MITIGACIÓN DE ATAQUES A LAS CASAS DE ADORACIÓN

Guía de seguridad

DICIEMBRE DE 2020

Departamento de Seguridad Nacional de EE. UU.
Agencia de Ciberseguridad y Seguridad de la Infraestructura

La mejor manera de mitigar un posible ataque es adoptar un enfoque integral en materia de seguridad.

Índice

Lista de figuras

La seguridad en la práctica

Un ambiente acogedor no es un ambiente indefenso.

Carta del subdirector

La libertad de religión es una de las libertades fundamentales consagradas en la Primera Enmienda de la Constitución de los Estados Unidos. Sin embargo, los ataques recientes contra fieles de diversas religiones representan desafíos de seguridad únicos que enfrentan las casas de adoración en todo el país. Si bien la pandemia de COVID-19 limitó temporalmente la capacidad de nuestra nación para reunirse en persona, muy pronto, el pueblo estadounidense podrá reunirse de manera segura en sus comunidades religiosas y debería hacerlo sin temor a sufrir daños.

La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) se compromete a colaborar con la comunidad religiosa para ayudar a mitigar la amenaza de la violencia dirigida y prepararse para los posibles incidentes.

La protección de las casas de adoración y la preservación de su ambiente acogedor y abierto es una prioridad para la agencia. En esta guía se presenta un análisis nuevo que surge a partir de una serie de incidentes durante la última década y se ofrece una serie de soluciones de mitigación diseñadas para lograr un enfoque de seguridad sólido y en capas.

Como subdirector interino de Seguridad de la Infraestructura de la CISA, le aseguro que continuamos trabajando con diligencia para identificar los medios innovadores a través de los cuales podamos mitigar de manera colectiva los riesgos que enfrentamos como nación. Gracias por su compromiso con la seguridad de nuestra nación y su continua dedicación para mantener las alianzas que permiten proteger al pueblo estadounidense.

Atentamente,

Scott Breor
Subdirector interino de Seguridad de la Infraestructura

Resumen ejecutivo

Los actos de violencia dirigida contra las casas de adoración (HoW, por sus siglas en inglés) son un problema real y potencialmente creciente en los Estados Unidos y la prioridad principal para el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) de los Estados Unidos. Como asesor de riesgos de la nación, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) preparó esta guía para ayudar a las organizaciones con base de fe (FBO, por sus siglas en inglés) a desarrollar una estrategia de seguridad integral que puede aplicarse de acuerdo con las circunstancias únicas de cada iglesia, mezquita, sinagoga, templo y otros sitios de práctica religiosa en todo el país.

Para comprender mejor la naturaleza del problema, la CISA se basó en una investigación de código abierto para recopilar 37 incidentes de violencia dirigida que abarcaron el período de diez años de 2009 a 2019. El análisis obtenido de estos estudios de caso brinda información de manera directa para la guía que se presenta aquí y revela varias tendencias significativas.

- **La CISA observó un aumento significativo en los incidentes de violencia dirigida en 2012 y un aumento perceptible en la cantidad de incidentes entre 2015 y 2019. Como resultado de estos 37 incidentes, fallecieron 64 personas y otras 59 resultaron heridas.**
- **El cincuenta y cuatro por ciento** (n=20) **de los ataques fueron asaltos a mano armada de algún tipo, que incluye tiroteos, armas blancas y asaltos con vehículos. Cinco de los ataques calificaron como tiroteos masivos.**
- **La CISA determinó que el 67 por ciento** (n=25) **de los ataques fueron motivados por el odio hacia una identidad racial o religiosa en particular y que el 22 por ciento** (n=8) **estaba relacionado con una disputa doméstica o una crisis personal. El motivo para el 11 por ciento restante** (n=4) **es desconocido.**
- **De los 36 perpetradores conocidos en estos incidentes, el 58 por ciento** (n=21) **se involucró en algún tipo de comportamiento de planificación que indica su intención de llevar a cabo un ataque.**

Dentro de este análisis, la CISA también describe varias tácticas y métodos que los perpetradores suelen utilizar. Estas tácticas y métodos apuntan a áreas específicas de vulnerabilidad que las casas de adoración pueden abordar a través del marco de seguridad que se incluye en esta guía. *La conclusión es que las casas de adoración pueden protegerse mejor si adoptan una estrategia de seguridad integral y en varias capas.*

Para desarrollar e implementar un programa de seguridad que pueda adaptarse a las necesidades de las casas de adoración individuales, la CISA recomienda las siguientes acciones generales de seguridad:

- **Asignar funciones y responsabilidades claras para desarrollar e implementar medidas de seguridad.**
- **Realizar una evaluación de vulnerabilidades para comprender los riesgos de la casa de adoración.**
- **Desarrollar el nivel de preparación y la resiliencia de la comunidad asegurándose de que la casa de adoración sea consciente de las posibles amenazas, esté preparada para responder en caso de una emergencia o un incidente y esté conectada con la comunidad en general.**
- **Aplicar medidas de seguridad física para controlar y proteger el perímetro exterior, central e interior, al mismo tiempo que respeta el propósito de cada área de la casa de adoración.**
- **Centrarse en el cuidado de los niños con medidas de seguridad para proteger los servicios de guardería y las escuelas.**
- **Implementar las mejores prácticas de ciberseguridad para salvaguardar la información importante y prevenir un posible ciberataque.**

Estas opciones de seguridad no detendrán todas las amenazas hacia una casa de adoración, pero un enfoque de seguridad integral ofrece la mejor solución para proteger a las personas, la propiedad y los datos. Las casas de adoración deben adaptar este conocimiento a las necesidades de sus comunidades, mientras mantienen un ambiente abierto y acogedor, lo que las hace una parte fundamental de la estructura social de los Estados Unidos.

Introducción: Protección de las casas de adoración

La función singular de las casas de adoración en la sociedad estadounidense

La religión es una poderosa fuerza capaz de organizar las comunidades de todo el país. De acuerdo con el Estudio del Paisaje Religioso (Religious Landscape Study) del Centro de Investigaciones Pew (Pew Research Center), se estima que el 36 por ciento de los estadounidenses asisten a servicios religiosos todas las semanas. Si se considera a los que asisten mensual o anualmente, el número crece a un estimado del 69 por ciento. En ocasiones importantes, como bodas, funerales y fiestas religiosas, el número aumenta aún más.[1]

La libertad de religión es un derecho garantizado por la Constitución de los Estados Unidos y reconocido como una parte fundamental de la sociedad estadounidense. Las organizaciones con base de fe (FBO) desempeñan una función importante en la prestación de servicios sociales, como alimentos, vivienda y ropa, y en el fomento de un sentido general de comunidad. Para muchas personas, la fe representa fuerza y esperanza; consuelo y tranquilidad; brújula moral y guía espiritual; y triunfo sobre el estrés y el miedo.

Ese sentido de comunidad y propósito a menudo se centra de manera física en torno a una casa de adoración (HoW). Las iglesias, mezquitas, sinagogas, templos y otros sitios de práctica religiosa son lugares de refugio y acogida, con pocas restricciones en el acceso o la admisión. Sin importar su religión, las casas de adoración casi siempre están diseñadas para ser abiertas y accesibles, lo que refleja una cultura de confianza y acogedora.

Sin embargo, un ambiente acogedor no es un ambiente indefenso.

Las casas de adoración enfrentan desafíos únicos en la lucha por lograr el equilibrio adecuado entre seguridad y accesibilidad. En esta guía se ofrece contexto y orientación para que las HoW tomen decisiones informadas sobre el nivel de seguridad que mejor se adapte a sus circunstancias y ambiente.

---

1 "Attendance at religious services" (Asistencia a los servicios religiosos), Pew Research Center, https://www.pewforum.org/religious-landscape-study/attendance-at-religious-services/ (consultado el 9 de julio de 2020). Véase también "Fast Facts about American Religion" (Datos rápidos sobre la religión en Estados Unidos), Hartford Institute for Religion Research, http://hartfordinstitute.org/research/fastfacts/fast_facts.html (consultado el 4 de mayo de 2020).

Ataques a las casas de adoración

En los últimos años, los ataques a las casas de adoración en ciudades como Charleston, Sutherland Springs, Pittsburgh, Poway y Monsey impulsaron la conversación a nivel nacional sobre violencia, conflicto social y salud mental.

El análisis de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) que se presenta aquí indica que estos incidentes de violencia dirigida aumentaron durante el período de diez años de 2009 a 2019. La naturaleza de estos ataques varía en gran medida, al igual que las denominaciones de las víctimas y las regiones geográficas en las que se produjeron los ataques.

Sin embargo, la CISA destaca que estos ataques siguen siendo poco frecuentes desde el punto de vista estadístico, incluso cuando parecen estar en aumento. Cada uno es un momento de profundo trauma para las personas afectadas de manera directa y la sociedad en general. Si bien estos ataques tienen un impacto terrible, es importante mantener el vínculo social que hace que las casas de adoración sean una parte integral y única de la comunidad. Las casas de adoración pueden cumplir con muchas medidas de seguridad sin restarle valor a esa característica especial. En esta guía, se pretende ayudar a las casas de adoración a encontrar el equilibrio que mejor se adapte a sus necesidades y circunstancias únicas.

¿Qué trabajo hace el Departamento de Seguridad Nacional?

El Departamento de Seguridad Nacional (DHS) identifica seis misiones generales que comprenden su plan estratégico.[2] Tres de esas misiones (contrarrestar el terrorismo y las amenazas a la seguridad nacional, asegurar el ciberespacio y la infraestructura crítica, y fortalecer el nivel de preparación y la resiliencia) se relacionan de manera directa con las organizaciones con base de fe y las casas de adoración de nuestra nación en su esfuerzo por reducir el riesgo de violencia y prevenir los ataques dirigidos contra sus miembros e instalaciones.

En respuesta a estos ataques recientes, el DHS está aumentando sus esfuerzos con el fin de fortalecer los recursos de prevención, preparación y mitigación para las HoW al proporcionar información, capacitación, ejercicios y experiencia. En abril de 2020, el departamento designó a la Oficina de Alianzas y Participación (OPE, por sus siglas en inglés) para liderar la coordinación de seguridad de las FBO. En junio de 2020, el DHS también anunció la creación del Consejo Asesor de Seguridad con Base de Fe (FBSAC, por sus siglas en inglés) para brindar recomendaciones sobre asuntos relacionados con las casas de adoración, las organizaciones con base de fe y la seguridad nacional al secretario de Seguridad Nacional.

Esta guía es parte del esfuerzo continuo de la CISA para abordar este urgente desafío de seguridad. Debido a la naturaleza de estos ataques, esta guía también representa parte del esfuerzo más amplio del DHS para comprender y abordar mejor los actos de violencia dirigida.[3] La violencia dirigida y la seguridad de las casas de adoración son misiones cada vez más importantes en todo el Gobierno federal, así como en los Gobiernos estatales, locales,

---

2 "Strategic Planning" (Planificación estratégica), Departamento de Seguridad Nacional de EE. UU., https://www.dhs.gov/strategic-planning.

3 Departamento de Seguridad Nacional de EE. UU., *Strategic Framework for Countering Terrorism and Targeted Violence* (Marco estratégico para contrarrestar el terrorismo y la violencia dirigida), septiembre de 2019, https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence.

tribales y territoriales (SLTT, por sus siglas en inglés). Este informe se basa en el importante trabajo realizado por el Centro Nacional de Evaluación de Amenazas (NTAC, por sus siglas en inglés) del Servicio Secreto de los Estados Unidos (USSS, por sus siglas en inglés), el Centro para Iniciativas de Fe y Oportunidades del DHS y el Servicio de Relaciones Comunitarias del Departamento de Justicia (DOJ, por sus siglas en inglés) de EE. UU.

Al igual que con los actos de terrorismo, la planificación y selección de objetivos son características de la violencia dirigida y ofrecen oportunidades críticas para la prevención, intervención y mitigación de riesgos. En esta guía, la CISA analiza cómo se pueden aplicar algunos de los resultados obtenidos en trabajos anteriores acerca de la violencia dirigida, como la violencia escolar, a la planificación de seguridad de las casas de adoración.

¿Qué trabajo hace la CISA?

La Ley de la Agencia de Ciberseguridad y Seguridad de la Infraestructura de 2018 estableció a la CISA como líder de los programas, las operaciones y las políticas federales de ciberseguridad y seguridad de infraestructura crítica.[4] Como asesor de riesgos de la nación, la CISA también tiene responsabilidades sobre las reuniones públicas, que suelen tener fácil acceso y cuentan con medidas de seguridad o protección limitadas.

Una de las misiones y prioridades operativas más importantes de la CISA es proteger las reuniones públicas.[5] La CISA trabaja en conjunto con entidades privadas, lo que le permite brindar liderazgo y apoyo al identificar, desarrollar e implementar medidas innovadoras y escalables para mitigar el riesgo en lugares concurridos, incluidas las casas de adoración.

Descripción general de la guía

En esta guía se ofrecen nuevos análisis, recomendaciones y recursos. Lo que es más importante, en esta guía también se presenta un marco conceptual tanto para pensar en la seguridad de las HoW como para lograr un plan de seguridad que se adapte mejor a las circunstancias únicas de cada comunidad.

CAPÍTULO 1: Presenta un análisis basado en diez años de incidentes que involucran actos de violencia dirigida contra las casas de adoración en los Estados Unidos, incluye una descripción general de las tácticas y los métodos que los perpetradores suelen utilizar con mayor frecuencia. Los resultados de este análisis brindan información de manera directa para la guía que se ofrece en los capítulos siguientes.

CAPÍTULO 2: Describe un proceso para que las HoW independientes piensen en sus necesidades de seguridad y desarrollen una estrategia de seguridad sólida y en capas sin sacrificar las cualidades únicas que hacen que los lugares de adoración sean una parte importante de la comunidad local.

---

4 Ley de la Agencia de Ciberseguridad y Seguridad de la Infraestructura de 2018, Ley de derecho público 115-278, compilación de leyes de EE. UU. 132 (2018): 4168-4186, https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf.

5 Agencia de Ciberseguridad y Seguridad de la Infraestructura, Strategic Intent (Propósito estratégico), agosto de 2019, https://www.cisa.gov/publication/strategic-intent. Véase también "Securing Soft Targets and Crowded Places" (Cómo asegurar objetivos secundarios y lugares concurridos), Agencia de Ciberseguridad y Seguridad de la Infraestructura, https://www.cisa.gov/securing-soft-targets-and-crowded-places.

