1. **Tenga procedimientos de verificación establecidos** para confirmar el contenido de los paquetes sospechosos.
2. **Confirme con el destinatario si espera un paquete o un sobre** y cuál es el contenido esperado.
3. **Comuníquese con la persona o compañía mencionada** en el remite.
4. **Si no se puede verificar fácilmente el paquete o usted continua preocupado,** esté preparado para tomar medidas de seguridad. Si sospecha que el correo o paquete puede contener una amenaza explosiva, radiológica, biológica o química:
   - Aísle el área inmediatamente.
   - Llame al 911.
   - Lávese las manos con agua y jabón.

(Véase el apéndice para más información.)

Capítulo 6

SEGURIDAD DE LOS COMPUTADORES Y LA INFORMACIÓN

La piratería informática, los programas malignos y otras amenazas digitales significan que un sistema de información y computador no protegido puede dejar a su organización, sus miembros individuales, los posibles donantes y el personal, en riesgo de sufrir acoso personal y dificultades financieras. Además, puede dañar la reputación de su organización. Puesto que su institución puede quedar lisiada por un ataque informático antes incluso de que usted se entere de él, la seguridad de los computadores y datos debe ser un componente integral de su programa general de seguridad.

Debido a las complejidades de estos temas, es recomendable que usted consulte a un profesional de seguridad informática respecto al plan más exhaustivo de seguridad.

Asuntos clave

Hoy día, la mayoría de los computadores y teléfonos móviles tienen algún tipo de conexión a Internet, ya sea de alta velocidad, inalámbrica, de marcación, etc. Eso hace que sus datos y equipo sean más susceptibles a ataques y robos que nunca antes. Si usted tiene un sitio web, este también puede ser objeto de ataques o desfiguraciones que pueden dañar la reputación de su organización y causarle pesadillas en sus relaciones públicas.

Además de las amenazas específicas de personas u organizaciones que pueden tener conflictos con su organización, usted debe tener en cuenta también los programas automatizados que escanean la red para detectar posibles víctimas. Esos programas buscan fallos conocidos del *software*, como códigos de red y de seguridad obsoletos, así como “brechas” por las que alguien podría acceder sin autorización al sistema. Cuando el programa automatizado encuentra una conexión vulnerable, le pasa esa información al *hacker* que puso en marcha el programa de exploración.

Esa persona entonces puede decidir violar su red para obtener información que puede ser utilizada con fines ilegales; sucede a diario. Una vez su sistema es invadido, el *hacker* puede acceder a toda la información de su red o computador (información de tarjetas de crédito, particularmente), utilizar su sistema como base para atacar otros sistemas, almacenar herramientas de piratería y *software* pirata e, incluso, eliminar toda la información.

Su sistema también es vulnerable a infecciones por programas malignos. Estos programas no discriminan y a menudo invaden el sistema por acciones involuntarias del usuario, incluyendo ser engañado por las suplantaciones de identidad que llegan en el correo electrónico. La negligencia en la seguridad por parte de

los administradores del sitio web o del servidor, actividades malévolas por parte de empleados, la descarga involuntaria de programas peligrosos o la divulgación de contraseñas, también pueden causar problemas.

Medidas prácticas de prevención

Existen métodos sencillos y económicos para prevenir los crímenes y el vandalismo informático. Los consejos que siguen no lo harán inmune a los ataques, pero dificultarán el trabajo a los delincuentes. La mayoría de los agresores no están lo suficientemente motivados para atacar un computador bien protegido, así que buscarán una presa más fácil.

Correo electrónico

- Disuada a la gente de utilizar direcciones de correo personales o no institucionales para actividades de trabajo.
- Discuta y establezca una política codificada para el uso de las direcciones institucionales de correo electrónico, incluyendo quién tiene derecho a tener una y quién está a cargo de su distribución.
- Establezca cuentas independientes para sus funcionarios, empleados, miembros o voluntarios en su sistema de correo. Estas cuentas solo deben utilizarse para asuntos de la institución, para comunicarse dentro de su comunidad de miembros y partes interesadas, y para comunicaciones externas de la entidad.
- Es recomendable evitar el uso del nombre de una persona, su ubicación o cualquier otra identidad en línea (Facebook, LinkedIn, etc.) en su dirección de correo institucional siempre que sea posible utilizar un identificador laboral (recursos humanos@, administración@, director@).
- Cierre las cuentas individuales tan pronto dejen de ser necesarias (un funcionario que renuncia, voluntarios que dejan de participar en las actividades de su organización, etc.).
- Cuando envíe un correo electrónico a una amplia lista de destinatarios, coloque la dirección del destinatario en el área “bcc” (copia ciega). Esto evitará revelar los nombres de los miembros si el correo fuese reenviado a un tercero.

Sitio web

- Evite hospedar su sitio web en el computador personal de alguien. Es mejor trabajar con un servidor.
- Pregunte a la empresa proveedora sobre sus protocolos de seguridad, políticas de copias de respaldo, procedimientos para ataques de denegación de servicio (DoS, por sus siglas en inglés) y acceso no

autorizado al sitio web. También averigüe si tienen un procedimiento de recuperación que incluya servicio 24/7 para emergencias.

- Limite y controle el número de personas que tienen acceso a las credenciales de administrador del sitio web y permisos de *web máster*. Adicionalmente, debe tener una política de asignación de contraseñas y un cronograma para cambiarlas.

Medios sociales

- Asigne a alguien como administrador de los medios sociales y pídale que controle quién tiene acceso a sus cuentas de los medios sociales. Limite la capacidad de publicar a unos pocos individuos, si no exclusivamente al administrador.
- Monitoree constantemente sus cuentas para detectar publicaciones o mensajes amenazadores o inapropiados. Recuerde que las cuentas de los medios sociales también pueden ser violadas.
- También revise las etiquetas (# y una palabra o frase) que mencionan a su organización o sus funcionarios.
- Revise periódicamente las fuentes del tráfico en sus medios sociales y su sitio web, para determinar si tiene visitantes de lugares o grupos inusuales que se oponen a la misión de su organización. Eso podría ser la señal de un problema inminente.

Dispositivos móviles

Hoy día, hay poca protección contra los virus o el malware para los dispositivos móviles y teléfonos inteligentes. Por tanto, recomendamos que usted solo conceda acceso móvil a los sistemas institucionales bajo la supervisión de un proveedor experimentado que entienda claramente las necesidades de seguridad de su institución.

Computadores

- A todo propietario de un computador le interesa estar enterado de quién tiene acceso a su computador, los permisos concedidos a cada cuenta, quién está autorizado como administrador del sistema y quién asigna las contraseñas.
- Si usted no tiene un departamento de tecnología de la información (TI), puede ser conveniente asignar como administrador de sistema para todos los computadores a uno o dos individuos de confianza. Esto es especialmente importante si usted tiene una red interna para compartir archivos e información.
- Una buena práctica es segregar, hasta donde sea posible, la información general, de contabilidad y sobre

los miembros de la entidad

- Contemple la opción de usar un proveedor primario (Comcast, Time Warner, Verizon, etc.) para el servicio de internet. Se debe evitar en lo posible a las compañías que revenden los servicios de otras empresas.
- Siempre es prudente tener activos y actualizados los cortafuegos (firewall), antivirus y programas de detección de amenazas.
- Aunque no siempre representa un problema el uso personal de los computadores de la institución, es razonable tener una política básica de "no uso personal". Cuando menos, prohíba subir programas que no hayan sido aprobados por la persona responsable de la TI.
- Cualquier descarga de material de internet debe ser estrictamente supervisada para evitar virus y violaciones de las leyes de derechos de autor.
- Como regla general, se debe disuadir a los usuarios de conectar dispositivos personales tales como teléfonos inteligentes, tarjetas SD, tabletas y discos externos a los computadores institucionales.
- También es conveniente realizar pruebas de funcionamiento y simulacros regularmente, con el fin de revisar los escenarios de respuesta de seguridad informática y asegurarse de que los programas hacen solamente lo que se supone deben hacer.
  - Los simulacros o pruebas conceptuales generalmente se realizan como ejercicios de discusión en los cuales se revisan los roles, responsabilidades y planes de respuesta ante potenciales incidentes de seguridad. Son similares a otras pruebas conceptuales que usted puede programar para revisar los mismos criterios para otras situaciones de emergencia y seguridad.
  - Las pruebas de funcionamiento del *software* y del sitio web normalmente son realizadas por un tercero, generalmente un especialista, para determinar si el *software* puede ser utilizado para propósitos incorrectos.

Contraseñas

- Deben tener por lo menos ocho caracteres y, en lo posible, incluir una letra mayúscula, un número y un símbolo. Use una regla mnemotécnica para recordar las contraseñas largas: un ejemplo de contraseña es ¡Yjlal50edeuda! que es "¡Yo juro lealtad a los 50 estados de Estados Unidos de América!"

  Las contraseñas deben cambiarse cada seis meses.

Detección

Desafortunadamente, no existe un método fácil y económico para detectar las violaciones a la seguridad de una red. Cuando la información es copiada y robada, la información original permanece igual y en su lugar. El propietario puede no enterarse del robo hasta que la información es utilizada o publicada en internet. De igual forma, la desfiguración de las páginas web puede pasar desapercibida.

Es útil escanear su sistema de vez en cuando para ver qué le está diciendo al mundo y determinar si es vulnerable en formas inesperadas. Existen una serie de sitios web que le permiten escanear su sistema sin costo. Ensaye, por ejemplo, www.grc.com o el test de www.anonymizer.com.[3] Tal vez descubra que debe hacer algunas cosas para poner a punto su sistema.

Si está interesado en detectar un evento y tiene un técnico en su planta de personal, pídale que le permita acceder a su cortafuego y revisar los registros de vez en cuando. Una vez alguien logra meterse en un sistema, tiende a permanecer un rato y regresar por más información. A menudo abren agujeros en su sistema para explotarlos más adelante. Revisar los registros para detectar si hay conexiones inadecuadas es una buena manera de determinar si tiene un problema en curso.

Respuestas prácticas

El truco para responder con eficacia a un caso de seguridad de la red o el computador es preverlo antes de que suceda. Si no, la primera respuesta al descubrir que su sistema informático ha sido violado es el pánico. Como en tantas otras áreas de la planeación de seguridad, la primera medida es decidir quién será el responsable de tomar las decisiones en caso de un problema. Esto es importante porque el nivel de la respuesta requerida depende de la naturaleza y significación del acontecimiento.

Por ejemplo, si su sistema está infectado con un virus o un gusano informático, la respuesta será diferente que si sus datos financieros fueron robados o borrados. En el primer ejemplo, el virus debe ser suprimido y tendrá que actualizar el programa antivirus. Los datos alterados tienen que ser restaurados a partir de una copia de seguridad (véase abajo). En el segundo caso, cuando su sistema ha sido violentado, usted podría decidir que busquen al delincuente y, si lo identifican, lo procesen. Si tal es el caso, tendrá que recurrir a profesionales.

En caso de un ataque a su sistema, tal vez convenga no utilizar el computador para no arriesgarse a perder evidencia.

3 La ADL menciona estos dos sitios web solo con fines informativos y no garantiza su eficacia o la de sus servicios.

Pasos de la respuesta

- Determine quién está a cargo.
- Determine qué ha sucedido.
- Decida si preservar la evidencia o reparar el daño inmediatamente.
- Documente la violación especialmente si hay delincuentes reincidentes.

Formas comunes de ataques cibernéticos y respuestas recomendadas

La violación de los computadores puede suceder de diversas maneras: acceso de forma no autorizada, acceso por un usuario no autorizado, internamente por parte de un miembro de la institución o externamente por el público.

El *software* avanzado puede alertar a un administrador de sistema cuando se produce un acceso no autorizado. Los sistemas más viejos pueden requerir una revisión manual periódica de los registros del computador para detectar los accesos indeseados.

Los registros del computador y el *software* avanzado, si se configuran correctamente, pueden indicar qué archivos, si alguno, han sido violados. Se debe establecer una política para informar a los miembros si los archivos que contenían información personal o sensible han sido invadidos. Probablemente es mejor pecar de exceso de precaución en tales situaciones.

Cuando se detecte una violación del sistema, el administrador del mismo debe ser informado inmediatamente. Posteriormente, se recomienda entrar en contacto con los especialistas en delitos informáticos de las autoridades y el FBI **(http: /www.ic3.gov/default.aspx)** .

Piratería del sitio web

La piratería de un sitio web puede presentarse de diversas maneras y por una variedad de motivos. En este documento definimos la piratería como las actividades realizadas en la sección segura de un sitio web que no son resultado de las acciones de un individuo autorizado. La forma en que se presenta es secundaria; lo importante es decidir qué hacer después del evento.

Sugerimos ponerse en contacto con el servidor de sitio web tan pronto se descubra el incidente. La empresa del servidor tendrá que conservar una copia de las páginas violadas y copias de todos los registros relevantes

del servidor. Las páginas pirateadas deben ser retiradas tan pronto sea posible en caso de que también haya programas maliciosos involucrados y también para limitar el objetivo principal del *hacker*: presumir.

Reporte el evento a la Policía y el FBI (**http://www.ic3.gov/default.aspx**) rápidamente. Facilíteles una copia del material dejado por el *hacker*, especialmente si incluye amenazas o lenguaje de odio.

Recupere el sitio web a partir de una copia de seguridad, pero solo después de que la empresa proveedora del servicio de internet (IPS, por sus siglas en inglés) confirme haber solucionado el problema que originó la violación.

Ataque de denegación de servicio distribuido (llamado Ataque DDoS, por sus siglas en inglés)

Los ataques DDoS son la forma más simple y común de ataque cibernético. Un ataque DDoS es un esfuerzo coordinado por parte de un grupo de computadores para solicitar acceso a un sitio web. Esto crea una situación que impide acceder al sitio o lentifica el acceso a sus contenidos. En muchos casos, una compañía proveedora cerrará un sitio temporalmente antes de crear un problema a sus clientes legítimos. Si un sitio web es víctima potencial de ataques, la compañía proveedora debe ser informada de la situación para que contribuya a la solución.

Un último consejo sobre la seguridad de la información del computador

La información aquí presentada es simplemente un resumen de los pasos necesarios para garantizar la seguridad de una red. En un ambiente laboral pequeño, particularmente uno con recursos limitados, proteger los activos electrónicos es de gran importancia. Ignorar el tema no es una solución.

Capítulo 7

PLANIFICACIÓN PARA AMENAZAS CON EXPLOSIVOS

Hoy, es fundamental que cada organización, sin importar su tamaño, tenga un plan de respuesta ante amenazas explosivas (ETRP, por sus siglas en inglés). El primer paso es incorporar medidas físicas en su plan general de seguridad que ayudan a prevenir la colocación de cualquier tipo de dispositivo explosivo. Pero, como ningún plan es infalible, incluso la institución más segura debe tener también un ETRP.

Seguridad física

Además de sus procedimientos para controlar el acceso y prevenir hurtos:

- Las oficinas y escritorios deben mantenerse cerrados, especialmente los que no se estén utilizando.
- Se debe identificar y asegurar incluso los espacios muy pequeños que podrían servir para esconder explosivos. (Un dispositivo explosivo no tiene que ser grande para causar graves daños físicos y psicológicos).
- Los armarios de servicios públicos y de conserjería deben estar siempre cerrados, al igual que los cuartos de calderas, salas de correspondencia, zonas de computadores, central de conmutador y salas de control de ascensores.
- Los grandes contenedores de basura deben permanecer en cuartos cerrados, inaccesibles para las personas no autorizadas y alejados de los edificios. Las áreas a su alrededor deben estar siempre libres basura y escombros.
- Se debe exigir a autos y camiones que circulen y permanezcan por lo menos a 50 - 100 pies de distancia de las instalaciones. (Véase la sección de este capítulo sobre coches-bomba para mayor información sobre las medidas de seguridad relacionadas con el estacionamiento).
- Cuando planee nuevas instalaciones, cree áreas tan amplias como sea posible que permitan a los vehículos mantenerse alejados de los edificios.
- Dado que los vidrios rotos son altamente peligrosos, contemple la posibilidad de utilizar en sus instalaciones paredes resistentes a estallidos y ventanas inastillables. Así mismo, procure minimizar los paneles de vidrio o recubrirlos con una lámina que los haga inastillables.
- Los setos, plantas y árboles deben mantenerse podados para que no se conviertan en escondite para maleantes y explosivos.

- Se debe urgir a los empleados a tener ordenadas sus zonas de trabajo para que ellos o sus colegas noten si hay algo inusual.
- Dado que en una explosión fuerte más de una de las salidas pueden quedar destruidas, prevea varias vías de escape alternativas.
- Haga simulacros de evacuación con todos los ocupantes de los edificios.

  Revise el área para identificar riesgos provenientes de instituciones vecinas y posibles víctimas.

Preparación

Como se explicó en el primer capítulo, en caso de emergencia es esencial tener claras las líneas de mando, control y comunicación. Esto es especialmente cierto al desarrollar e implementar un ETRP. Es esencial identificar al responsable de tomar decisiones, que tal persona tenga la autoridad para actuar y que sus decisiones se transmitan efectivamente a quienes necesitan conocerlas.

- Sopese la opción de crear un centro de mando para que los responsables sepan inmediatamente donde reunirse en caso de emergencia.
  - Usted podría tener los planos del edificio, la información de contacto y otra información crítica sobre la institución almacenada en ese lugar para tales emergencias.
  - Puede ser necesario definir un segundo sitio por si el primero es inseguro o inasequible.
  - Asegúrese de que se pueda ingresar y funcionar desde su centro de mando antes, durante y después de los horarios de oficina.
  - Instale sus centros de mando y de comunicaciones (primarios y secundarios) tan pronto sea posible para que estén listos cuando se necesiten.
- Recuerde que tiene que tener en cuenta la posibilidad de que un responsable escogido no esté disponible durante una emergencia.
  - Cerciórese de establecer una cadena de mando clara cada día, teniendo en cuenta el personal disponible y presente.
  - Asegúrese de que las personas que encabezan la lista estén informadas de ello.
  - Dependiendo de su plan de seguridad, un gerente o líder puede asumir esa labor como parte de sus actividades diarias.
- Identifique los objetivos más probables. Redacte una lista de objetivos probables y utilícela para reducir una búsqueda a la luz de la información recibida durante una amenaza.