CAPÍTULO 3: Proporciona una guía específica sobre cómo realizar la *evaluación de vulnerabilidades* integral que ayudará a las HoW a evaluar la situación actual en materia de seguridad y las necesidades específicas que poseen.

CAPÍTULOS 4-7: Ofrecen análisis más detallados sobre los diferentes aspectos de la planificación de la seguridad y los componentes que podrían ser necesarios para que las HoW desarrollen una estrategia de seguridad en capas.

Por último, en el **APÉNDICE 1** se presenta una *Guía de recursos* con una lista completa de los productos que las casas de adoración pueden usar para mejorar su seguridad en general. En el capítulo se organizan los recursos por tema para que los usuarios puedan explorar la gran cantidad de opciones y decisiones que serán más beneficiosas para sus necesidades.

Los lectores también encontrarán estos recursos y materiales de referencia seleccionados a lo largo de la guía. Estos recursos, la mayoría de los cuales han sido producidos por el DHS y otros profesionales de la seguridad y el orden público, brindan la oportunidad de realizar el seguimiento y un estudio adicional para que las HoW interesadas continúen con su planificación estratégica de seguridad.

1 Interpretación del problema

Introducción

Las casas de adoración (HoW) varían en tamaño, denominación y ubicación geográfica, y cada una tiene necesidades de seguridad únicas. Esta guía es, en parte, una respuesta directa a una serie de ataques de alto perfil que llamaron la atención a nivel nacional durante los últimos años y afectaron a comunidades de todas las religiones. La guía también incluye las mejores prácticas generales para proteger a las multitudes, moderadas por las consideraciones especiales de las HoW.

Para comprender mejor cómo ha evolucionado el problema de la violencia contra los sitios de práctica religiosa durante los últimos años y abordar la gran variedad de necesidades de seguridad que existen en todo el país, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) realizó una revisión exhaustiva de la documentación y las investigaciones sobre el tema y analizó diez años de datos de investigación de código abierto, informes de los medios y bases de datos nacionales para compilar una lista de 37 incidentes de estudio de caso de 2009 a 2019. Junto con la documentación existente, estos estudios de caso revelan tendencias de alto nivel y lecciones importantes sobre las medidas que se pueden tomar para hacer que las casas de adoración sean más seguras.

Estas lecciones orientan de manera directa las opciones de seguridad descritas en esta guía. En síntesis, la investigación deja en claro que las HoW enfrentan distintos desafíos de seguridad y destacan la necesidad de un enfoque integral y en múltiples capas para la seguridad.

Revisión de la documentación y las tendencias nacionales

Algunos académicos estiman que hay entre 350.000 y 400.000 congregaciones individuales en los Estados Unidos.[1] Cada una representa una parte fundamental de la comunidad local, y las casas de adoración de todas las religiones se consideran tradicionalmente santuarios que valoran la apertura y la inclusión. Al mismo tiempo, esa apertura, importancia social y relevancia simbólica crean desafíos de seguridad únicos.

La CISA revisó documentación de una gran variedad de campos y disciplinas para esta guía, que incluye lo siguiente: informes de medios de código abierto; publicaciones académicas en revistas analizadas por colegas; informes gubernamentales, documentos y bases de datos; y artículos publicados por profesionales del orden público, en evaluaciones de amenazas y otros profesionales de la seguridad.

Las casas de adoración varían en tamaño, denominación y ubicación geográfica...

En general, el campo de la seguridad de las HoW es relativamente pequeño y existe aún menos documentación establecida sobre el problema específico de la violencia dirigida. Los profesionales de la seguridad aumentaron su atención en las necesidades de las iglesias, sinagogas, mezquitas, templos y otros sitios religiosos durante los últimos años, pero la mayor parte de la documentación producida por la industria es de naturaleza prescriptiva (en lugar de analítica).[2] Mientras tanto, los académicos acaban de iniciar investigaciones sistemáticas sobre actos de violencia dirigidos a las HoW.[3] Así como los investigadores no pueden establecer con certeza el número exacto de congregaciones individuales en los Estados Unidos, no existe una contabilización precisa de la cantidad de actos violentos dirigidos de manera deliberada hacia las casas de adoración.

Un desafío es la necesidad de un sistema de seguimiento unificado y sólido. La investigación y el análisis existentes a menudo provienen de informes de los medios o bases de datos no conectadas, como *The Violence Project* de Hamline University[4] o el programa Uniform Crime Reporting (UCR) de la Agencia Federal de Investigación (FBI, por sus siglas en inglés), que agrupa los delitos de odio notificados por las jurisdicciones locales.[5] La mayoría de los investigadores

---

1 C. Kirk Hadaway y Penny Long Marler, "How Many Americans Attend Worship Each Week? An Alternative Approach to Measurement" (¿Cuántos estadounidenses asisten a cultos todas las semanas? Un enfoque alternativo sobre la medición), *Journal for the Scientific Study of Religion* (2005), 44 (3): 307-322; Simon Brauer, "How Many Congregations Are There? Updating a Survey-Based Estimate" (¿Cuántas congregaciones existen? Actualización del cálculo basado en encuestas), *Journal for the Scientific Study of Religion* (2017) 56 (2): 438-448.

2 Jim McGuffey, Paula L. Ratliff, Doug Meacham, Phil Purpura, Dick Raisler, Carl Chinn y Alistair Calton, *Securing HoWs Around the World* (Seguridad de casas de adoración en todo el mundo) (ASIS International, 2017), https://www.asisonline.org/globalassets/get-involved/councils/documents/best-practices-securing-houses-of-worship.pdf.

3 Para consultar una breve descripción de la bibliografía académica existente, véase Christopher P. Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports" (Delitos en lugares de adoración: análisis de los informes en los periódicos de 2012), *International Review of Victimology* 22 (1), enero de 2016: 65-74, y Christopher P. Scheitle y Caitlin Halligan, "Explaining the adoption of security measures by places of worship: perceived risk of victimization and organizational structure" (Explicación de la incorporación de medidas de seguridad en lugares de adoración: riesgos percibidos de victimización y la estructura organizativa), *Security Journal* 31, julio de 2018: 685-707.

4 "The Mass Shooter Database" (Base de datos sobre tiroteos masivos), *The Violence Project*, https://www.theviolenceproject.org/.

5 "Uniform Crime Reporting Program" (Programa de notificación uniforme de la actividad delictiva), Agencia Federal de Investigación, https://www.fbi.gov/services/cjis/ucr/.

sostienen que esas bases de datos, si bien son útiles, se ven limitadas por la notificación incompleta o incoherente y plantean la hipótesis de que los incidentes registrados allí probablemente representen un conteo insuficiente.[6]

Aun así, los datos indican dos tendencias distintas: que las HoW se enfrentan a una persistente actividad delictiva dirigida y que la amenaza específica de violencia dirigida puede estar en aumento.

En un extremo del espectro se encuentra el tipo de incidentes que son comunes desde el punto de vista estadístico, pero que no representan necesariamente una amenaza para la vida. El vandalismo, por ejemplo, parece ser un problema habitual para las HoW de todo el país.[7] Sin embargo, las HoW también parecen enfrentar un cierto nivel de violencia persistente que amenaza la vida, pero que puede no cumplir con los criterios de violencia dirigida utilizados en esta guía. Una estimación basada en datos del FBI proyecta que entre 2000 y 2016 hubo alrededor de 480 incidentes violentos por año, incluidos robos a mano armada, asaltos y ataques con bombas, que dieron como resultado 46 muertes y 218 lesiones graves al año.[8]

... y cada una tiene necesidades de seguridad únicas.

En el otro extremo del espectro, está el creciente problema de los tiroteos masivos, que son poco frecuentes desde el punto de vista estadístico, pero representan la principal causa de trauma y el mayor número de víctimas mortales. Estos ataques aumentaron durante los últimos cinco años junto con la tendencia general ascendente de los tiroteos masivos en todo el país y, a menudo, cumplen con la definición de violencia dirigida (descrita a continuación). El ataque a la iglesia bautista en Sutherland Springs, por ejemplo, fue el quinto tiroteo masivo más mortífero en los Estados Unidos que se registró en *The Violence Project*.[9]

Cualitativamente, parece existir una fuerte asociación entre el entorno social y las amenazas a las HoW. El análisis histórico revela que los ataques contra distintos grupos étnicos y religiosos, y casas de adoración individuales a menudo acompañan períodos de intensas luchas raciales y religiosas. Algunos ejemplos reconocidos incluyen el ataque con bombas y la quema de iglesias de la comunidad afroestadounidense o la desfiguración y el vandalismo de sinagogas y mezquitas durante estallidos de antisemitismo y animadversión antimusulmana.[10]

---

6 Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports" (Delitos en lugares de adoración: análisis de los informes en los periódicos de 2012).

7 Christopher P. Scheitle, "Crimes occurring at places of worship: An analysis of 2012 newspaper reports" (Delitos en lugares de adoración: análisis de los informes en los periódicos de 2012), *International Review of Victimology* 22 (1), enero de 2016: 65-74; William Bourns y Wesley D. Wright, "A Study of Church Vulnerability to Violence: Implications for Law Enforcement" (Estudio sobre la vulnerabilidad de las iglesias ante la violencia: las repercusiones para los funcionarios de orden público), *Journal of Criminal Justice* 32 (2), marzo de 2004: 151–157.

8 "Serious violence at places of worship in the U.S.—Looking at the numbers" (Incidentes graves en lugares de adoración en EE. UU.: un análisis de los números), Dolan Consulting Group, 9 de septiembre de 2019, https://www.dolanconsultinggroup.com/news/serious-violence-at-places-of-worship-in-the-u-s-looking-at-the-numbers/.

9 Jillian Peterson y James Densely, "Opinion: Why do people attacks places of worship? Here's what we know from our mass shootings database" (Opinión: ¿por qué las personas atacan los lugares de adoración? Información de acuerdo con la base de datos sobre tiroteos masivos), *Los Angeles Times*, 30 de diciembre de 2019; Jilian K. Peterson y James A. Densely, "The Violence Project: Database of Mass Shootings in the United States, 1966-2019" (The Violence Project: base de datos sobre tiroteos masivos en los Estados Unidos de 1966 a 2019), noviembre de 2019, pág. 16, https://www.theviolenceproject.org/.

10 Para obtener una selección de ejemplos más recientes, consulte los siguientes documentos: John P Bartkowski, Frank M Howell y Lai Shu-Chuan, "Spatial Variations in Church Burnings: The Social Ecology of Victimized Communities in the South" (Variaciones en el espacio de iglesias incendiadas: la ecología social

Algunas señales preocupantes indican que el país está, una vez más, en un período de malestar social con un aumento simultáneo de los ataques motivados por prejuicios y delitos de odio. *Associated Press* señala que tres de los ataques más mortíferos contra las HoW han ocurrido desde 2015. Mientras tanto, el auge de las redes sociales generó un ambiente propicio para que se desarrollen los discursos de odio y las ideologías de odio en ciertos rincones de Internet.[11]

Para hacer frente a estos desafíos, el Departamento de Seguridad Nacional (DHS) destinó cada vez más recursos para abordar el problema específico de la violencia dirigida y, en septiembre de 2019, publicó *Strategic Framework for Countering Terrorism and Targeted Violence* (Marco estratégico para contrarrestar el terrorismo y la violencia dirigida) a fin de lograr una mejor coordinación de la acción del Gobierno. El informe es notable por llamar la atención sobre las amenazas a la seguridad que se originan en los Estados Unidos. El DHS identificó dos categorías amplias de especial preocupación: (1) extremistas violentos locales (HVE, por sus siglas en inglés) motivados por los mensajes y las ideologías de organizaciones terroristas extranjeras y (2) terroristas nacionales, en particular aquellos asociados con el extremismo violento de la supremacía blanca.[12] Ambas categorías representan una posible amenaza para las HoW.

Además, es posible que la pandemia de COVID-19 esté aumentando la prevalencia de los delitos de odio y los prejuicios raciales en todo el mundo occidental, lo que exacerba aún más la amenaza para las HoW y lleva a la CISA a emitir un aviso para las organizaciones con base de fe advirtiendo que "los factores estresantes causados por la pandemia pueden contribuir a la decisión de un individuo de cometer un ataque o influir en la elección del objetivo".[13]

Junto con los ataques más aleatorios e impredecibles provocados por crisis personales y domésticas, la creciente prevalencia de ataques motivados por el odio, que se representan en las figuras 1 (pág. 13) y 2 (pág. 14), representa un grave riesgo para las HoW en los Estados Unidos.

---

de las comunidades víctimas del sur), *Rural Sociology* 67 (4), diciembre de 2002: 578–602; Yehudut Barsky, "Terrorist Incidents and Attacks Against Jews and Israelis in the United States" (Incidentes y ataques terroristas contra la comunidad israelí y judía de EE. UU.), Community Security Service, 2016, https://jewishpgh.org/app/uploads/2018/09/Terrorist-Attacks-Against-Jews-in-US-1969-2016.pdf; American Civil Liberties Union, "Nationwide Anti-Mosque Activity" (Actividad en contra de las mezquitas a nivel nacional), diciembre de 2019, https://www.aclu.org/issues/national-security/discriminatory-profiling/nationwide-anti-mosque-activity.

11 Adeel Hassan, "Hate-Crime Violence Hits 16-Year High, FBI Reports" (Los delitos de odio alcanzaron el nivel más alto en 16 años, de acuerdo con el FBI), New York Times, 12 de noviembre de 2019; Agencia Federal de Investigación, "2018 Hate Crime Statistics" (Estadísticas sobre delitos de odio en 2018), https://ucr.fbi.gov/hate-crime/2018/hate-crime; Gary Fields y David Crary, "Year-end violence highlights danger of worshipping" (Aspectos importantes sobre la violencia anual en los cultos), *Associated Press*, 1 de enero de 2020; Marc Fisher, Roxana Popescu y Kayla Epstein, "Ancient hatreds, modern methods: How social media and political division feed attacks on sacred spaces" (Odio antiguo, método moderno: cómo las redes sociales y la división política alientan los ataques a lugares sagrados), Washington Post, 28 de abril de 2019.

12 Departamento de Seguridad Nacional de EE. UU., *Strategic Framework for Countering Terrorism and Targeted Violence* (Marco estratégico para contrarrestar el terrorismo y la violencia dirigida), septiembre de 2019, https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence.

13 Anna Russel, "The rise of coronavirus hate crimes" (El aumento de los delitos de odio durante el coronavirus), New Yorker, 17 de marzo de 2020; Natasha Bertrand, "DHS warns pandemic 'stressors' could trigger attacks on HoWs" (El DHS advierte que los factores estresantes de la pandemia pueden desatar ataques a las HoW), *Politico*, 8 de abril de 2020.

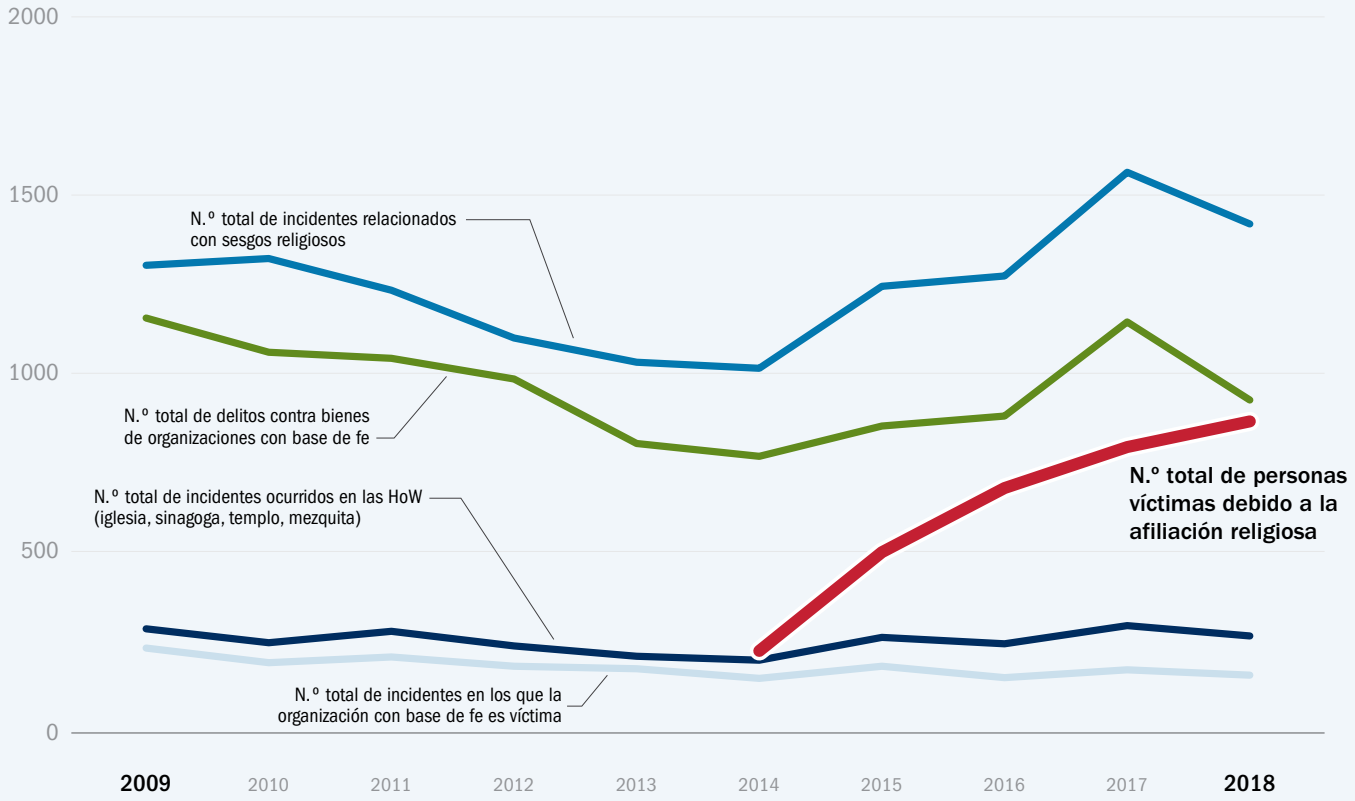


Figura 1. Datos de delitos de odio del FBI: incidentes con sesgo religioso y selección de las HoW

En la figura 1 se muestra una serie de categorías recopiladas en los datos de delitos de odio del FBI relacionadas con los sesgos religiosos. La línea azul media (superior) representa el número total de incidentes de delitos de odio por sesgos religiosos. La línea verde representa el número de delitos relacionados con la propiedad cometidos en contra de las organizaciones con base de fe. La línea roja representa la cantidad de personas víctimas (que incluye asesinatos/homicidios, violación, asalto agravado, asalto simple, intimidación y otros) por motivos de afiliación religiosa, una categoría distinta que el FBI comenzó a registrar en 2014. La línea azul claro (inferior) representa la cantidad de incidentes en los que una organización con base de fe se registra como víctima. La línea azul oscuro (la segunda desde abajo) representa el número total de incidentes de delitos de odio que ocurren en las HoW. Los datos de 2019 no estaban disponibles en el momento de la publicación.

En conjunto, estas tendencias de datos brindan información valiosa sobre el carácter general de la vida cívica estadounidense y la prevalencia de los delitos de odio relacionados con la religión.

Fuente: Estadísticas de delitos de odio del FBI UCR, tablas 1, 7, 8 y 10 https://www.fbi.gov/services/cjis/ucr/hate-crime.

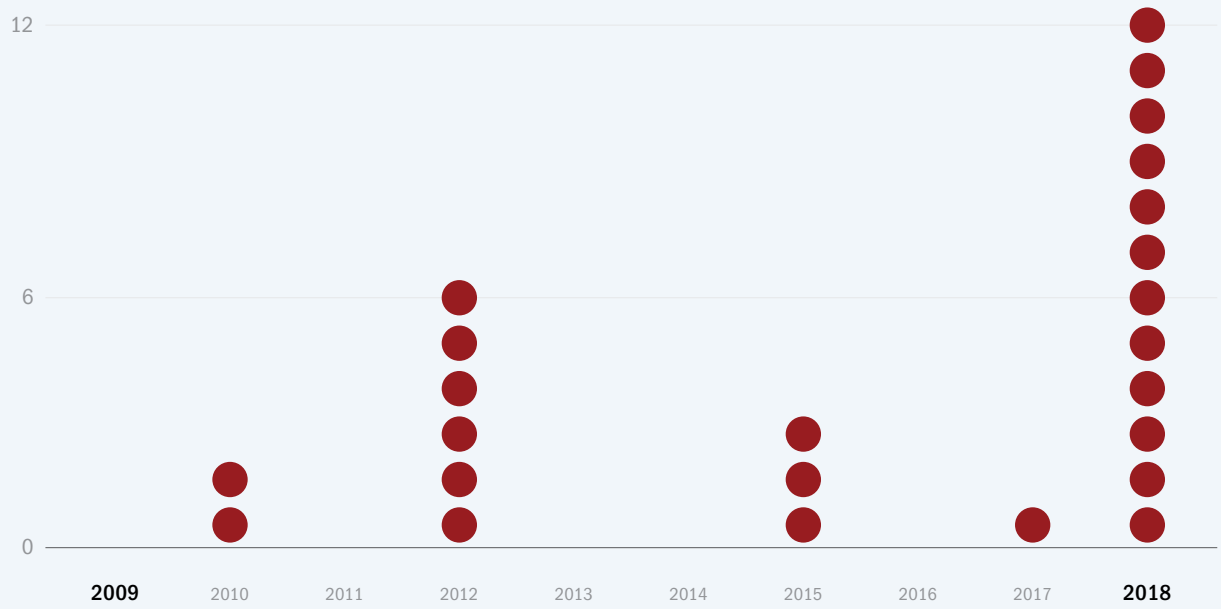


Figura 2. Datos de delitos de odio del FBI: personas asesinadas debido a su afiliación religiosa

En la figura 2 se muestra la cantidad de personas asesinadas por motivos de afiliación religiosa y prejuicios según las estadísticas de delitos de odio del FBI. Este número se incluye como un subconjunto de la cantidad total de personas víctimas debido a su afiliación religiosa que se refleja en la figura 1.

Fuente: Estadísticas de delitos de odio del FBI UCR, tabla 7, https://www.fbi.gov/services/cjis/ucr/hate-crime.

Metodología para la elaboración de estudios de caso

Con el fin de complementar la investigación existente y proporcionar contexto para las consideraciones de seguridad que se incluyen en esta guía, la CISA desarrolló una serie de estudios de caso para registrar la violencia dirigida contra las HoW durante el período de diez años entre 2009 y 2019. La CISA reunió estos incidentes a través de una búsqueda exhaustiva en diversas fuentes, que incluyen las estadísticas de delitos de odio del FBI (parte del programa UCR); el Bomb Arson Tracking System (BATS) de la Oficina de Control de Bebidas Alcohólicas, Tabaco, Armas de Fuego y Explosivos (ATF, por sus siglas en inglés); Technical Resource for Incident Prevention (TRIP*wire*) del DHS; la base de datos sobre terrorismo mundial de University of Maryland; y *The Violence Project* de Hamline University. Sin embargo, la CISA extrajo la mayoría de los estudios de caso de informes de medios de código abierto, que proporcionaron la información pública más sustancial disponible. Aunque algunos detalles eran limitados o estaban incompletos, la CISA corroboró los hechos esenciales con múltiples fuentes, siempre que ha sido posible.

Con el fin de diferenciar los actos de violencia deliberada de los actos delictivos aleatorios, la CISA utilizó la siguiente definición como criterio para la inclusión en estos estudios de caso: *un acto de violencia dirigida contra una casa de adoración o propiedad afiliada en los Estados Unidos que genera daños, lesiones o víctimas mortales.*

La cantidad de casos que cumplieron con los criterios de inclusión fue relativamente pequeña en comparación, por ejemplo, con los datos ofrecidos en las estadísticas sobre delitos de odio del FBI. Por lo que la CISA anticipa que hay incidentes adicionales que no se incluyeron ni se evaluaron en esta guía.

Violencia dirigida

La violencia dirigida se refiere a la violencia hacia un objetivo y enfocada en individuos, grupos o lugares específicos. Los perpetradores seleccionan sus objetivos para lograr motivos específicos, como la resolución de un reclamo o hacer una declaración política o ideológica. La violencia dirigida es distinta a la violencia que es impulsiva, aleatoria o espontánea y, a menudo, se distingue por indicadores claros o comportamientos de planificación previos al ataque. Esos comportamientos, si se detectan, pueden ser útiles para frustrar o mitigar un incidente.

El marco estratégico del DHS de 2019 define la violencia dirigida de la siguiente manera:

> … cualquier incidente de violencia que implique a la seguridad nacional o actividades del DHS, y en las que un atacante conocido o que se puede conocer selecciona un objetivo en particular antes del ataque violento. A diferencia del terrorismo, la violencia dirigida incluye ataques que carecen de una motivación política, ideológica o religiosa claramente perceptible, pero que son de tal gravedad y magnitud que sugieren la intención de infligir un grado de lesiones, destrucción o muerte masivas de acuerdo con las tácticas terroristas conocidas.[14]

Definición operativa para su inclusión en los estudios de caso

A los efectos de este análisis, la CISA se centró en los incidentes en los Estados Unidos durante el período de 2009 a 2019 y definió "un acto de violencia dirigida contra una HoW" como cualquier incidente en el que un perpetrador selecciona de manera deliberada a una HoW como objetivo para:

1. Matar o herir a una o más personas afiliadas a la HoW, que incluye al clero, el personal y a los feligreses.
2. Causar daños importantes a la propiedad de la HoW.
3. Participar en delitos cibernéticos dirigidos a la HoW, incluidos actos como intrusiones en la red, piratería de programas informáticos, robo de identidad, fraude financiero y suplantación de identidad.

---

14 Departamento de Seguridad Nacional de EE. UU., *Strategic Framework for Countering Terrorism and Targeted Violence* (Marco estratégico para contrarrestar el terrorismo y la violencia dirigida), septiembre de 2019, pág. 4. Véase también Robert A. Fein, Bryan Vossekuil y Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence" (Evaluación de la amenaza: un enfoque para prevenir la violencia dirigida), *Research in Action* (Instituto Nacional de Justicia, Departamento de Justicia de EE. UU.), julio de 1995.

Este análisis se limita a los incidentes de violencia dirigida y **NO** incluye lo siguiente:

- **Incidentes en los que no se pudo identificar a un perpetrador o no se pudo determinar un interés enfocado en la HoW.**
- **Incidentes que generaron daños menores a la propiedad.**
- **Incidentes de agresiones leves, robo, grafiti, hurto, etc.**
- **Incidentes relacionados con violencia de pandillas, violencia por drogas u otros incidentes con una conexión criminal independiente.**
- **Violencia de la comunidad circundante que invadió la propiedad de la HoW por casualidad.**
- **Actos espontáneos e impulsivos que no fueron planeados y en los que la HoW no era el objetivo específico.**

Estudios de caso de incidentes

Una búsqueda detallada produjo un total de 37 incidentes independientes que cumplieron con la definición operativa. Aunque una comprensión integral de las tendencias nacionales requiere más datos, estos estudios de caso ofrecen un comienzo y una aproximación sobre cómo evolucionó la violencia dirigida contra las HoW durante la última década. Más importante aún, el estudio en profundidad de estos estudios de caso aporta información importante sobre las tácticas y los métodos utilizados por los atacantes. Si se aplican de manera correcta, esos conocimientos pueden ayudar a anticipar vulnerabilidades y mitigar amenazas.

Para obtener una lista completa de los incidentes, consulte el APÉNDICE 2.

Descripción general de los incidentes

En general, la CISA descubrió que la violencia dirigida contra las casas de adoración tiene motivaciones ideológicas religiosas, raciales y personales, y que afecta a las HoW de todos los tamaños y denominaciones. Los incidentes que se analizaron aquí ocurrieron en 20 estados de todo el país e incluyeron ubicaciones urbanas y rurales, como se indica en la figura 4 (págs. 18-19).

Aunque no es determinante, una cronología de los estudios de caso (figura 5, pág. 18) confirma los informes de los medios que muestran un aumento en los incidentes de violencia contra las HoW durante el período de 10 años de 2009 a 2019. Esta cronología revela que, si bien la cantidad de incidentes de esta magnitud no aumentó todos los años, hubo un aumento notable en la cantidad de ataques entre 2015 y 2019, lo que indica que la violencia contra las casas de adoración sigue siendo una amenaza genuina para el pueblo estadounidense.