- Defina procedimientos para las búsquedas y monitoree el progreso de los equipos de búsqueda.
- Tenga siempre disponible una lista de números telefónicos y medios de contacto.

Amenazas telefónicas

Las llamadas de amenaza (y la amenaza más frecuente es de bomba) es una forma muy frecuente de hostilizar a las instituciones. Lo más probable es que su organización se entere inicialmente de una amenaza por vía telefónica.

- Responder a tales amenazas requiere una planeación a conciencia y mucha práctica por parte del personal del conmutador, los recepcionistas y toda persona que reciba llamadas directas de fuera de la institución.
- Al igual que con otras áreas de la planificación de seguridad, el primer paso para desarrollar un plan de respuesta para una amenaza telefónica es reunirse con el departamento de Policía o la brigada de explosivos. Ellos podrán decirle qué información necesitan que usted obtenga de la persona que hace la amenaza.

Mantenga la calma y reúna información

Cuando se recibe una amenaza, es importante mantener la calma; especialmente porque una respuesta tranquila puede ayudarle a obtener información importante de la persona que llama. También podría darle a quien hace la amenaza "un rostro humano" para la situación. Adicionalmente:

- No enoje ni insulte a quien llama.
- No cuelgue de golpe.
- Procure que otra persona escuche la conversación. Es buena idea establecer con anticipación un sistema de señales entre los empleados para que la persona que queremos que escuche la conversación telefónica sepa hacerlo sin preocupar o asustar a otros.
- Mantenga al interlocutor en la línea todo el tiempo que sea posible. Pedirle que repita la información puede ser una buena táctica para lograrlo.
- Registre todo lo dicho por la persona que hace la llamada. La posibilidad de grabar las llamadas telefónicas es un factor que se debe tener en cuenta en su plan general de seguridad.
- Tome notas detalladas incluso si tiene una grabadora instalada. (Las fallas en el equipo o errores humanos son siempre una posibilidad con tales equipos).

- Registre la información de forma que sea fácilmente legible para otros. (***Véase la lista de verificación en el Apéndice).***
- Preste especial atención a los ruidos de fondo. Detecte el sonido de motores en marcha, música y cualquier otro sonido que pueda dar pistas sobre la ubicación de quien llama.
- Escuche atentamente la voz de quien llama.
- Transmita esa información inmediatamente a sus administradores de ETRP y jefes de seguridad.
- Si quien llama no da información específica, pregúntele cuándo estallará el explosivo y dónde se encuentra escondido.
- Infórmele que el edificio está ocupado y que el estallido de un explosivo podría causar muertes y heridas serias a muchas personas inocentes.
- Permanezca disponible para las autoridades.

Recuerde: *Durante una amenaza de bomba, no utilice ningún aparato que produzca señales de radio, tales como teléfonos móviles, radioteléfonos, etc.*

El primer punto a decidir

La persona responsable de tomar decisiones tiene tres opciones disponibles después de recibir una amenaza de bomba:

Evacuar inmediatamente.

Hacer una búsqueda y evacuar si es necesario.

Continuar con el funcionamiento normal.

En los tres casos, se debe informar inmediatamente a las autoridades. No realice la búsqueda hasta que la Policía llegue y le ordene hacerlo.

Por lo general, la evacuación inmediata es probablemente la mejor opción salvo en zonas específicas de sus instalaciones (ej. un hospital) en las que otro procedimiento puede ser más conveniente. Aunque esto representará la pérdida de tiempo laboral e interrumpirá el desarrollo de su trabajo, la evacuación inmediata es, sin duda, la política más segura ante el riesgo para la vida y seguridad de las personas. Aun cuando existe la posibilidad de que una evacuación incite a otros a imitar las amenazas, usted siempre podrá revisar sus políticas si después descubre que las llamadas de amenaza están siendo utilizadas solo para acosarlo.

Hay otros motivos para preferir la política de evacuación inmediata:

- Usted evita tener que tomar esa misma difícil decisión en circunstancias más apremiantes y extremas.
- Aunque la probabilidad estadística es que la amenaza sea falsa, tales amenazas han llevado a descubrir explosivos.
- Sus empleados y colegas apreciarán su precaución y, en cambio, podrían reaccionar mal si las instalaciones no son evacuadas inmediatamente.
- Si no se hace la evacuación, quien hace la amenaza puede sentirse ignorado y decidir intensificar sus actividades.

Procedimientos de evacuación

Hay tres pasos clave para realizar una evacuación exitosa:

Informe a las personas la decisión de evacuar.

Realice la evacuación de manera segura y ordenada.

Siga un plan que sea lo suficientemente flexible para que la evacuación pueda hacerse incluso si las salidas normales están bloqueadas, representan un peligro o han sufrido daños.

Cada lugar y situación es diferente, pero las mejores prácticas sugieren:

- Los planes de evacuación deben prever diferentes situaciones y el posible bloqueo de las rutas de salida normales.
- Los grupos deben ser guiados por alguien familiarizado con las rutas de salida. Mientras guía a otros a una zona segura, esa persona debe estar atenta a obstrucciones o explosivos.
- Las distancias consideradas seguras en una evacuación varían pero, si usted puede ver el dispositivo o vehículo sospechoso, está demasiado cerca.
- Si es posible, tenga un lugar para albergar a los evacuados en caso de mal tiempo. Un acuerdo con otras instalaciones de la zona (una escuela, hospital, hogar de ancianos o supermercado) le permitirá disponer de un lugar seguro. En algunas áreas rurales o en los suburbios podría no haber un lugar suficientemente amplio para ubicar a los evacuados; la casa de un vecino solidario podría ser el mejor lugar para albergar a los niños pequeños.

- Algunas instituciones tienen más de un lugar seguro, cada uno a mayor distancia de sus instalaciones (a una manzana, a cinco manzanas, a 25 manzanas).

- Los dispositivos secundarios (explosivos dejados fuera de las instalaciones para hacer daño a quienes evacúan) también son una amenaza. Cuando mínimo, procure asegurarse de que los evacuados son llevados a suficiente distancia para evitar los peligros secundarios.

- Los niños y otras personas que requieran ayuda y supervisión pueden representar problemas especiales para la evacuación. También pueden tener necesidades especiales una vez abandonan el edificio. Estudie la posibilidad de tener preparadas bolsas con cosas que puedan necesitar quienes enfrentarán dificultades extra durante una evacuación larga.

Realizar una búsqueda

Después de recibir una amenaza, es muy posible que se realice una búsqueda. Dependiendo de las circunstancias y con autorización de la Policía, usted podría hacer la búsqueda del explosivo antes de evacuar el edificio o después de llevar a las personas a una zona segura.

No realice la búsqueda hasta que la Policía llegue y le ordene hacerlo.

La búsqueda debe ser realizada exclusivamente por empleados y funcionarios de seguridad o con la ayuda de la Policía local y la brigada de explosivos. Este es otro caso en que es fundamental entender cuándo y cómo responden las autoridades locales a una emergencia. Por ejemplo, aunque recomendamos encarecidamente no realizar una búsqueda antes de que llegue la Policía, en algunas áreas la Policía o brigada de explosivos no responderán hasta que no se encuentre un dispositivo explosivo. En otros sitios, la Policía puede responder a una amenaza creíble pero no realizará una búsqueda en las instalaciones si no está presente un miembro del personal.

Consejos para la búsqueda

- Si es seguro hacerlo, pida a todo el personal que revise su espacio de trabajo para asegurarse que no haya nada escondido allí.

  Exija que más de una persona revise cada espacio, incluso si es pequeño.

- Idealmente, sus principales buscadores deben estar organizados en varios equipos de dos personas cada uno.

- Los equipos pueden estar conformados por personal de supervisión, ocupantes del área específica o gente especialmente entrenada para esa labor (como la unidad de explosivos).
- Aunque los supervisores y usuarios de un área pueden realizar una búsqueda más rápida, los especialistas están mejor preparados para realizar una búsqueda más segura y exhaustiva.

Si la Policía recomienda que el personal de la institución realice la búsqueda, un equipo de dos personas debe:

1. Ingresar a un salón o área juntos.

2. Recorrer cuidadosamente varias zonas del salón y escuchar atentamente para detectar el sonido de un temporizador. Como es común que haya bastante ruido en los edificios, esta labor requerirá mucha concentración.

3. Dividir el salón en cuatro rangos de altura: del suelo a la altura de la cadera, de la cadera a la barbilla, de la barbilla a encima de la cabeza y, finalmente, los techos y muebles fijos.

4. Comenzar la búsqueda juntos en un lugar determinado, espalda contra espalda, y recorrer la circunferencia del salón buscando dispositivos en el primer rango de altura (del suelo a la cadera). Examinar todo en la habitación, incluyendo alfombras, canales, calentadores, etc.

5. Cuando se encuentren, deben proceder al centro del salón y revisar todos los objetos y muebles.

6. Repetir los pasos cuatro y cinco para los siguientes dos rangos de altura.

7. Buscar dispositivos que puedan estar escondidos en falsos techos o cielorrasos, luces y elementos estructurales (ej. vigas, montantes, etc.).

8. Marcar las áreas revisadas de manera que no se dupliquen los esfuerzos y ninguna área quede sin revisar. Los métodos comunes para marcarlas son pegar cintas en las paredes o colgar un letrero de “Búsqueda realizada” en lugar visible.

- Se debe realizar la búsqueda también en el exterior del edificio. Es conveniente revisar:
  - A lo largo de las paredes y detrás de los arbustos.
  - Dentro de cualquier recinto cerrado, incluyendo macetas, cobertizos, etc.
  - Debajo y dentro de todo vehículo estacionado cerca al edificio. Busque un coche o camión que parezca demasiado cargado o de otra forma sospechoso. Identifique y examine todos los vehículos que no pertenecen en las instalaciones.

- Los equipos y/o todo el personal deben ser entrenados en estas técnicas.

- Si tiene motivos para pensar que las oficinas y espacios no utilizados pueden representar un peligro (ya anteriormente sugerimos que se mantuvieran cerrados), tendrá que revisarlos también. Su centro de mando debe tener las llaves y tarjetas de acceso de todas las áreas.

Descubrimiento

Es imprescindible que el personal involucrado en la búsqueda de explosivos entienda que no debe tocar, mover o agitar ningún objeto sospechoso. Un buscador tan solo debe buscar y reportar los objetos sospechosos. Deben:

- Informar la ubicación del dispositivo.
- Dar instrucciones claras para ubicarlo.
- Describir el aparato.
- Evacuar el edificio.

Nota: Abra las puertas y ventanas para minimizar los daños ocasionados por un estallido.

Coches-bomba

Su mejor defensa contra este tipo de bombas es en gran medida un asunto de prevención y fuerte seguridad física. Su mejor defensa es una remodelación física a fondo y un amplio y detallado programa de seguridad; sin ellos, defender su organización de los coches-bomba es muy difícil. Aun así, hay medidas menos drásticas que pueden contribuir a mitigar la amenaza.

Recomendaciones para las zonas de estacionamiento

Su principal prioridad debe ser excluir del área los vehículos potencialmente peligrosos, pero no siempre es posible revisar todos los autos y camiones antes de que ingresen a los predios. Examinar los vehículos o conductores sospechosos cuando ya están en los predios sigue siendo una buena medida de seguridad, al igual que mantener los vehículos lo suficientemente lejos del edificio para evitar daños.

- Exigir a autos y camiones que permanezcan por lo menos a 50 - 100 pies de distancia de las instalaciones.

- Si eso no es posible, contemple la posibilidad de eliminar los estacionamientos más cercanos al edificio o restringir el acceso a esa zona a empleados y directivas. Su organización puede emitir etiquetas adhesivas de identificación para los parabrisas y así distinguir los vehículos que pertenecen a la organización y cuáles deben ser revisados más a fondo por no pertenecer a ella.
- Estudie la opción de poner barreras físicas, tales como barreras de seguridad de hormigón, entre la calle y sus instalaciones.
- Utilice verjas y rejas para evitar el ingreso de personas no autorizadas.
- En un ambiente urbano, donde es posible estacionar en la calle cerca a las instalaciones, considere la posibilidad de pedirle a la Policía prohibir el estacionamiento en tales áreas.
- Entrene a los empleados y personal de seguridad sobre los tipos y apariencia de los vehículos más frecuentemente usados como coche-bomba (véase más abajo).
- Como ya se sugirió, considere el uso de paredes resistentes a estallidos y vidrios inastillables para controlar los daños a sus instalaciones.

Identificación de coches y camiones-bomba

Ante una amenaza de bomba, es esencial revisar los vehículos sospechosos. Los coches y camiones-bomba pueden ser identificados por la apariencia exterior del vehículo, el comportamiento del conductor y otras señales sospechosas. Ninguno de los siguientes detalles es prueba definitiva de posible violencia y muchos son coherentes con un comportamiento inocente. Sin embargo, podrían ser pistas de que algo está mal:

El conductor del vehículo lo estaciona pero luego se aleja (corriendo o no) en lugar de entrar a sus instalaciones.

El coche o camión parece estar excesivamente cargado.

El vehículo está estacionado ilegalmente o demasiado cerca al edificio.

El coche o camión es un modelo viejo o de arriendo (que son los más comúnmente usados para bombas).

Sospeche de cualquier vehículo que parezca abandonado y tenga un autoadhesivo de revisión, un registro o unas placas vencidas.

Endurecimiento del objetivo

Hacer que sus instalaciones parezcan difíciles de violar es un procedimiento llamado endurecimiento del objetivo, y se basa en la hipótesis comprobada de que los delincuentes prefieren los blancos fáciles. Entre más difícil parezca el ingreso sin autorización, más posibilidad hay de que una persona sospechosa pase de largo y busque otra víctima o se ponga nerviosa.

Las tácticas de endurecimiento incluyen:

- Señales vistosas anunciando la existencia de un sistema de alarma.
- Vehículos y patrullas de seguridad visibles.
- Cercas e iluminación exterior en buen estado.
- La apariencia general de unas instalaciones bien mantenidas.
- La presencia frecuente de las autoridades en o alrededor del recinto.

Para información adicional sobre el desarrollo e implementación de medidas de seguridad ETRP, **consulte el Apéndice** o visite **www.threatplan.org** y **www.adl.org/security**.

Capítulo 8

TIRADORES ACTIVOS

El término "tirador activo" se refiere a un individuo que activamente busca asesinar o intenta asesinar personas en un área limitada y poblada. En la mayoría de los casos, los tiradores activos usan armas de fuego, y no hay un patrón o método en su selección de las víctimas. Aunque cada situación y sus circunstancias son únicas, todos estos eventos son impredecibles y se dan muy rápidamente.[4]

La inmediata intervención de la Policía es el mejor procedimiento y puede contribuir a mitigar el daño para quienes son atacados pero, debido a que estas situaciones suelen escalarse e incluso terminar antes de que las autoridades lleguen al lugar, los individuos deben estar preparados tanto mental como físicamente para enfrentar la situación.

La información y las recomendaciones que siguen reflejan prácticas generalmente aceptadas por el Departamento de Seguridad Nacional de Estados Unidos y otras respetables organizaciones. Sus acciones, por supuesto, también estarán muy influenciadas por los factores únicos de cualquier situación que involucre a un tirador activo.

Sin importar la situación o la acción apropiada específica, informar a las autoridades es prioritario. Debe hacerse tan pronto sea posible.

Evacuar (Salir)

Si hay una forma segura de hacerlo, evacue el área inmediatamente. (Véase la página XXXXX) Si es posible, escoja la mejor ruta, la que ofrezca oportunidades para cubrirse o esconderse y ayude a otros a evacuar el lugar. (Se deben tomar medidas especiales para personas incapacitadas y otros que necesiten ayuda). Deje sus pertenencias personales atrás y mantenga las manos visibles todo el tiempo (para no confundir a la Policía) y, una vez fuera, siga las instrucciones de las autoridades.

Buscar refugio (Esconderse)

Si no es seguro evacuar el lugar, tome medidas para proteger su vida y las de otros. Escóndase. Busque refugio en una zona o salón donde el atacante tenga menor probabilidad de encontrarlo, y procure encerrarse ahí y/o bloquear el paso.

4 La orientación de esta sección sobre tiradores activos fue preparada por el Comité Nacional de Seguridad Comunitaria de la ADL.

- Cierre todas las cortinas, apague radios y computadores, y silencie el teléfono móvil, localizadores y otros dispositivos que puedan emitir sonidos.
- Escóndase detrás de cosas grandes, como escritorios o armarios.
- Protéjase tras un muro cortafuegos si lo hay.
- Permanezca alejado de puertas por las que le puedan disparar desde afuera.
- Planee la forma de protegerse a sí mismo y a otros en caso de que el sospechoso traspase la puerta.

Pida ayuda

Tan pronto pueda y cuando la comunicación sea viable, comuníquese con el 911 y deles la siguiente información:

- Ubicación específica, incluyendo nombre del edificio y número del salón/oficina.
- Número de personas con usted.
- Número de personas heridas y descripción de sus heridas.
- Ubicación del agresor, número de agresores y otra información pertinente:
  - Raza y género.
  - Descripción de sus ropas y características físicas.
  - Tipo de armas (arma larga, arma corta, puñal), sonidos de diversos disparos, etc. y descripción de cualquier bolsa que tengan.

  Identidad (si se conoce) y comportamiento del atacante(s): calmado, agitado, furioso, violento.

  Intenciones o exigencias del atacante(s).