Tipos de ataques

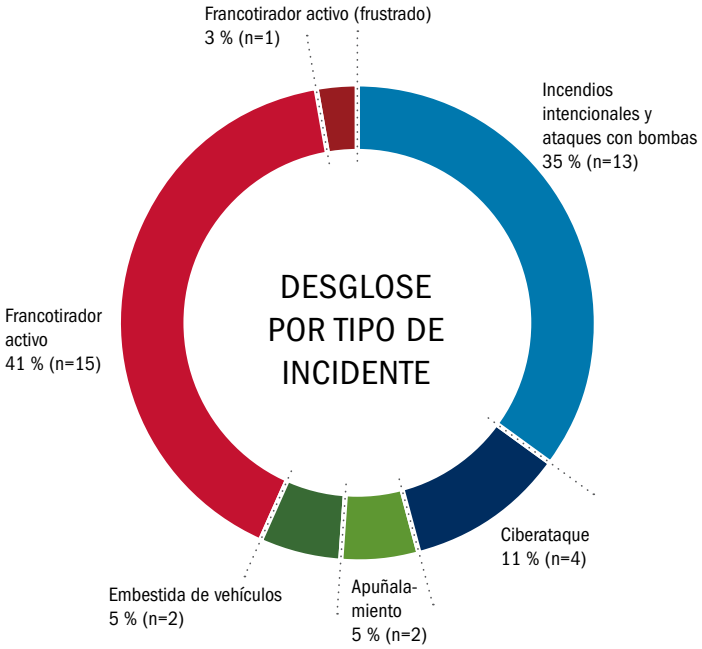
La CISA examinó distintos tipos de incidentes, incluidos tiroteos activos, apuñalamientos, ciberataques, incendios intencionales, ataques con bombas y embestidas de vehículos, que se muestran en la figura 3. Más de la mitad (54 por ciento, n=20) de los estudios de caso identificados representan un asalto a mano armada de algún tipo, como tiroteos, ataques con armas blancas y con vehículos. En este estudio se incluye el incidente frustrado de un francotirador activo como una herramienta de capacitación importante sobre las estrategias de desescalada que todas las HoW pueden tener en cuenta.

Los atacantes utilizaron distintas armas, desde pistolas y cuchillos hasta explosivos o dispositivos incendiarios y herramientas de explotación de redes, para llevar a cabo sus ataques. Las pistolas eran el arma más común (n=16), seguido por los dispositivos incendiarios (n=6) y los ciberataques (n=4).

Las figuras 4 y 5 (págs. 18-19) muestran los ataques según la ubicación y el año en que ocurrió cada incidente.

Figura 3. Tipos de ataques

En la figura 3 se muestra el desglose por tipos de ataques que se ajustan a los criterios de la CISA con respecto a los actos de violencia dirigida contra una casa de adoración.



Incendios intencionales y ataques con bombas

La CISA identificó 13 incidentes de incendios intencionales o ataques con bombas. Aunque cada uno representa una categoría distinta de ataque, las agencias federales, como la ATF y la Oficina para la prevención de atentados con bomba (OBP, por sus siglas en inglés) de la CISA, suelen registrar juntos los incendios intencionales y los ataques con bombas. El análisis de estos 13 incidentes reveló una combinación de dispositivos, incluido el uso de aceleradores de gasolina (n=4), dispositivos incendiarios improvisados (IID, por sus siglas en inglés), como bombas Molotov (n=6), y artefactos explosivos improvisados (IED, por sus siglas en inglés), como bombas caseras (n=1). Uno de los ataques incluyó tanto un IID como un IED. En tres de los ataques, cada uno de los cuales fue un incendio intencional, no se registró el tipo de material acelerador o inflamable que se utilizó. La CISA determinó que el 85 por ciento (n=11) de estos ataques fueron motivados por el odio hacia una determinada identidad religiosa o racial.

Estos 13 incidentes representan un fenómeno mucho más grande. La mayoría de los casos de incendios intencionales tienen como objetivo edificios después del horario comercial normal y, por lo general, tienen la intención de infligir daños a la propiedad. Por otro lado, en los casos de los ataques con bombas, los perpetradores suelen tener la intención de dañar a las personas reunidas en un lugar específico. Históricamente, tanto los incendios intencionales como los ataques con bombas se han utilizado durante mucho tiempo para atacar las casas de adoración en los Estados Unidos, y las amenazas de bomba a menudo sirven como herramienta de intimidación. La CISA anticipa que puede haber casos adicionales de incendios intencionales y ataques con bombas dirigidos contra las HoW durante este período de diez años, pero que no se incluyeron en este análisis.

TIPOS DE INCENDIOS INTENCIONALES Y ATAQUES CON BOMBAS:

3 NO SE REGISTRÓ EL ACELERADOR

4 USO DE ACELERADORES DE GASOLINA

6 DISPOSITIVOS INCENDIARIOS IMPROVISADOS

1 DISPOSITIVOS EXPLOSIVOS IMPROVISADOS

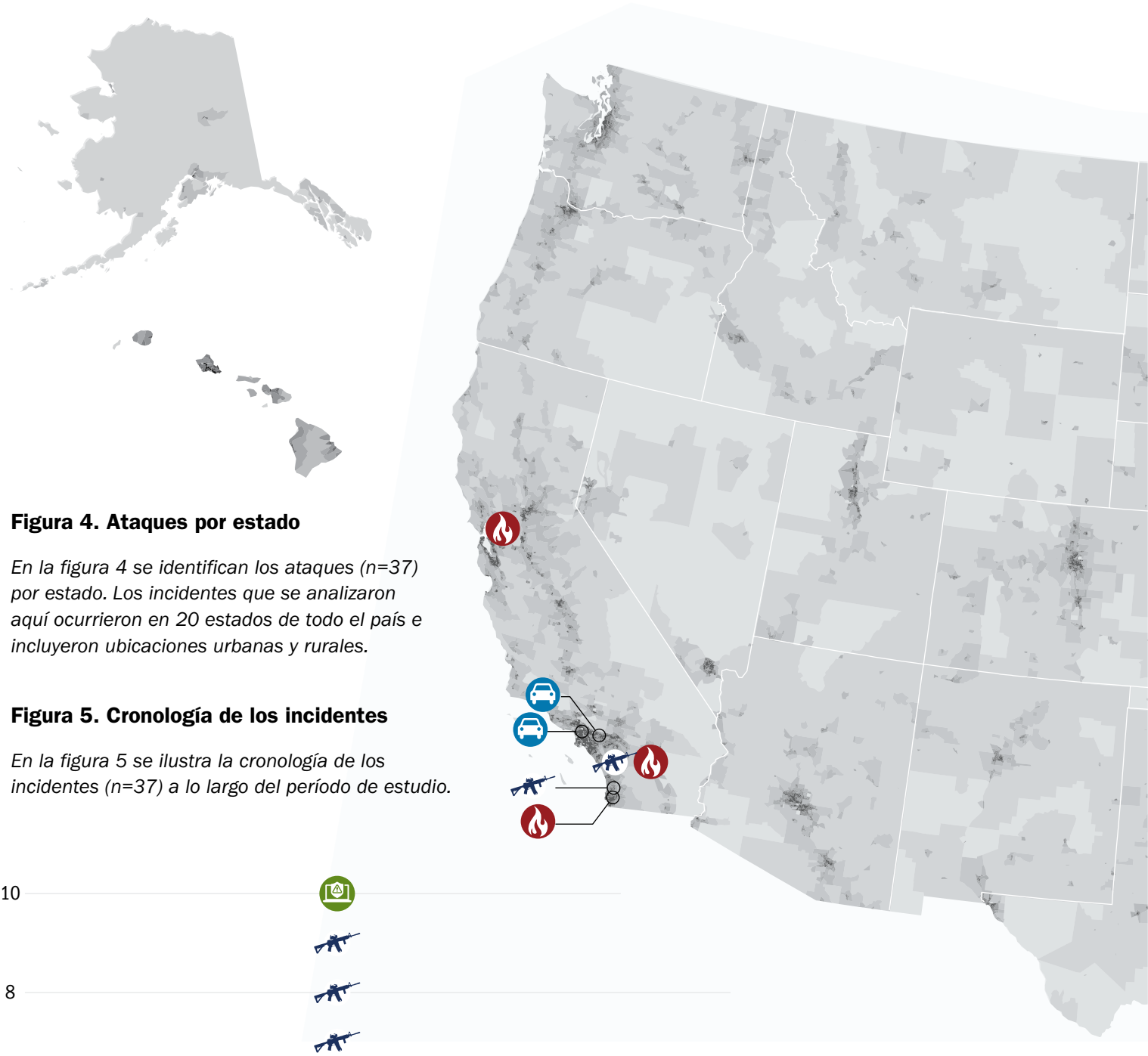
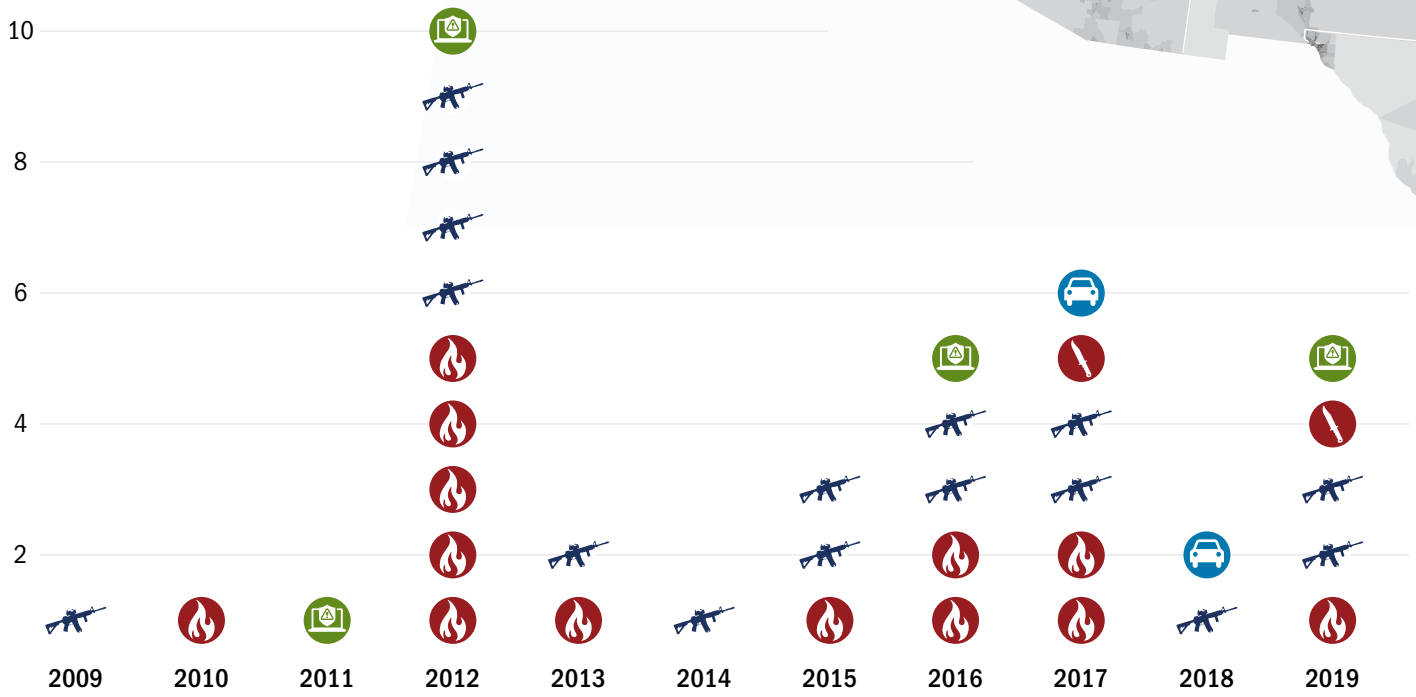


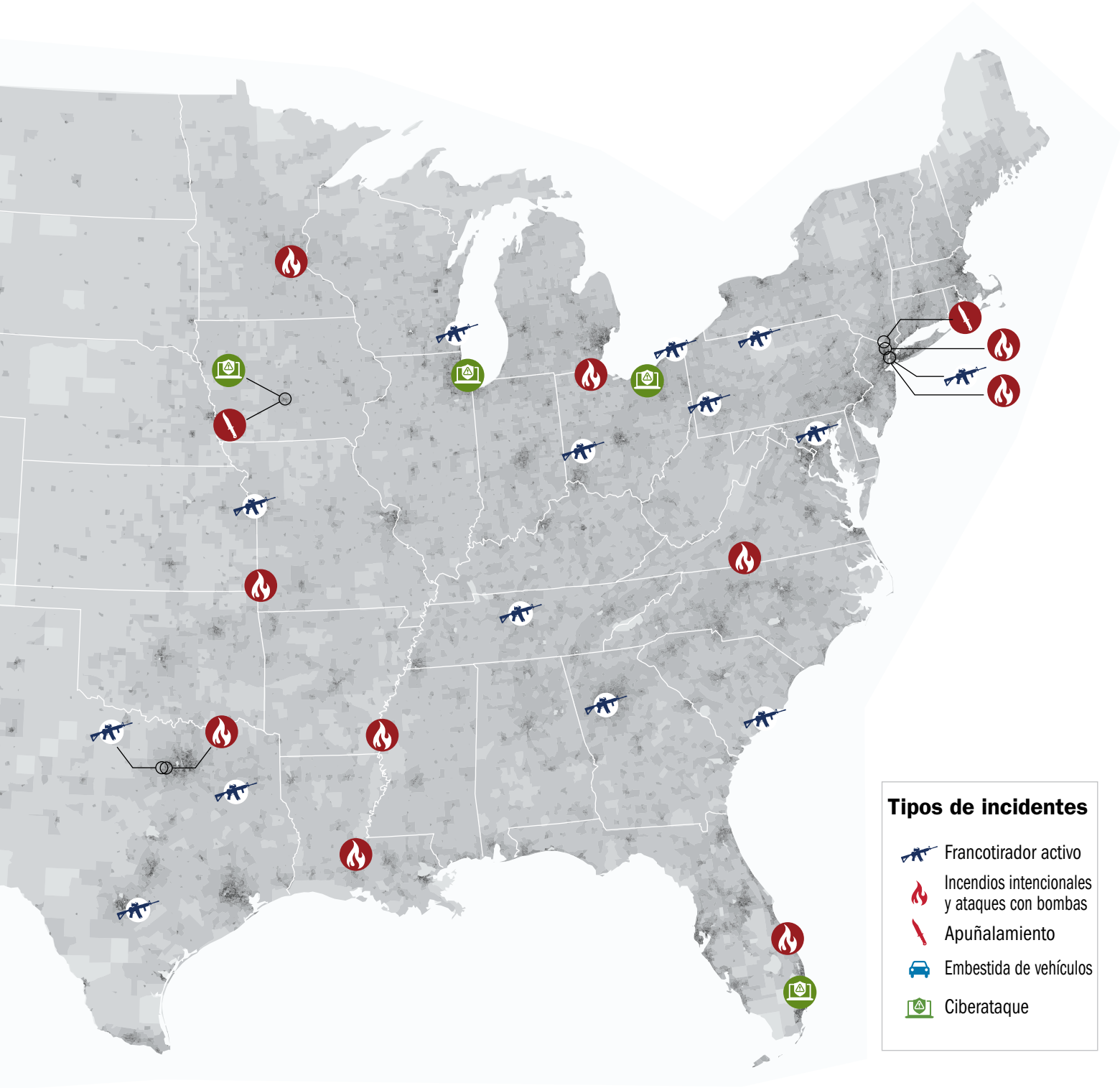
Figura 4. Ataques por estado

En la figura 4 se identifican los ataques (n=37) por estado. Los incidentes que se analizaron aquí ocurrieron en 20 estados de todo el país e incluyeron ubicaciones urbanas y rurales.