Confrontar al tirador activo

Enfrentar al atacante es algo que solo debe hacerse cuando su vida está en peligro inminente, usted no puede abandonar el área ni refugiarse en el lugar, y realmente no le queda ninguna otra opción. Como último recurso, intente perturbar al atacante:

- Levantando la voz o gritando.
- Actuando agresivamente.
- Lanzando objetos o improvisando armas.

Operaciones de las autoridades

La Policía y servicios de emergencia tienen que cumplir protocolos y es importante que usted los entienda, sepa cómo ayudarles y no interferir con sus operaciones.

- Una vez en el lugar, las autoridades tienen que asumir que todo el mundo es una amenaza para su seguridad.
- Los oficiales se dirigirán directamente a la zona en que se escucharon los últimos tiros.
- Generalmente forman grupos de cuatro agentes para acercarse o establecer contacto con el tirador activo.
- Los oficiales pueden lucir sus uniformes normales de patrulleros o chalecos antibalas, cascos y otros equipos protectores.
- Pueden estar armados con rifles, escopetas y revólveres.
- Pueden utilizar gas pimienta o gases lacrimógenos para controlar la situación.
- Es probable que griten órdenes y empujen a los individuos al suelo para protegerlos.

Cuando interactúe con las autoridades durante un tiroteo, usted necesitará ser consciente de lo que puede esperar y lo que se espera de usted:

- Mantenga sus manos a la vista.
- Esté dispuesto a que lo registren.
- Siga las instrucciones cuando lo guíen fuera del edificio.
- Después de la evacuación, es posible que lo lleven a una zona acordonada para darle cuidados médicos, interrogarlo, asesorarlo, etc.
- Una vez evacuado, no se le permitirá retirar nada ni ingresar al área hasta que las autoridades den su visto bueno.

Los gerentes, funcionarios de seguridad y líderes de la organización presentes deben:

- Comunicarse con la Policía y trasmitirle toda la información que tengan.
- Informar el número de sospechosos, rehenes, ubicaciones, heridos, etc. (Tal vez el informante inicial dio estos datos, pero es necesario repetirlos o confirmarlos según la situación).
- Revisar las grabaciones del circuito cerrado de TV para ubicar al sospechoso(s) y víctimas potenciales.
- Aislar (*lockdown*) las instalaciones, dependiendo de la ubicación del sospechoso(s). Esto evitará que ingresen más personas a las instalaciones, pero permitirá escapar a los que están adentro.
- Anunciar la presencia del tirador a través de un tablero digital, mensaje instantáneo u otro sistema de comunicación apropiado. Describir la ubicación y dar instrucciones.
- Guiar a las autoridades a la ubicación del incidente, darles la información apropiada y proveerlos de las tarjetas de acceso, llaves y planos de las instalaciones.
- Lidiar con las repercusiones del evento. (Aunque toda situación es única, las posibles soluciones deben estar contempladas en su plan general de seguridad). Esto incluye cuidar de las víctimas y sus familias.

(Véase el Apéndice para más información.)

Capítulo 9

SEGURIDAD EN LOS EVENTOS

La seguridad en los eventos se apoya en el sencillo principio de *excluir* a las personas indeseables e *incluir* a las deseables. No excluir a alguien a quien debe excluirse es bastante más peligroso que bloquear a alguien que debe ser incluido. Lo primero es un tema de seguridad vital, lo segundo un problema de relaciones públicas.

Los pasos para garantizar la seguridad durante un evento son:

Evaluar los riesgos

Hay una serie de elementos que forman parte de la evaluación del riesgo. Entre los principales están:

- La existencia de amenazas o incidentes previos.
- Hasta qué punto el evento está abierto al público.
- La cantidad de publicidad hecha al evento.

Establecer un perímetro

- Identifique el área que quiere proteger (por ejemplo, el vestíbulo y el salón de baile, la zona social, el gimnasio o todo un edificio) y establezca un perímetro a su alrededor.
- Identifique todas las salidas y entradas a ese perímetro, incluyendo accesos, salidas de emergencia, puertas de cocinas, ventanas y su zona de control de seguridad.
- Despeje el área dentro del perímetro y revísela a fondo, fijándose en objetos o personas sospechosas que pueden haberse escondido antes de que usted definiera el perímetro.

Cree un centro de seguridad

Es conveniente asegurar el área de manera que cualquiera que quiera ingresar deba pasar por un puesto de control de seguridad. Dependiendo del tipo de evento y el nivel de riesgo, ese podría ser el lugar donde se revisan las boletas, se consulta la lista de invitados o se ubican los detectores de metales. La Policía local puede ayudarle a determinar lo que debe hacer para garantizar la seguridad de su evento. Cuando menos, todo el mundo debe ser registrado visualmente para detectar características o comportamientos sospechosos.

Consideraciones

- Todo acceso al perímetro de seguridad debe estar cerrado, vigilado o con una alarma activada. Recuerde que, al hacerlo, debe cumplir la legislación sobre incendios.
- Alguien debe estar a cargo de mantener el perímetro y supervisar a quienes están encargados de patrullarlo, vigilarlas puertas y ventanas, etc.
- Es importante mantener las medidas de seguridad incluso cuando los responsables de la vigilancia del perímetro están distraídos de sus obligaciones (por ejemplo, por una emergencia médica). Tenga a disposición un plan B desde antes del inicio del evento.
- Los guardias deben tener claro que ellos están allí para velar por la seguridad del evento, no para participar en él. Por tanto, deben vigilar a la multitud y el perímetro, sin distraerse con el artista, discurso o actividades.
- Como con todo, es fundamental recordar que usted está sujeto a las leyes locales, estatales y federales en relación a la discriminación y lugares públicos, así como a la legislación de incendios.

Capítulo 10

TRATAR CON LOS DISIDENTES EN SU INSTITUCIÓN

Es importante estar preparado para esta situación incluso si usted nunca ha enfrentado una protesta en sus oficinas o propiedad. Las siguientes pautas pueden ser útiles, pero por favor recuerde que cada protesta es diferente y, por tanto, no todos los puntos a continuación aplican para toda situación.

Primero y antes que nada, no dude en llamar a las autoridades si se siente de alguna forma amenazado.

Segundo, es importante que usted se abstenga de entablar conversación con los manifestantes.

Nadie debe hablarles o responderles, especialmente el personal que ingrese o abandone las instalaciones. Esto puede ser difícil en ese momento pero es muy importante, ya que discutir con ellos o responder a sus cantos y burlas puede elevar la tensión y, por tanto, aumentar los riesgos a su seguridad.

Usted también puede sentirse tentado a organizar inmediatamente una contra-protesta o manifestación informativa. No recomendamos realizar contra-protestas o eventos educativos en el mismo lugar o cerca de las protestas. Si lo hace, reunirá a los manifestantes y sus opositores y aumentará dramáticamente los problemas de seguridad; hable con el departamento de Policía sobre esto.

Asegúrese de que sus empleados sepan lo que se espera de ellos.

Revise y mantenga sus procedimientos de seguridad

Aunque usted querrá evaluar la situación cuando se presente y responder como convenga, puede ser muy útil preparar previamente a su organización para enfrentar posibles protestas. Las siguientes pautas cubren tanto su periodo de preparación como una situación ya presente.

- Asegúrese de que las normas y procedimientos de seguridad de su institución con respecto al ingreso a las instalaciones son suficientes para las potenciales circunstancias.
  - — Asegúrese de que su sistema está activo y funcionando.
  - — Vuelva a revisar todo a la primera señal de protestas y esté preparado para hacer cumplir las normas relacionadas con el ingreso de potenciales manifestantes.
  - — Monitoree cuidadosamente quién y cuántos ingresan a sus instalaciones.
- Aparte del control de ingreso, asegúrese de que todos los procedimientos de seguridad de su institución sean suficientes para la situación y funcionen correctamente.

- Confirme que todos los dispositivos de seguridad funcionan y están en uso (incluyendo cerraduras y sistemas de alarma).
- Haga ejercicios de práctica (ensayos) para esta situación con frecuencia.
- Asegúrese de que las entradas no utilizadas o vigiladas estén cerradas.
- Mientras se sienta cómodo y seguro al hacerlo, puede ser útil que grabe o tome fotografías de los manifestantes. Consulte con un abogado las implicaciones legales del asunto.

Comuníquese con el Departamento de Policía

- Informe a la Policía tan pronto se entere de que se está planeando o realizando una protesta.
- Si lo considera necesario (y es mejor pecar de precavido), pida que le envíen agentes para ayudar a mantener la seguridad.
- Entienda que, cuando los límites físicos de sus instalaciones no son claros, en ese lugar se reunirán legalmente los manifestantes. **Averigüe con frecuencia la reglamentación local sobre el derecho de reunión para confirmar que no haya cambiado.**
- Informe a la Policía si los manifestantes se comportan de forma amenazante, son violentos o amenazan llegar a actos violentos. Hágalo incluso si ya hay oficiales de policía presentes en la manifestación.
- Conozca los permisos vigentes en su área, tanto para los manifestantes como para cualquier contra-protesta que quiera llevar a cabo (recuerde que no se recomienda realizar contra-protestas en el mismo lugar que las protestas). Si los manifestantes no tienen las autorizaciones necesarias, pregunte a la Policía cómo debe proceder.
- Consulte con la Policía si la situación permite continuar con la operación normal o si sería mejor modificar la rutina de trabajo.