Figura 5. Cronología de los incidentes

En la figura 5 se ilustra la cronología de los incidentes (n=37) a lo largo del período de estudio.




Tipos de incidentes
Francotirador activo
Incendios intencionales y ataques con bombas
Apuñalamiento
Embestida de vehículos
Ciberataque
Población por milla cuadrada
1
10
50
200
500
1.000
2.000
4.000

Ciberataques

La CISA revisó cuatro ciberataques a las HoW, incluidos dos incidentes de sistemas financieros y dos incidentes de desfiguración de sitios web. Los daños financieros a las HoW fueron de $680.000 y $1.750.000 respectivamente, así como la preocupación y el daño a la reputación que resultó de la desfiguración del sitio web. Como ocurre en la mayoría de los delitos cibernéticos, se desconoce al perpetrador de los ataques. No está claro si las desfiguraciones del sitio web y los ataques financieros tuvieron una motivación ideológica o son crímenes de oportunidad.

Asaltos a mano armada y tiroteos masivos

De los casos examinados, el 54 por ciento (n=20) se calificó como algún tipo de asalto a mano armada, ya sea con una pistola, un cuchillo o un vehículo que se usó de manera deliberada para dañar a las personas en una HoW. Los tiroteos masivos se incluyen en los datos de asaltos a mano armada y representan los incidentes con la mayor cantidad de víctimas mortales. Las definiciones de tiroteo masivo varían, pero suelen implicar el uso de un arma de fuego para matar o herir a cuatro o más personas al mismo tiempo y en el mismo lugar. En este informe, se incluyen quince eventos en los que participaron francotiradores activos y cinco tiroteos masivos.

Los tiroteos masivos que se identificaron para este informe incluyeron varias tácticas y métodos comunes y se utilizaron para orientar muchas de nuestras recomendaciones. Consulte la figura 6 para ver la cronología de estos incidentes.

EVENTOS DE TIROTEOS MASIVOS:

En agosto de 2012, un hombre de 40 años armado con una pistola comenzó a disparar afuera del templo sij de Wisconsin en Oak Creek. Luego, ingresó y continuó disparando a los miembros de la congregación. La policía se enfrentó al francotirador cuando salía del edificio. Seis personas perdieron la vida y cuatro personas, incluido un policía, sufrieron heridas. El francotirador se suicidó después de que los oficiales que asistieron a la emergencia le dispararon en el estómago.

En abril de 2014, un hombre de 73 años armado con dos pistolas y una escopeta comenzó a disparar en el estacionamiento del Jewish Community Center en el área metropolitana de la ciudad de Kansas, en Overland Park, Kansas, donde mató a dos personas. Luego, condujo hasta la comunidad de jubilados Village Shalom cercana y abrió fuego en el estacionamiento donde mató a una persona. Nadie más resultó herido. La policía detuvo al francotirador, quien luego recibió la sentencia de muerte.

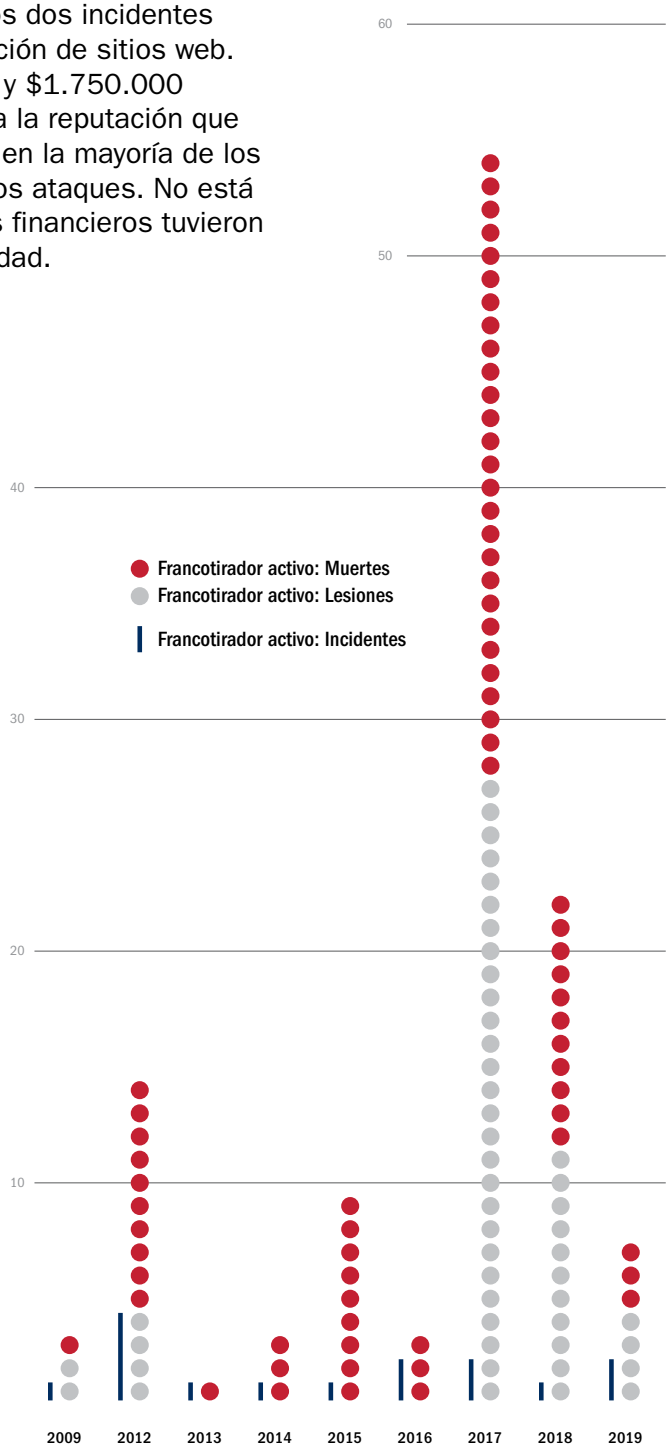


Figura 6. Cronología de incidentes con francotiradores activos

La figura 6 ilustra la cronología de los incidentes en los que participaron francotiradores activos incluidos en el análisis (Tiroteos activos n=15). El aumento significativo de muertes y lesiones en 2017 se debió al tiroteo masivo en Sutherland Springs, Texas, en el que murieron 26 personas y 20 resultaron heridas.

En junio de 2015, un hombre de 21 años armado con una pistola comenzó a disparar durante un servicio de oración en la Iglesia Episcopal Metodista Africana Emanuel en Charleston, South Carolina, y mató a nueve personas. El francotirador huyó del lugar, y los funcionarios de orden público lo detuvieron al día siguiente. Recibió una sentencia de muerte.

En noviembre de 2017, un hombre de 26 años vestido con un equipo táctico completo y armado con un rifle salió de su vehículo y comenzó a disparar frente a First Baptist Church en Sutherland Springs, Texas. Entró al edificio por una puerta lateral y continuó disparando a los miembros reunidos en el interior. Al salir, un vecino que tenía un arma de fuego se enfrentó al atacante, lo que provocó una persecución en automóvil. Al final, 26 personas perdieron la vida y 20 sufrieron heridas. El francotirador se suicidó. Fue el ataque más mortífero contra una casa de adoración en la historia de Estados Unidos.

En octubre de 2018, un hombre de 46 años armado con un rifle y tres pistolas comenzó a disparar dentro de la sinagoga Tree of Life en Pittsburgh, Pensilvania. Once personas murieron y seis sufrieron heridas, incluidos cuatro funcionarios de orden público. La policía detuvo al francotirador en la escena después de intercambiar disparos. Los fiscales acusaron al perpetrador de cometer un delito de odio; y está esperando su juicio.

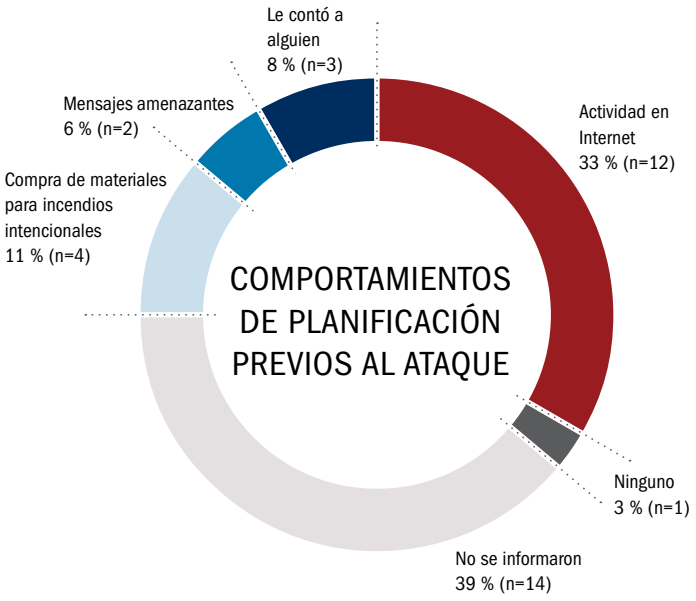


Figura 7. Comportamientos de planificación previos al ataque

En la figura 7 se ilustran los comportamientos de planificación previos al ataque exhibidos por los perpetradores de los incidentes que se incluyen en el análisis.

Resultados de los ataques

Como resultado de estos 37 incidentes, fallecieron 64 personas, otras 59 resultaron heridas, y 14 incidentes provocaron daños importantes a la propiedad. La cantidad de muertes por incidente oscila entre 0 y 27, y la cantidad de heridos oscila entre 0 y 20. Los incidentes en los que participaron francotiradores activos produjeron la mayor cantidad de víctimas en relación con todos los otros tipos de ataques.

Los perpetradores

La CISA identificó a 36 perpetradores individuales en los 37 incidentes. Los individuos responsables llevaron a cabo 30 de los ataques, tres conspiradores perpetraron un incidente, dos conspiradores perpetraron un ataque, y los cuatro ciberataques no tuvieron un perpetrador identificado. Los 36 atacantes tenían entre 17 y 73 años, con una edad promedio de 38 años. Un atacante era mujer; los otros 35 eran hombres. De los 36 atacantes, el 67 por ciento (n=24) era blanco, el 22 por ciento (n=8) era negro, el 5 por ciento (n=2) era asiático y el 5 por ciento (n=2) no se identificó según su raza en la cobertura del incidente. La CISA utilizó los estándares de la Oficina del Censo de EE. UU. para definir la raza en esta guía.

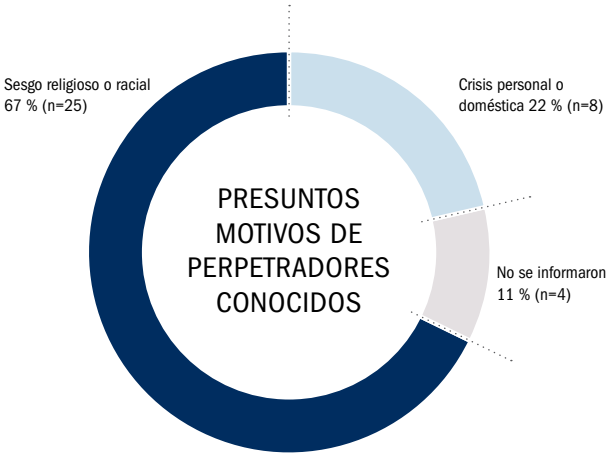


Figura 8. Presuntos motivos de perpetradores conocidos

En la figura 8 se muestra el desglose de los presuntos motivos para cada uno de los 36 perpetradores conocidos.

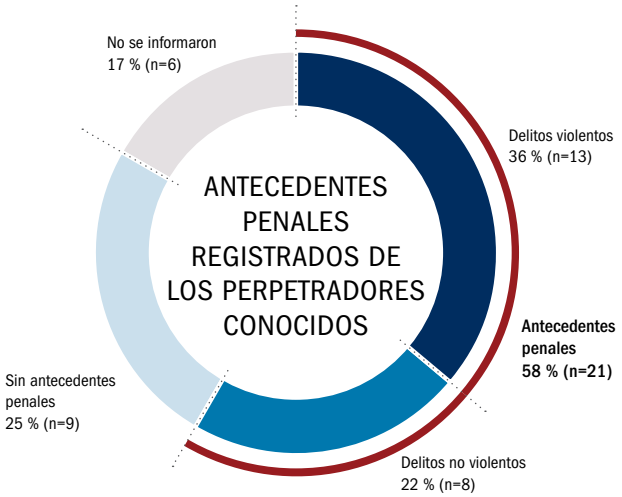


Figura 9. Antecedentes penales registrados de los perpetradores conocidos

En la figura 9 se muestra la cantidad de perpetradores conocidos que se cree que tienen antecedentes penales (58 por ciento en total, n=21), como se informó en los medios, con una distinción adicional entre delitos violentos y no violentos.

Los informes de los medios indican que el 58 por ciento (n=21) de los perpetradores participaron en algún tipo de comportamiento de planificación previo al ataque que indicaba su intención de atacar, ya sea contándole directamente a alguien, dejando mensajes amenazantes a la HoW, comprando los materiales necesarios para el ataque (como incendiarios) o describiendo sus planes en un foro en Internet. En la figura 7 (pág. 21) se muestran estos comportamientos.

La CISA concluyó que el 69 por ciento (n=25) de los perpetradores (n=36) estaban motivados por el odio hacia una identidad racial o religiosa asociada con la casa de adoración seleccionada. Los atacantes a menudo revelaron motivos específicos en comentarios hechos durante o después del ataque, y muchos se identificaron a sí mismos como portadores de sentimientos de odio. La CISA determinó que el 22 por ciento (n=8) de los perpetradores estaban motivados por una disputa doméstica o una crisis personal, incluidos varios casos de posibles crisis de salud mental u otros factores estresantes individuales. Cada tipo de motivación, ilustrado en la figura 8, tiende a producir diferentes conjuntos de comportamientos previos a la planificación y ofrece diferentes oportunidades para la detección e intervención tempranas, como se describe en capítulos posteriores.