Comuníquese con su abogado

Pida a su abogado que le explique y aclare los derechos de los manifestantes y los suyos. (Si no tiene un abogado, puede buscar ayuda con el colegio local de abogados).

- Sea consciente que los discursos y formas de expresión de los manifestantes pueden estar protegidos por la ley, especialmente si están en propiedad pública. Eso incluye, pero no se limita a, la distribución de volantes y otros materiales, cánticos, exhibición de pancartas y fotografías.
- Conozca sus derechos en caso de una protesta

Contemple la opción de contratar profesionales de seguridad

Un profesional de seguridad puede orientarlo y proveerlo de personal para manejar una protesta. Por favor consulte la sección de esta guía dedicada a la contratación de profesionales de seguridad externos.

Prepare un comunicado para los medios de comunicación

Las protestas tienen como finalidad llamar la atención de la comunidad y pueden atraer a los medios de comunicación. Tal vez desee que un representante de su organización esté preparado para dar una breve declaración en caso de que los medios de comunicación se hagan presentes.

- Cualquier declaración debe estar por escrito y ser revisada antes de la entrevista. Puede ser difícil hablar espontáneamente en medio de la tensión del momento.
- Utilice frases simples y cortas.
- Desarrolle dos o tres puntos clave y cíñase a ellos.
- Procure evitar que los medios inviten a los manifestantes a dar declaraciones mientras usted hace la suya.

Capítulo 11

EMPLEAR A UN CONTRATISTA DE SEGURIDAD

Como ya se discutió en esta guía, su institución puede decidir que es conveniente contratar a un consultor en seguridad externo para ayudarles a diseñar e implementar el plan de seguridad. Dependiendo del tamaño de su organización y sus necesidades específicas, usted probablemente comenzará por resolver si le conviene más contratar personal de seguridad para trabajos a corto plazo (como eventos) o contratar personal permanente. En cualquier caso, usted deberá realizar una búsqueda e investigación detallada sobre el contratista externo[5].

Trabajos a corto plazo

Si su organización considera que es necesario contratar personal de seguridad adicional para los eventos especiales celebración de festividades, reuniones grandes o conferencias usted deberá reunir ofertas competitivas y comenzar un proceso de investigación tan pronto sea posible. Las autoridades locales y otras organizaciones en su zona pueden darle recomendaciones. Conviene que usted prepare un informe del ámbito de trabajo para que las compañías puedan desarrollar sus propuestas y estimar los costos. Este debe incluir:

- Un informe conciso pero detallado de las labores de seguridad a realizar, incluyendo su duración en días y horas.
- Un recuento exhaustivo de instrucciones generales y especiales. Es importante que dichas instrucciones sean desarrolladas en su organización; no recurra al contratista de seguridad para hacerlas.
- El nombre e información de la persona de contacto en su organización, que recibirá al personal de seguridad y se asegurará de que entiendan su oficio y responsabilidades para cada ocasión.

5 La información de este capítulo fue preparada por el Comité de Seguridad de la oficina regional de San Diego de la ADL.

Interactuar con el personal de seguridad

La principal responsabilidad del personal de seguridad es desalentar y detectar actividades inusuales o sospechosas, así como proteger la propiedad y las personas. Algunos de los puntos clave que el responsable en su organización debe revisar con el personal de seguridad al comienzo de un trabajo son:

- Requisitos de la tarea, con una explicación del ámbito de trabajo y expectativas escritas.
- Objetivo de la seguridad durante las horas especificadas.
- Informar que el personal será evaluado durante su turno para verificar que esté alerta.
- Normas de conducta que incrementan la efectividad —no fumar, bromear, fraternizar, etc.
- Información de la persona de contacto.
- Plano de las instalaciones.
- Reglamentación de seguridad y/o incendios en las instalaciones.
- Ubicación de áreas vulnerables.
- Ubicación de teléfonos, equipo de extinción de incendios y alarmas de incendio, salidas de emergencia, etc.
- Ubicación de escaleras y puertas.
- Pautas claras de procedimientos en caso de una emergencia (incendio, paquetes sospechosos, amenaza de bomba, etc.).

Criterios para escoger al contratista

Tan pronto su organización tome la decisión de contratar seguridad externa, ya sea a corto o largo plazo, será necesario elegir un contratista. La compañía debe ser confiable y estar acreditada, tener una licencia estatal válida y cumplir al menos con los siguientes criterios:

- Tener un seguro adecuado y vigente (consulte nuestro sitio web para una lista de criterios).
- Excelentes antecedentes y reputación.

— Consulte a un abogado o en el juzgado local si tiene una historia reciente (10 años) de demandas o quejas válidas y exitosas ante agencias estatales. Pída al contratista que le facilite informes de Loss Experience" o "Lose Runs".

—Tenga en cuenta el historial de la compañía en casos de negligencia, experiencia y reclamos por compensaciones a trabajadores, y administración. Pida Employment Modification Rate (EMR) de los últimos tres años; entre más baja la relación, mejor el desempeño del contratista.

—Buenas referencias.

- Un personal de seguridad bien entrenado y que cumpla con las cualificaciones especificadas planteadas en la propuesta.
- Suficiente equipo de trabajo. Un teléfono móvil es esencial y el personal también puede disponer de gas pimienta, bastones, etc.
- Una propuesta hecha a la medida de las necesidades de su organización. La propuesta también debe describirm exactamente cómo se supervisará al personal.
- Costos razonables:

— ¿Cobran una tarifa plana, tarifa por hora para todos los empleados o una tarifa por hora/empleado? (La última suele ser la opción más económica).

— ¿La propuesta o contrato revela el salario pagado al personal de seguridad asignado a sus instalaciones (en contraste con la tarifa que usted estará pagando, de manera que usted pueda determinar la relación tarifa/margen de ganancia de la compañía)?

— ¿Las facturas periódicas enumeraran los sueldos y bill rates de cada empleado? Los detalles deben ofrecer un buen seguimiento de auditoría.

— ¿Cómo se manejaran los aumentos de salarios? Los salarios inadecuados o estancados producen una muy alta rotación de empleados. Los aumentos salariales deben ser propuestos con antelación por el contratista.

— ¿Habrá cargos adicionales para uniformes, equipo, suministros, etc.?

- Una sólida documentación de seguimiento
- La propuesta debe describir el tipo y frecuencia de los informes y documentación, por ejemplo reportes de actividades diarias del guardia, informes de incidentes, informes de crímenes, hojas de servicio y otros informes especiales.
- Buena experiencia y administración
- Averigüe la permanencia en la industria, especialmente la del presidente de la compañía, el gerente regional y el gerente de operaciones. Si es posible, el contratista de seguridad debería haber ofrecido servicios de seguridad a una institución similar a la suya.
- La propuesta debe incluir ejemplos de Post Orders o el Manual de procedimientos estándar.

El contrato

El contrato con una compañía de seguridad define los derechos y responsabilidades que rigen la relación entre usted y el proveedor del servicio, y garantiza que el contratista satisfaga sus necesidades. Hay numerosos temas y criterios que se deben tratar específicamente en un contrato de seguridad para garantizar que la compañía sea responsable y confiable.

- El contratista ¿lo indemnizara por toda responsabilidad de seguridad de la que es responsable? En los casos en que un juzgado determine una responsabilidad parcial, ¿el acuerdo especifica claramente cómo se aplicarán tales indemnizaciones?
- Al renovarse el contrato, ¿habrá un incremento en los precios? ¿De cuánto y por qué?
- ¿Tiene usted el derecho a dar por terminado el contrato en cualquier momento y por cualquier motivo? ¿Es un derecho mutuo?
- ¿Es razonable el preaviso exigido para dar por terminado el contrato? (30 días es lo común)
- El acuerdo, ¿es lo suficientemente flexible para sus necesidades?
- ¿Es justo para el contratista y le garantiza a usted, el cliente, un adecuado control?
- ¿Puede usted reemplazar un guardia si lo considera necesario?

Administración

El contratista y usted deben entender los motivos por los que se hace el contrato.

- Comparta sus deseos y expectativas con la administración de la compañía de seguridad.
- Discuta con el contratista, personal y administración las condiciones de supervisión. El personal de seguridad debe saber, entender y acatar el manual de políticas de su institución. Si un guardia de seguridad no se desempeña según lo esperado, es importante saber que el individuo será aconsejado, disciplinado o reemplazado por el contratista según sea necesario.
- Una vez los guardias estén asignados, usted deberá supervisarlos para asegurarse de que cumplen su labor con profesionalismo, su apariencia y comportamiento es profesional y alerta, y responden eficientemente ante los asuntos relacionados con la seguridad. Exija que todos los materiales escritos presentados por el guardia(s) (registros, informes, etc.) sean claros, completos y utilizables. Usted debe recibir una copia de todo informe presentado por el personal de seguridad.