El historial de actividad delictiva o los problemas de salud mental, a veces, pueden utilizarse como indicadores de comportamiento futuro. De los 36 perpetradores individuales incluidos en estos estudios de caso, 21 tenían antecedentes penales de algún tipo según lo descrito por miembros de la familia, testigos, tribunales o informes de los medios de comunicación y, de acuerdo con la notificación del incidente, se cree que 14 de los individuos experimentaron un problema de salud mental, ya sea algún tiempo antes del incidente o en el transcurso de este. Consulte la figura 9 para ver el desglose de los perpetradores con antecedentes penales.

Casas de adoración específicas

De los 37 incidentes, el 54 por ciento (n=20) eran instituciones cristianas, el 24 por ciento (n=9) instituciones musulmanas, el 19 por ciento (n=7) instituciones judías y el 3 por ciento (n=1) instituciones sij, como se muestra en la figura 10. El análisis de la CISA determinó que el 65 por ciento de los ataques (n=25) ocurrió dentro del edificio principal de una HoW; los incidentes restantes (n=12) tuvieron lugar en instalaciones relacionadas, como centros comunitarios religiosos, residencias, estacionamientos o sistemas informáticos de las HoW involucradas.

Durante los asaltos a mano armada (n=20), el 40 por ciento (n=8) de los perpetradores comenzaron su ataque dentro del edificio principal durante el servicio de adoración. En el 45 por ciento (n=9) de los ataques a mano armada, testigos o miembros de la congregación intentaron intervenir con el perpetrador antes de que lleguen funcionarios de orden público.

En el 22 por ciento (n=8) del total de incidentes, el perpetrador tenía alguna relación previa con la HoW, como se indica en la figura 11. En el 78 por ciento restante de los incidentes (n=29), no hubo relación previa, lo que sugiere la necesidad de un protocolo de bienvenida sólido y bien definido como se describe en el capítulo 4.

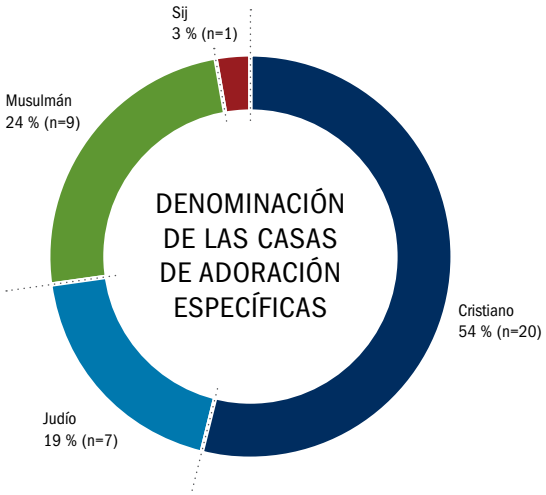


Figura 10. Denominación

En la figura 10 se muestra el desglose de las denominaciones de las casas de adoración específicas.

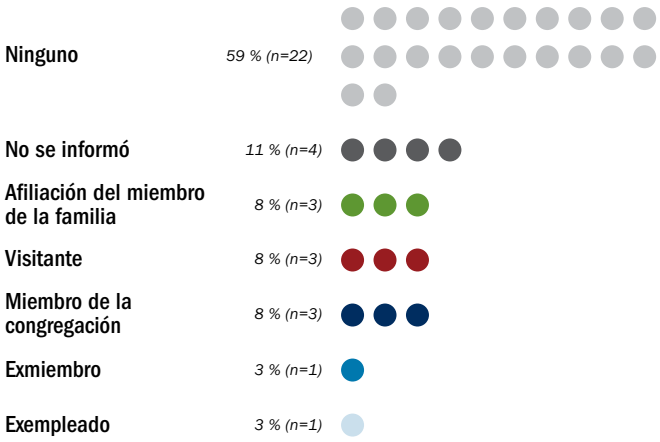


Figura 11. Relación con la instalación

En la figura 11 se muestra el desglose de la cantidad de incidentes en los que el perpetrador tenía alguna relación previa con la HoW que recibió el ataque.

Tácticas y métodos del perpetrador

Como parte de este análisis, la CISA examinó las tácticas y los métodos que los perpetradores utilizaron para llevar a cabo los ataques. Varias de las tácticas y los métodos identificados brindan información sobre los esfuerzos que una HoW podría realizar para prevenir o mitigar los posibles incidentes. Estos van desde vulnerabilidades específicas que el perpetrador aprovechó hasta tendencias de comportamiento individuales importantes que una HoW debe considerar al fomentar la participación de la comunidad.

En la siguiente sección, se brinda una breve descripción de varios incidentes, con un enfoque en las características distintivas que las casas de adoración podrían considerar al revisar sus procedimientos de seguridad.

RELACIÓN PREVIA

22 % En el 22 por ciento (n=8) de los casos, el perpetrador tenía alguna relación previa con la HoW.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En 2012, un hombre buscó y mató a su exesposa en su antigua iglesia. Entró al edificio durante los servicios y le disparó mientras ella tocaba el órgano. El francotirador salió de la iglesia y regresó unos minutos más tarde para dispararle dos veces más a la víctima antes de que los testigos lo detuvieran.

DESCRIPCIÓN GENERAL DEL INCIDENTE

Durante diez noches en abril de 2019, un individuo incendió tres iglesias bautistas históricamente afroestadounidenses. El individuo responsable publicó fotos y videos de los delitos en las redes sociales en tiempo real. Animado por las reacciones en Internet a los dos primeros ataques, el perpetrador llevó a cabo un tercer incendio intencional y lo arrestaron después de que los investigadores vincularan la evidencia de los delitos a los datos del teléfono celular y a compras recientes de gasolina y otros materiales inflamables. El perpetrador se declaró culpable de múltiples delitos de odio e incendios intencionales.

INDICADORES DE COMPORTAMIENTO

57 % En el 57 por ciento (n=21) de los casos, el perpetrador participó en algún tipo de comportamiento de planificación que reveló su intención de atacar.

19 % En el 19 por ciento (n=7) de los casos, el perpetrador publicó sus planes en foros en Internet relacionados con la supremacía blanca.

INCENDIOS INTENCIONALES Y ATAQUES CON BOMBAS

LOS INCENDIOS Y ATAQUES CON BOMBAS OCURRIERON MIENTRAS LOS FELIGRESES ESTABAN EN EL EDIFICIO

8 % En el 8 por ciento (n=3) de los casos, se produjo un incendio intencional mientras había personas en el edificio.

DESCRIPCIÓN GENERAL DEL INCIDENTE

Durante un incidente en 2017, los atacantes rompieron una ventana exterior de una mezquita y arrojaron una bomba casera y una mezcla de aceleradores en el edificio. En el momento del ataque, había feligreses en el edificio para las oraciones de la mañana. Sin embargo, la oficina en la que se arrojó la bomba estaba desocupada y no hubo víctimas fatales ni heridos.

CASOS DE INCENDIOS INTENCIONALES QUE OCURRIERON LA NOCHE DESPUÉS DE LOS SERVICIOS

24 % En el 24 por ciento (n=9) de los casos, se produjo un incendio intencional durante la noche o fuera del horario comercial.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En 2017, un asaltante irrumpió en una iglesia durante la noche y pasó varias horas destruyendo la propiedad, ventanas y muebles antes de incendiar todo el edificio. La policía recibió una llamada para investigar un robo en curso y llegó en el momento del incendio. El incendio se extinguió con rapidez, pero la iglesia resultó con daños graves.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En 2014, ocurrieron incidentes en los estacionamientos de dos ubicaciones diferentes. El atacante primero condujo hasta un centro comunitario judío y comenzó a disparar en el estacionamiento, donde mató a dos personas. El personal dentro de la instalación inició procedimientos de cierre de inmediato, aseguró las puertas exteriores y llevó a los visitantes a las habitaciones interiores. Un policía fuera de servicio que trabajaba en seguridad lo enfrentó, y el atacante condujo hasta una comunidad de jubilados cercana, donde le disparó a otra persona en el estacionamiento antes de que los funcionarios de orden público lo detuvieran.

ASALTO A MANO ARMADA

EL ATAQUE OCURRIÓ EN EL EXTERIOR

11 % En el 11 por ciento (n=4) de los casos, el ataque ocurrió, en su totalidad, en el estacionamiento o en el exterior del edificio.

EL FRANCOTIRADOR SE TRASLADÓ DEL PERÍMETRO EXTERIOR HACIA EL INTERIOR DEL SANTUARIO

8 % En el 8 por ciento (n=3) de los casos, el ataque comenzó en el perímetro exterior o central y se trasladó hacia el santuario interior de la casa de adoración.

DESCRIPCIÓN GENERAL DEL INCIDENTE

Durante un incidente en 2017, el francotirador estacionó afuera de una iglesia y esperó a que terminaran los servicios. El atacante le disparó a una mujer que caminaba hacia su automóvil antes de ingresar por las puertas principales de la casa de adoración y les disparó a otras seis personas dentro del santuario. Después del incidente, las renovaciones incluyeron cambios en el diseño para permitir que los feligreses vieran la entrada principal durante los servicios.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En diciembre de 2019, un gran grupo se reunió en la casa de un rabino de New York para celebrar el final de Hanukkah cuando un hombre con problemas mentales entró en la casa y atacó a las personas reunidas con un machete. Los feligreses se defendieron y varias personas resultaron gravemente heridas en el tumulto que se generó. Un hombre murió más tarde a causa de sus heridas. El atacante huyó e intentó ingresar a la sinagoga de al lado, pero personas que escucharon la conmoción habían cerrado las puertas con llave. El atacante se escapó, pero luego lo detuvo la policía.

EL ATAQUE OCURRIÓ FUERA DEL SERVICIO FORMAL

14 % En el 14 por ciento (n=5) de los casos, el ataque tuvo lugar fuera del servicio de adoración principal.

EL FRANCOTIRADOR COMENZÓ EL ATAQUE DESPUÉS DE INICIADO EL SERVICIO DE ADORACIÓN

19 % En el 19 por ciento (n=7) de los casos, el ataque ocurrió durante el servicio de adoración principal.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En septiembre de 2017, un hombre armado con dos pistolas se acercó a una iglesia cuando finalizaban los servicios. Al parecer, en busca de venganza por el tiroteo en la iglesia de Charleston de 2015, el hombre disparó y mató a una mujer en el estacionamiento. Luego, ingresó al edificio por una puerta trasera y disparó e hirió a otras seis personas. Un ujier se enfrentó al hombre armado, quien se disparó accidentalmente durante la lucha. El ujier pudo someter al francotirador herido hasta que llegó la policía.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En 2019, un hombre armado ingresó a una casa de adoración durante una importante festividad religiosa portando equipo táctico, un rifle de asalto y al menos 50 rondas de municiones. El atacante disparó y mató a una persona e hirió a tres antes de que el rifle se atascara, luego huyó.

LOS ATACANTES SELECCIONARON UNA HoW DURANTE LOS PERÍODOS DE MAYOR ASISTENCIA (P. EJ., SERVICIOS FESTIVOS)

22 % En el 22 por ciento (n=8) de los casos, el ataque ocurrió durante una festividad religiosa o en alguna fecha cercana.

EL FRANCOTIRADOR PASÓ POR EL SERVICIO ANTES DEL ATAQUE

8 % En el 8 por ciento (n=3) de los casos, el ataque ocurrió después de que el perpetrador se sentara durante parte del servicio de adoración.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En un incidente de 2019, el francotirador se sentó durante parte del servicio de adoración antes de pararse con una escopeta, disparar y matar a una persona que estaba cerca. El agresor vestía un disfraz evidente y su comportamiento sospechoso llamó la atención del equipo de seguridad de voluntarios de la HoW, quienes respondieron de inmediato y sometieron al atacante.

DESCRIPCIÓN GENERAL DEL INCIDENTE

Durante una festividad religiosa de 2012, una casa de adoración fue víctima de un ciberataque en el que una persona desconocida destrozó la página de inicio de la HoW y redirigió a los visitantes a un sitio que expresaba su apoyo a un conocido grupo terrorista. La desfiguración del sitio web incluyó imágenes perturbadoras y mensajes presuntuosos de los delincuentes cibernéticos.

CIBERATAQUE

DESFIGURACIÓN DEL SITIO WEB

5 % En el 5 por ciento (n=2) de los casos, el ataque involucró la desfiguración de un sitio web de una HoW.

EXPLOTACIÓN FINANCIERA

5 % En el 5 por ciento (n=2) de los casos, el ataque involucró una explotación financiera.

DESCRIPCIÓN GENERAL DEL INCIDENTE

En 2019, una campaña de suplantación de identidad tuvo como objetivo una casa de adoración, en la que falsificaron el correo electrónico de un proveedor y redirigieron los pagos mensuales de la HoW a una cuenta fraudulenta. El ataque generó una pérdida financiera significativa y solo se descubrió cuando la empresa "real" llamó para preguntar sobre los pagos atrasados.