Escoger el tipo de seguridad

Es importante saber que contratar una compañía de seguridad, en cualesquiera condiciones, es algo serio y no debe tomarse a la ligera. Diferentes tipos de guardias de seguridad son apropiados para diferentes situaciones. Un tema importante es si desea que el personal de seguridad de sus instalaciones sea uniformado o vista de civil.

- El principal objetivo de contratar personal de seguridad uniformado es la disuasión.
- El principal objetivo de contratar personal de seguridad que viste de civil es la aprensión.

Después de decidir qué tipo de seguridad contratar, usted tendrá que determinar si los guardias de seguridad estarán armados o desarmados. Hay muchos costos y beneficios que se deben tener en cuenta al elegir un guardia de seguridad armado o desarmado.

Los siguientes puntos pueden ayudarle a analizar el tema y decidir cuál es la mejor opción para su institución.

Guardias de seguridad armados

Es importante determinar si contratar guardias armados cumple con las expectativas de seguridad de su institución.

- Tenga una política sobre el uso de armas como fuerza letal. Decida si la presencia de un arma puede extender la posibilidad de actos de fuerza y violencia que de otra manera no se presentarían. **Sea consciente de que los guardias armados pueden utilizar la fuerza letal.**
- Determine si los miembros de su institución aceptarán a un guardia armado en las instalaciones.
- Tenga en cuenta las implicaciones morales de emplear a un guardia de seguridad armado.
- Determine la política del contratista sobre el uso de armas como fuerza letal.
- Por favor tenga en cuenta que se debe ser especialmente cuidadoso si su institución atiende a muchos jóvenes. Las escuelas deben ser particularmente conscientes del mensaje que transmite un guardia de seguridad armado a los estudiantes, padres y empleados.
- Estudie la relación costo/rendimiento de un guardia de seguridad armado. Son mucho más costosos que los guardias desarmados, debido a los requisitos de licencias y entrenamiento.
- Averigüe el entrenamiento y cualificaciones de los guardias de seguridad en armas de fuego.
- Los seguros pueden verse afectados adversamente por la presencia de guardias armados.

Guardias de seguridad desarmados

- El uso de la fuerza letal no es deseable ni necesario.
- Los guardias de seguridad desarmados con frecuencia son tan disuasivos como los armados.
- La protección ofrecida por guardias desarmados es menos costosa, puede causar menos responsabilidades y exigir menos seguros.

Capítulo 12

PROCEDIMIENTOS DESPUÉS DEL INCIDENTE

Ya sea que se presenten problemas durante un evento, que haya una protesta u otro problema de seguridad en su institución, su primera responsabilidad es aplicar los procedimientos de emergencia y seguridad de las personas. Su siguiente tarea es lidiar de forma apropiada con las repercusiones del incidente, incluyendo comunicaciones, protección de la evidencia, recuperación de desastres y revisiones posteriores al incidente. Es conveniente incluir estos procedimientos en sus planes de seguridad y revisarlos antes de un evento.

Control de la línea de mando y comunicaciones

Como ya se explicó en esta guía, es fundamental establecer líneas de mando, control y comunicación. Además de evitar una gran confusión durante el incidente, lo cual podría ser contraproducente o incluso mortal, también le ayudará a lidiar con las personas externas al incidente, incluyendo a quienes necesitan o solicitan información tales como los medios de comunicación y familiares de los participantes en el evento. Algunos de estos puntos ya se trataron en otros capítulos pero tal vez sea útil incluirlos en esta lista.

- Nombre a una sola persona como portavoz de la institución. Si es necesario nombrar más de una persona, es fundamental que estén muy coordinadas. Este portavoz debe ser el único contacto con los medios de comunicación, partes interesadas y cualquier otro que necesite información de la institución.
- La persona nombrada para ser portavoz no debe tener otras obligaciones más importantes que atender durante un incidente.
- Dependiendo de la naturaleza del incidente, especialmente si hay niños involucrados, el portavoz podría remitir a las personas interesadas a otro contacto.
- La información debe ser clara, basada en los hechos, objetiva y consistente con las exigencias de las autoridades.

Con respecto a los medios de comunicación:

- Usted puede optar por no llamarlos para minimizar el exceso de atención sobre el evento, pero su interés a veces es inevitable. Así que se debe planear para ello.
- Los medios de comunicación también pueden ser la forma más efectiva de comunicar información importante a todas las partes interesadas. Dependiendo de dónde está usted, los medios pueden estar más o menos dispuestos a prestarse para tal función. Identifique otra forma de comunicación alternativa como parte de su plan de seguridad.

- Sea claro, directo y honesto. Exprésese con frases cortas y declaratorias como “Las instalaciones permanecerán cerradas durante dos días”.

  Escriba su mensaje antes de que lo entrevisten. Desarrolle dos o tres puntos clave y cíñase a ellos. En muchos casos usted puede responder cualquier pregunta con estas concisas frases:

  — “Todo el mundo está a salvo; los padres se deben comunicar con el xxx-xxx-xxxx”.

  — “La institución ha tomado medidas de seguridad apropiadas”.

  — “Se ha entablado la demanda”.

- Si es posible, comparta con anticipación su mensaje con los servicios de emergencia. Eso es especialmente importante si se ha cometido un crimen. La Policía podría pedirle que se abstenga de mencionar ciertos detalles para no influir sobre un jurado, socavar los procedimientos para determinar si un incidente posterior es una imitación o garantizar que no se vea afectada una investigación en curso.
- Usted no está obligado a responder las preguntas de los medios de comunicación pero tenga en cuenta que, si la historia igual se va a difundir, tal vez sea deseable contribuir con su punto de vista.

Recuperación de desastres

La recuperación de desastres es una parte fundamental del trabajo posterior a un incidente y, como con tantas otras cosas relacionadas con la seguridad, es más fácil si se han hecho preparativos previos.

- Mantenga fuera del recinto copias de respaldo actualizadas de la información crítica, listas de proveedores, información de los empleados, lista de contactos de contribuyentes y donantes, y cualquier otra información fundamental para el desempeño de su misión. Se recomienda pecar por exageración en el número de copias de respaldo, puesto que los CD o memorias externas pueden dañarse o destruirse, los computadores de respaldo o servidores pueden dejar de funcionar, etc.
- Revise los seguros de su institución para asegurarse de que su cubrimiento sea adecuado a sus necesidades. Mantenga los registros de seguros con el resto de la información de respaldo.
- Explore con su abogado las consideraciones legales que le afectan. La discusión debe incluir la suposición de autoridad, es decir si se puede conceder a alguien autoridad legal para tomar medidas de emergencia en nombre de la institución.
- Antes de que el desastre ocurra, haga planes para reubicar estudiantes residentes, pacientes, campistas, ancianos y empleados.
- Haga un inventario de todas las cosas que al ser destruidas obligarían a la institución a cancelar sus operaciones.
- Revise todos los acuerdos de servicios vigentes para establecer si incluyen un servicio post-desastre adecuado y asistencia en la recuperación.

Evidencia

Cuando se descubren daños o grafitis, la primera tentación es limpiar y ordenar inmediatamente. Lo instamos a resistirse a la tentación y no tocar el escenario del crimen hasta que la Policía llegue. Al esperar, usted ayuda a proteger valiosa evidencia y a que los delincuentes sean apresados.

Así mismo, si se reciben cartas, correos electrónicos o mensajes de voz con amenazas, se deben guardar cuidadosamente para que las autoridades puedan evaluar las amenazas y determinar si se ha cometido algún crimen.

CONCLUSIÓN

La mayoría de las instituciones religiosas y comunitarias se esfuerzan por mantener un ambiente abierto y amable pero también seguro. Esperamos que la información de esta guía permita a su institución estar en mejor posición para frustrar una emergencia de seguridad y responder a una amenaza potencial. Un plan exhaustivo de seguridad y sólidas relaciones con las autoridades locales mejorarán la capacidad de su institución para realizar con seguridad su misión y trabajo.

Para información adicional o más detalles sobre los temas tratados en esta guía, por favor visite www.adl.org o comuníquese con su Oficina Regional de la ADL.

Apéndice

HOW TO RESPOND
WHEN AN ACTIVE SHOOTER IS IN YOUR VICINITY

QUICKLY DETERMINE THE MOST REASONABLE WAY TO PROTECT YOUR OWN LIFE. CUSTOMERS AND CLIENTS ARE LIKELY TO FOLLOW THE LEAD OF EMPLOYEES AND MANAGERS DURING AN ACTIVE SHOOTER SITUATION.

1. EVACUATE
- Have an escape route and plan in mind
- Leave your belongings behind
- Keep your hands visible

2. HIDE OUT
- Hide in an area out of the active shooter's view.
- Block entry to your hiding place and lock the doors

CALL 911 WHEN IT IS SAFE TO DO SO

3. TAKE ACTION
- As a last resort and only when your life is in imminent danger.
- Attempt to incapacitate the active shooter
- Act with physical aggression and throw items at the active shooter

HOW TO RESPOND
WHEN LAW ENFORCEMENT ARRIVES ON THE SCENE

1. HOW YOU SHOULD REACT WHEN LAW ENFORCEMENT ARRIVES:
- Remain calm, and follow officers' instructions
- Immediately raise hands and spread fingers
- Keep hands visible at all times
- Avoid making quick movements toward officers such as attempting to hold on to them for safety
- Avoid pointing, screaming and/or yelling
- Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

2. INFORMATION YOU SHOULD PROVIDE TO LAW ENFORCEMENT OR 911 OPERATOR:
- Location of the active shooter
- Number of shooters, if more than one
- Physical description of shooter/s
- Number and type of weapons held by the shooter/s
- Number of potential victims at the location

RECOGNIZING SIGNS
OF POTENTIAL WORKPLACE VIOLENCE

AN ACTIVE SHOOTER MAY BE A CURRENT OR FORMER EMPLOYEE. ALERT YOUR HUMAN RESOURCES DEPARTMENT IF YOU BELIEVE AN EMPLOYEE EXHIBITS POTENTIALLY VIOLENT BEHAVIOR. INDICATORS OF POTENTIALLY VIOLENT BEHAVIOR MAY INCLUDE ONE OR MORE OF THE FOLLOWING:

- Increased use of alcohol and/or illegal drugs
- Unexplained increase in absenteeism, and/or vague physical complaints
- Depression/Withdrawal
- Increased severe mood swings, and noticeably unstable or emotional responses
- Increasingly talks of problems at home
- Increase in unsolicited comments about violence, firearms, and other dangerous weapons and violent crimes

Contact your building management or human resources department
for more information and training on active shooter response in your workplace.

PROCEDIMIENTOS PARA LLAMADAS CON AMENAZA DE BOMBA

La mayoría de las amenazas de bomba son recibidas por teléfono. Todas las amenazas de bomba son serias hasta que se pruebe lo contrario. Actúe rápidamente, pero mantenga la calma y obtenga información con la lista de comprobación que aparece en el revés de esta tarjeta.

Si recibe una amenaza de bomba por teléfono:

1. Mantenga la calma. Mantenga al interlocutor en la línea todo el tiempo que sea posible. NO CUELGUE, incluso si el otro cuelga.
2. Escuche cuidadosamente. Sea cortés y demuestre interés.
3. Intente hacer hablar a la persona para obtener más información.
4. Si es posible, escriba una nota a un colega para que se comunique con las autoridades o, tan pronto la persona cuelgue, avíseles inmediatamente usted mismo.
5. Si su teléfono tiene pantalla, copie el número y/o las letras que aparezcan en ella.
6. Diligencie la lista de comprobación de amenaza de bomba (al dorso) inmediatamente. Anote todos los detalles que pueda recordar. Procure anotar las palabras exactas.
7. Cuando termine la llamada, no cuelgue pero contacte inmediatamente al FPS desde otro teléfono, deles la información y espere instrucciones.

Si recibe una amenaza de bomba manuscrita:

- Llame a _____
- Manipúlela lo menos posible.

Si recibe una amenaza de bomba por correo electrónico:

- Llame a _____
- No borre el mensaje.

Señales de un paquete sospechoso:

- No tiene remitente
- Exceso de franqueo
- Manchas
- Olor extraño
- Ruidos raros
- Entrega inesperada
- Mala letra
- Errores de ortografía
- Cargos incorrectos
- Franqueo extranjero
- Notas restrictivas

NO:

- Utilice radioteléfonos ni teléfonos móviles; las señales de radio tienen la capacidad de detonar una bomba.

- Evacue el edificio hasta que la Policía llegue y evalúe la amenaza.

- Active la alarma de incendios.

- Toque ni mueva un paquete sospechoso

A QUIÉN CONTACTAR (escoja uno)

Siga las pautas locales:

Policía del Servicio Federal de Protección
(FPS, por sus siglas en inglés) 1-877-4-FPS-411 (1-877-437-7411)

911

LISTA DE VERIFICACIÓN PARA AMENAZA DE BOMBA

Fecha: _____ Hora: _____

Hora en que terminó: _____ Número telefónico en que se recibió la llamada: _____

Pregunte a quien llama:

- ¿Dónde está colocada la bomba? (edificio, piso, salón, etc.)
- ¿Cuándo estallará?
- ¿Cómo es?
- ¿Qué tipo de bomba es?
- ¿Qué la hará explotar?
- ¿Usted la colocó? Sí No
- ¿Por qué?
- ¿Cuál es su nombre?

Palabras exactas de la amenaza:

_____

_____

_____

_____

Información sobre la persona que llama:

- ¿Dónde está ubicada? (Sonidos de fondo e intensidad)
- Edad estimada:
- La voz, ¿es familiar? Si es así, ¿como quién suena?
- Otros puntos:

Voz de quien llama
Acento
Enojado
Calmado
Carraspea
Tosiendo
Voz entrecortada
Llorosa
Profunda
Respiración profunda
Disfrazada
Marcada
Excitado
Femenina
Risas
Ceceo
Alta
Masculina
Nasal
Normal
Cansada
Rápida
Áspera
Lenta
Con dificultad
Suave
Tartamudo

Sonidos de fondo:
Sonidos animales
Ruidos de casa
Ruidos de cocina
Ruidos de la calle
Cabina telefónica
PA system
Conversación
Música
Motor
Claros
Estática
Maquinaria de oficina
Maquinaria de fábrica
Locales
Larga distancia

Otra información:
_____

_____

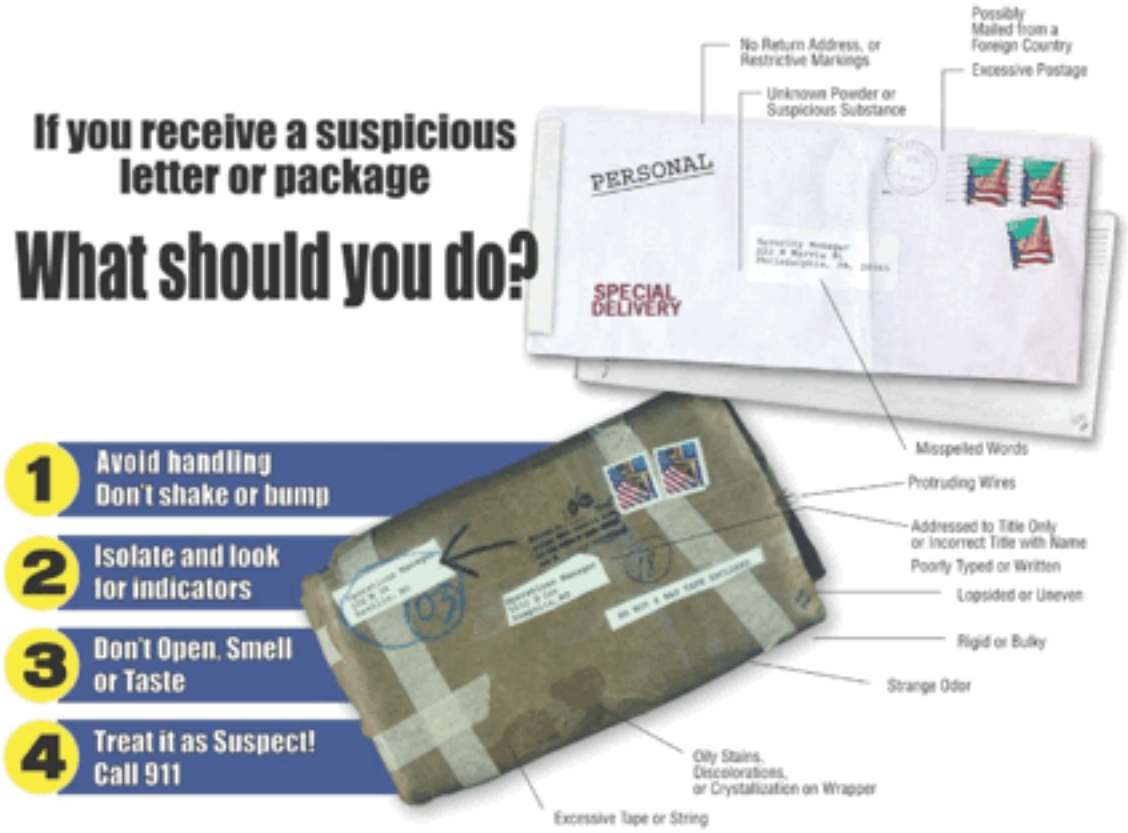
Lenguaje de la amenaza:
Incoherente
Mensaje leído
Grabado
Irracional
Profano
Bienhablado

Homeland Security

U.S. Department of Justice
Federal Bureau of Investigation

If you receive a suspicious letter or package

What should you do?



1. **Avoid handling**
   Don't shake or bump
2. **Isolate and look for indicators**
3. **Don't Open, Smell or Taste**
4. **Treat it as Suspect!**
   Call 911

If you suspect letter or package contains a bomb, radiological, biological, or chemical threat:

- Isolate area immediately
- Call 911
- Wash your hands with soap and water

Police Department _____

Fire Department _____

Local FBI Office _____

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)


ADL®