TÁCTICA Y MÉTODOS

Táctica o método	Porcentaje de incidentes	Recomendaciones	Descripción del evento
INDICADORES DE COMPORTAMIENTO			
El perpetrador presentó un comportamiento de planificación que indica su intención de atacar	**57 %** (n=21)	Capacitación para identificar actividades sospechosas **Capítulo 4**	Más de la mitad de los perpetradores revelaron su intención de atacar a través de acciones o palabras.
RELACIÓN PREVIA			
El perpetrador tenía alguna relación previa con la HoW	**22 %** (n=8)	Programas de bienestar y capacitación de bienvenida **Capítulo 4**	Los miembros de la comunidad de la HoW conocían a un número considerable de atacantes, pero la mayoría no tenía ninguna asociación previa.
ASALTO A MANO ARMADA			
El ataque ocurrió en el exterior	**11 %** (n=4)	Control del acceso **Capítulo 5**	Los ataques, que incluyeron incidentes con francotiradores activos y ataques vehiculares, ocurrieron, en su totalidad, en el estacionamiento o en el exterior del edificio de la HoW.
El francotirador participó del servicio antes del ataque	**8 %** (n=3)	Capacitación de bienvenida **Capítulo 4**	En cada caso, el agresor se sentó durante parte del servicio antes de atacar a los feligreses.
El francotirador se trasladó del perímetro exterior hacia el interior	**8 %** (n=3)	Capacitación sobre francotiradores activos y control del acceso **Capítulo 4 y 5**	En cada caso, el agresor comenzó a disparar en el estacionamiento y continuó el ataque mientras avanzaba hacia el interior del santuario principal.
El francotirador comenzó el ataque dentro del edificio principal durante el servicio de adoración.	**19 %** (n=7)	Capacitación sobre francotiradores activos **Capítulo 4**	Los atacantes ingresaron al edificio principal con el único propósito de dañar a los feligreses, ya sea de forma indiscriminada o porque sabían que su objetivo individual estaba allí.
El agresor atacó durante períodos en los que se esperaba una asistencia mayor de la normal (p. ej., servicios festivos)	**22 %** (n=8)	Mayor seguridad durante eventos concurridos **Capítulo 4**	Los perpetradores planearon estos ataques en torno a una gran cantidad de feligreses.
El ataque ocurrió durante actividades ajenas al culto (p. ej., grupos de colaboradores, teatro comunitario)	**14 %** (n=5)	**Capítulo 4**	El agresor optó por atacar a los feligreses durante las reuniones de grupos pequeños.
INCENDIOS INTENCIONALES Y ATAQUES CON BOMBAS			
Los ataques con bombas ocurrieron mientras los feligreses estaban en el edificio	**8 %** (n=3)	Capacitación para identificar actividades sospechosas **Capítulo 4**	Los perpetradores tenían la intención de dañar a la mayor cantidad posible de feligreses al atacar durante los servicios de adoración.
Los casos de incendios intencionales que ocurrieron durante la noche, después de los servicios	**24 %** (n=9)	CCTV con iluminación exterior visible **Capítulo 5**	La mayoría de los casos de incendios intencionales ocurrieron después del horario comercial y, a menudo, provocaron importantes daños a la propiedad.
CIBERATAQUE			
Planes financieros (p. ej., programas de chantaje, suplantación de identidad)	**5 %** (n=2)	Resiliencia cibernética **Capítulo 7**	Los planes financieros generaron pérdidas de casi $2,5 millones.
Desfiguración del sitio web	**5 %** (n=2)	Resiliencia cibernética **Capítulo 7**	En ambos casos, los perpetradores desfiguraron sitios web para demostrar el apoyo a grupos terroristas extranjeros.

La seguridad en la práctica

En los siguientes capítulos, la CISA destaca las mejores prácticas generales y ejemplos de los estudios de caso en los que las HoW tenían las herramientas y los procedimientos para responder de manera efectiva a medida que se desarrollaban los ataques. Algunas instalaciones tenían directores de seguridad designados y programas formales de capacitación establecidos; otras tenían un equipo de seguridad de voluntarios que realizaba simulacros de respuesta a emergencias de manera habitual y estaba a cargo de la protección de otros feligreses durante el incidente. En algunas instalaciones se iniciaron procedimientos de cierre después de que comenzaron los ataques. En varios casos, la capacitación sobre francotiradores activos salvó vidas porque los líderes y feligreses sabían cómo responder y ayudaron a otros a escapar o esconderse. Busque los recuadros de "La seguridad en la práctica" que contienen ejemplos de las lecciones aprendidas y mejores prácticas.

De acuerdo con las tácticas y los métodos identificados, las recomendaciones de la CISA para las HoW contienen muchas pautas tangibles para elaborar una estrategia de seguridad en niveles, realizar evaluaciones de la vulnerabilidad, desarrollar una cultura de seguridad organizativa, mejorar la seguridad física, fortalecer la preparación de la ciberseguridad y desarrollar una guía para la seguridad en las guarderías y escuelas, cuando corresponda.

LA SEGURIDAD EN LA PRÁCTICA

PLANIFICACIÓN DE ACCIONES DE EMERGENCIA

Después de un ataque, un centro comunitario afiliado brindó un apoyo fundamental a las víctimas y sus familias en cuestión de horas. Los líderes de los centros comunitarios enfatizaron que contar con un plan de respuesta ante emergencias ya establecido resultó esencial para albergar y cuidar a las víctimas.

Resumen

Los estudios de caso que se analizan aquí brindan una perspectiva de la violencia dirigida contra las HoW que ha ocurrido en los Estados Unidos durante un período de diez años. Aunque es poco frecuente desde el punto de vista estadístico, cada uno fue un momento de profundo trauma, tanto para las víctimas como para la sociedad en general. A pesar de que son eventos traumáticos, también representan una oportunidad para aprender sobre las fuerzas que dan forma a la sociedad estadounidense, la motivación de los atacantes y, lo que es más importante, sobre los pasos que las casas de adoración pueden seguir para proteger mejor la vida y la propiedad.

2 Desarrollo del enfoque integral de la seguridad

Introducción

Los expertos enfatizan de manera constante la necesidad de que las casas de adoración (HoW) adopten un enfoque integral y en capas para la seguridad.[1] Esa tarea puede parecer una perspectiva desalentadora y potencialmente costosa para las comunidades que carecen del conocimiento específico. Sin embargo, desarrollar una estrategia de seguridad integral es bastante simple con el marco de referencia adecuado, y la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) está aquí para ayudarlo.

En este capítulo, la CISA proporciona un marco para pensar en la seguridad de su HoW y comenzar a planificar el futuro.

La planificación de la seguridad es un acto de equilibrio complejo entre el costo, la cultura y la necesidad. La forma más confiable de resolver esas demandas contrapuestas y tomar decisiones acertadas y rentables es desarrollar un plan que se base en una sólida comprensión de los conceptos básicos de la planificación de seguridad y los desafíos únicos que existen en cada casa de adoración.

¿Qué es el enfoque integral de la seguridad y cómo se logra?

Los profesionales de la seguridad a veces hablan sobre el concepto de *seguridad empresarial*, un término que suele usarse con mayor frecuencia en el ámbito cibernético. En la práctica, solo significa adoptar un enfoque integral de las necesidades de seguridad de toda una organización.

Un programa de seguridad efectivo nunca es unidimensional.

Otra forma de pensar en esta idea es considerar la seguridad de la HoW como un esfuerzo integral que se basa en la suma de sus partes y abarca todos los diferentes aspectos de los edificios, la comunidad y las actividades. Cada uno de esos aspectos y actividades de la organización necesita alguna medida de protección. Al mismo tiempo, también es importante conocer las diversas amenazas, los riesgos y las vulnerabilidades que pueden presentarse en su HoW.

---

1 Hady Mawajdeh, "Experts Encourage Layered Approach to Church Security Protocols" (Los expertos recomiendan un enfoque en capas para los protocolos de seguridad de las iglesias), *NPR*, 3 de enero de 2020; Scott Stewart y Fred Burton, "Security at Places of Worship: More than a Matter of Faith" (Seguridad en los lugares de adoración: no es solo una cuestión de fe), *Stratfor*, 17 de junio de 2009.

En la práctica, avanzar hacia una solución y desarrollar una estrategia de seguridad integral significa considerar (o tal vez revisar) una serie de medidas necesarias para mantener segura la casa de adoración. Esto incluye seguridad física, ciberseguridad, concienciación comunitaria, planificación de eventos, gestión de incidentes, preparación para emergencias, desarrollo de políticas, capacitación y recursos humanos.

En el resto de este capítulo se describen los conceptos clave, las consideraciones y los distintos pasos que lo ayudarán a desarrollar un enfoque de seguridad sólido, inclusivo y en varias capas.

Preguntas, términos y conceptos clave

La variedad de medidas que podrían ser necesarias para mantener segura a su congregación puede parecer abrumadora. Comience por hacer una serie de preguntas básicas que lo ayudarán a aclarar su situación actual en materia de seguridad y cualquier cambio que pueda ser necesario:

- **¿Cuáles son las amenazas y vulnerabilidades?**
- **¿Cuál es la probabilidad de que ocurra una determinada amenaza?**
- **¿Cuáles son las consecuencias si esas amenazas ocurren?**
- **¿Cuál es la tolerancia de su comunidad con respecto a las consecuencias asociadas?**
- **¿Cuál es la actitud de su comunidad hacia las prácticas de seguridad?**
- **¿Qué recursos de personal tiene para dirigir, administrar y supervisar las operaciones de seguridad?**
- **¿Cuál es su presupuesto para respaldar las iniciativas de seguridad, ya sean inmediatas o a largo plazo?**

RIESGO, AMENAZA, VULNERABILIDAD Y CONSECUENCIA

El riesgo, las amenazas, la vulnerabilidad y las consecuencias tienen distinciones importantes que debe tener en cuenta al desarrollar la estrategia de seguridad. Puede pensar que la relación entre estos conceptos es de la siguiente manera: ***riesgo = amenaza × vulnerabilidad × consecuencia.***

El Departamento de Seguridad Nacional (DHS) define específicamente estos términos de la siguiente manera:

RIESGO: La posibilidad de tener un resultado no deseado a causa de un incidente, evento o suceso determinado por su probabilidad y las consecuencias asociadas. El riesgo es una función de la amenaza, vulnerabilidad y consecuencia.

AMENAZA: Suceso natural o provocado por el hombre, un individuo, una entidad o acción que tiene o indica la capacidad y la intención de dañar la vida, la información, las operaciones, el entorno o la propiedad.

VULNERABILIDAD: Característica física o atributo operativo que hace que una entidad esté abierta a la explotación o sea susceptible a un determinado peligro.

CONSECUENCIA: Efecto de un evento, incidente o suceso.

Departamento de Seguridad Nacional de EE. UU., *DHS Risk Lexicon, edición 2010* (septiembre de 2010), https://www.cisa.gov/dhs-risk-lexicon.

Este tipo de preguntas brinda información para cualquier tipo de proyecto de seguridad empresarial. Las casas de adoración también deben enfrentar consideraciones especiales adicionales debido a la naturaleza única del ambiente de amenaza y la preferencia general por mantener un ambiente abierto, pacífico y acogedor.

Al iniciar este proceso, es importante considerar algunas de las siguientes dinámicas que le brinden información para la estrategia general y el enfoque:

LA NATURALEZA PARTICULAR DE LA VIOLENCIA DIRIGIDA CONTRA LAS HoW. Como sitios de práctica religiosa, las casas de adoración tienen una gran importancia simbólica dentro de la comunidad y, por lo tanto, pueden atraer la atención hostil de los posibles perpetradores. El análisis de la CISA indica con claridad que la ideología o las crisis personales constituyen la motivación de la mayoría de los incidentes de violencia dirigida contra las HoW, algunos de los cuales pueden ser detectados e intervenidos a tiempo.

CONCIENCIACIÓN SOBRE AMENAZAS. La mayoría de las casas de adoración suelen estar en sintonía con los ritmos y las actitudes de las comunidades a las que sirven y son una parte fundamental de la sociedad. Adoptar esa función puede ser un activo importante para mejorar la seguridad al aumentar la concienciación sobre las tensiones sociales o crisis personales que podrían anunciar un incidente violento.

LA CAPACIDAD DE INTERVENIR ANTE LAS SOSPECHAS DE AMENAZAS. Si bien la participación de la comunidad es la mejor manera de aumentar la concienciación, para actuar contra una amenaza potencial a menudo se necesitan asociaciones formales con otras casas de adoración (incluidas las de diferentes religiones), grupos comunitarios, funcionarios de orden público y proveedores de servicios sociales. Debe evaluar el tipo de asociaciones formales que mantiene la HoW como parte de este proceso.

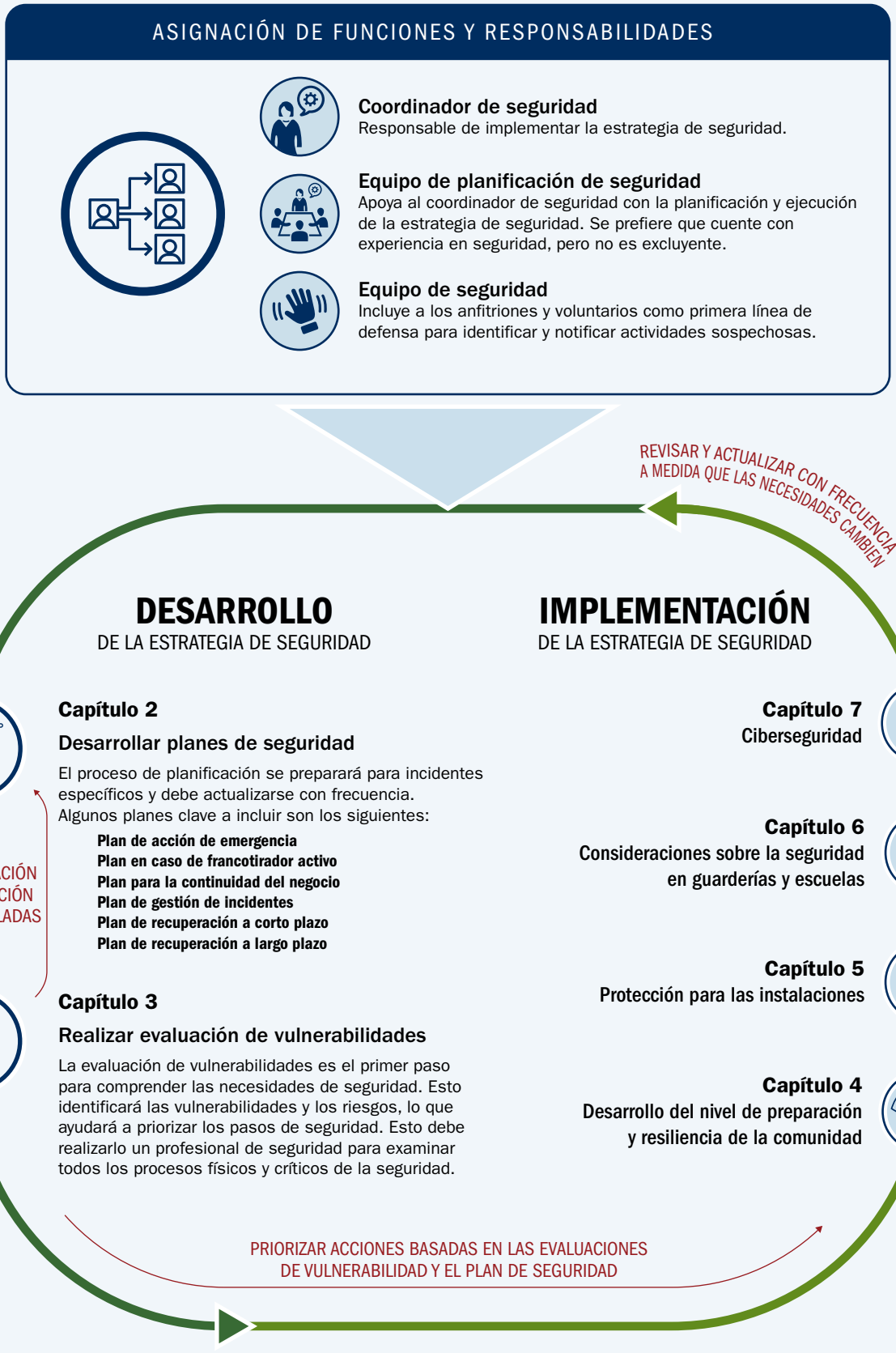
EL EQUILIBRIO ENTRE PRACTICIDAD, APERTURA Y SEGURIDAD. Ninguna casa de adoración quiere ser una fortaleza. Deberá decidir usted mismo, junto con su comunidad y de acuerdo con sus valores, cómo lograr el equilibrio entre la creación de un entorno seguro y uno abierto. Sin embargo, la elección no es absoluta, y el marco que se ofrece en esta guía pretende ayudarlo a encontrar el equilibrio adecuado para su casa de adoración.

Estos son temas complejos que requieren deliberación interna, debate filosófico, análisis de costo-beneficio y, en última instancia, la creación de consenso entre las partes interesadas clave dentro de cada casa de adoración. La conclusión es que un programa de seguridad efectivo nunca es unidimensional y se logra mejor a través de un proceso constante de análisis y (re)evaluación.

Busque las flechas rojas a lo largo de todo el informe que resaltan las fuentes en las que puede obtener más información.

Un buen lugar para comenzar a pensar en estas consideraciones especiales son los informes HOUSES OF WORSHIP: HOMETOWN SECURITY REPORT SERIES (Casas de adoración: serie de informes de seguridad nacional) (mayo de 2017) de la CISA, en los que se ofrece orientación específica sobre cómo las comunidades religiosas pueden conectarse, planificar, capacitarse y realizar informes para mejorar la seguridad. La CISA continúa desarrollando un CONJUNTO DE RECURSOS DE SEGURIDAD para organizaciones con base de fe (FBO) y HoW.

Marco de seguridad para casas de adoración



Marco para desarrollar una estrategia de seguridad integral

La CISA recomienda varios pasos importantes a lo largo del resto de la guía para que las casas de adoración logren una estrategia de seguridad integral. Este proceso comienza con el establecimiento de funciones y responsabilidades claras para implementar procedimientos de seguridad y requiere una evaluación regular.

Primeros pasos: Asignación de funciones y responsabilidades

Establecer funciones, responsabilidades y expectativas claras es fundamental para el éxito. El primer paso para desarrollar una estrategia de seguridad integral es determinar quién supervisará el programa. Si bien las obligaciones y los títulos específicos pueden diferir según las circunstancias únicas de cada HoW, esta persona, el *coordinador de seguridad*, suele ser la persona principal que toma las decisiones relacionadas con la seguridad y está a cargo de supervisar los detalles diarios del programa de seguridad. Idealmente, será un miembro del personal a tiempo completo o parcial o un voluntario comprometido con experiencia profesional relevante.

La planificación es una de las partes más importantes del proceso.

La CISA recomienda formar un *Equipo de planificación de seguridad* para apoyar al coordinador de seguridad al realizar investigaciones, evaluar las necesidades, brindar recomendaciones y ayudar con el desarrollo del plan. Este grupo debe representar a la HoW e incluir al clero, al personal y a los miembros de la congregación. El Equipo de planificación de seguridad puede ser útil para diversos propósitos y debe brindar ayuda en la planificación y la implementación.

Al identificar candidatos para estos puestos, considere encuestar al personal y a los miembros con el fin de identificar profesionales internos cuya experiencia podría brindar información para el proceso de planificación. Por ejemplo, si la comunidad tiene profesionales en el campo de la seguridad, el orden público, la salud mental, la preparación para emergencias o la gestión de incidentes, su conocimiento y experiencia pueden reforzar sus esfuerzos y ayudar a construir asociaciones formales. Otros conjuntos valiosos de habilidades incluyen el desarrollo de políticas, la planificación estratégica, las finanzas y la contabilidad, y la capacitación. Uno de los desafíos es diseñar un proceso que fomente el pensamiento crítico y la innovación, mientras se delega autoridad para evitar sobrecargar a los voluntarios.

Además, la CISA recomienda que las HoW tengan en cuenta las consideraciones de seguridad y protección para la mayor variedad de personas afiliadas a la HoW, como feligreses, voluntarios, anfitriones, ujieres y personal de mantenimiento, etc. Este grupo puede constituir un *Equipo de seguridad* más grande para ayudar a llevar a cabo el programa de seguridad y protección. Si bien la mayor parte de la toma de decisiones estaría a cargo del coordinador de seguridad y el Equipo de planificación de seguridad, el Equipo de seguridad es fundamental para crear una cultura de seguridad más amplia y garantizar que toda la comunidad de la HoW participe en la conversación general sobre seguridad. Esto podría incluir todo, desde cómo miran los anfitriones para identificar actividades sospechosas, hasta identificar quién es responsable de cerrar las puertas cuando no hay actividades.

El proceso de planificación

Para desarrollar e implementar una estrategia de seguridad eficaz se requiere tiempo, y la planificación es una de las partes más importantes del proceso. El objetivo es desarrollar una estrategia integral a largo plazo, por lo que es más importante avanzar de manera reflexiva y deliberada en cada paso que hacerlo con rapidez.

Hay dos actividades principales que entran en la etapa de planificación y están vinculadas. El objetivo principal al iniciar este proceso es identificar sus vulnerabilidades y comenzar a desarrollar un plan para abordarlas.

Las necesidades de cada casa de adoración son diferentes.

En el capítulo 3 se brindan más detalles sobre la *Evaluación de vulnerabilidades*, la cual lo ayudará a identificar las amenazas específicas que podrían existir en su comunidad y la exposición a ciertos riesgos. La evaluación de vulnerabilidades es el primer paso en el proceso de planificación. El siguiente paso es comenzar a hacer planes para abordar esas vulnerabilidades e implementar una estrategia de seguridad dinámica y de múltiples capas.

El proceso de planificación y la evaluación de vulnerabilidades son tareas distintas, pero están estrechamente vinculadas. Una le brinda información a la otra y, en muchos aspectos, el proceso nunca termina porque una característica clave de una estrategia de seguridad receptiva es revaluar las necesidades y modificar los planes periódicamente.

A medida que avanza en el proceso de planificación más amplio y comienza a implementar la estrategia de seguridad, es posible que desee considerar el desarrollo de una serie de planes relacionados para tipos específicos de situaciones e incidentes. Para obtener más información sobre la planificación avanzada, consulte el capítulo 4.

Los componentes de la estrategia de seguridad integral: Cómo proteger la casa de adoración

El proceso de planificación es parte de un ciclo y una estrategia a largo plazo, y es probable que la evaluación de vulnerabilidades revele una lista (potencialmente larga) de necesidades y deseos. Algunos se pueden abordar de inmediato, pero otros llevarán tiempo. Todos sus planes requerirán cierto nivel de organización y priorización. Esta guía tiene el propósito de ayudarlo a formular los juicios necesarios.

En cada uno de los capítulos restantes de esta guía se analiza un componente clave diferente de la estrategia de seguridad integral y se destacan los recursos federales, cuando es posible; todo con un énfasis general en el desarrollo de un enfoque reflexivo, inclusivo y en múltiples capas para la planificación de la seguridad.

CAPÍTULO 3: Se proporcionan más detalles y orientación sobre cómo realizar la *evaluación de vulnerabilidades* integral, que lo ayudará a comprender las formas en que su HoW podría estar expuesta al riesgo.

CAPÍTULO 4: Se describe la forma en que el *desarrollo del nivel de preparación y resiliencia de la comunidad* puede ofrecer protección al educar a su comunidad, establecer asociaciones y hacer cambios en las prácticas y los comportamientos generales dentro de la casa de adoración.

CAPÍTULO 5: Se ofrece un marco sobre la *Protección para las instalaciones* y se insta a las HoW a pensar cómo se puede mejorar la seguridad física mediante cambios en el perímetro exterior, central e interior de la propiedad, los terrenos y los edificios.

CAPÍTULO 6: Se describe el cuidado especial que se debe tener en las *Consideraciones sobre la seguridad en guarderías y escuelas*, cuando corresponda.

CAPÍTULO 7: Se ofrece una introducción a la *Ciberseguridad* para las casas de adoración. A menudo, esta es una vulnerabilidad que se pasa por alto, pero que se puede abordar y mitigar mediante el desarrollo de una cultura de higiene cibernética y la aplicación de una serie de recursos gratuitos y de fácil acceso.

Por último, en el **APÉNDICE 1** se presenta una *Guía de recursos* con una lista completa de los productos que puede usar para mejorar la seguridad general de la casa de adoración.

Resumen: Lograr una estrategia de seguridad integral

La planificación de la seguridad es una tarea complicada y las necesidades de cada casa de adoración son diferentes. El propósito de la CISA no es hacer de esta guía un manual completo y de una sola fuente, sino proporcionar un marco integral para desarrollar una estrategia de seguridad sólida e integral. Aunque las posibilidades de que su casa de adoración sufra un ataque son pocas, los preparativos descritos aquí pueden salvar vidas y aplicarse a distintas situaciones de emergencia en caso de que ocurra un incidente.

3 Realización de una evaluación integral de la vulnerabilidad

Introducción

Realizar una evaluación integral de la vulnerabilidad es un paso crítico en el desarrollo de un programa de seguridad sólido, y el proceso es tan importante como los resultados que se obtengan. En la evaluación que se describe aquí se identifican las características y prácticas de seguridad existentes, se determinan las amenazas y vulnerabilidades actuales, y se destacan las áreas que deben mejorarse.

La evaluación debe considerar el panorama de amenazas exclusivo de cada casa de adoración (HoW) y considerar las posibles situaciones que involucren francotiradores activos, embestidas de vehículos, dispositivos explosivos improvisados (IED) o un IED en vehículos (VBIED, por sus siglas en inglés), incendios intencionales, armas blancas y ciberataques, por mencionar algunos casos. Las HoW con escuelas o guarderías en el lugar deben tener en cuenta los desafíos únicos asociados a las instituciones educativas y consultar el capítulo 6 en el que obtendrán orientación específica para proteger este tipo de instalaciones.

El modelo de evaluación de vulnerabilidades que se proporciona en este capítulo y la herramienta HoW SECURITY SELF ASSESSMENT de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) respaldan el enfoque sistemático para este proceso. Todos los tipos y tamaños de organizaciones pueden aprovechar estas y otras herramientas y recursos disponibles para personalizar el proceso de evaluación, desarrollar una estrategia de seguridad sólida y orientar la asignación de personal y recursos financieros para implementar esa estrategia. El análisis periódico de los resultados de la evaluación ayudará a abordar las amenazas en evolución y garantizará que las medidas de seguridad respondan al ambiente de amenaza actual.

Asignación de funciones y responsabilidades

La realización de la evaluación de vulnerabilidades comienza con la decisión de quién liderará el proceso. El tamaño, la ubicación y los recursos disponibles de una organización son consideraciones importantes que pueden determinar la evaluación de vulnerabilidades y deben tenerse en cuenta en las decisiones sobre quién asume esta función.

Sería ideal que el coordinador de seguridad lidere este proceso con el apoyo del Equipo de planificación de seguridad. Compartir la responsabilidad de la toma de decisiones ayudará a garantizar que los resultados representen una opinión consensuada y que cualquier cambio resultante de la evaluación cuente con el apoyo de la comunidad de la HoW.

Si los desafíos de seguridad parecen bastante sencillos, como en el caso de una pequeña HoW rural, es probable que la evaluación de vulnerabilidades se pueda realizar de manera interna.

ASESORES DE SEGURIDAD PREVENTIVA (PSA) DE LA CISA

Los asesores de seguridad preventiva (PSA, por sus siglas en inglés) son expertos en la materia, especialmente capacitados en mitigación de vulnerabilidades y protección de infraestructura crítica. Los PSA facilitan las actividades de campo locales de la CISA en coordinación con otras oficinas del Departamento de Seguridad Nacional (DHS). También asesoran y ayudan a los funcionarios estatales, locales y del sector privado, así como a los operadores y propietarios de instalaciones de infraestructura crítica. Los PSA suelen realizar las evaluaciones de la vulnerabilidad en las casas de adoración y escuelas.

Para obtener más información sobre los PSA, visite HTTPS://WWW.CISA.GOV/PROTECTIVE-SECURITY-ADVISORS o comuníquese con CENTRAL@CISA.DHS.GOV.

Las evaluaciones que involucran entornos de seguridad más complejos, como una megaiglesia, un área urbana densa o una HoW que es particularmente prominente, podrían considerar comunicarse con un PSA de la CISA para ayudar a diseñar un proceso personalizado que un equipo de voluntarios puede llevar a cabo.

Determinación del alcance de la evaluación de vulnerabilidades

Adapte la evaluación de vulnerabilidades a los intereses y necesidades específicos de su organización. Para determinar el alcance y la complejidad de una evaluación, tenga en cuenta algunas de las siguientes preguntas:

- **¿Por qué realiza la evaluación ahora?**
- **¿Ha realizado evaluaciones similares? Si es así, ¿cómo utilizó los resultados y las recomendaciones?**
- **¿Ya identificó amenazas o vulnerabilidades específicas? ¿Su organización experimentó amenazas o incidentes de violencia en el pasado?**
- **¿Cómo influye la ubicación y el tamaño de la HoW sobre sus preocupaciones de seguridad?**
- **¿La comunidad local enfrenta problemas de seguridad que podrían afectar a la comunidad de su HoW?**
- **¿Tiene presupuesto para las medidas de seguridad? De no ser así, ¿habrá oportunidades para la planificación del presupuesto destinado a la seguridad en el futuro?**

Las respuestas a estas preguntas ayudarán a definir el alcance de la evaluación y a desarrollar un proceso que contemple todos los aspectos de la situación de su organización en materia de seguridad. Idealmente, esto conducirá a una toma de decisiones clara que se base en las evidencias sobre prioridades, la contraposición de deseos y necesidades, los objetivos a corto y largo plazo, las consideraciones presupuestarias y la viabilidad. En muchos casos, este proceso dará como resultado elementos de acción que son bastante fáciles de implementar. Otros resultados pueden ser más complejos y requerir la participación de recursos externos, como los PSA de la CISA.

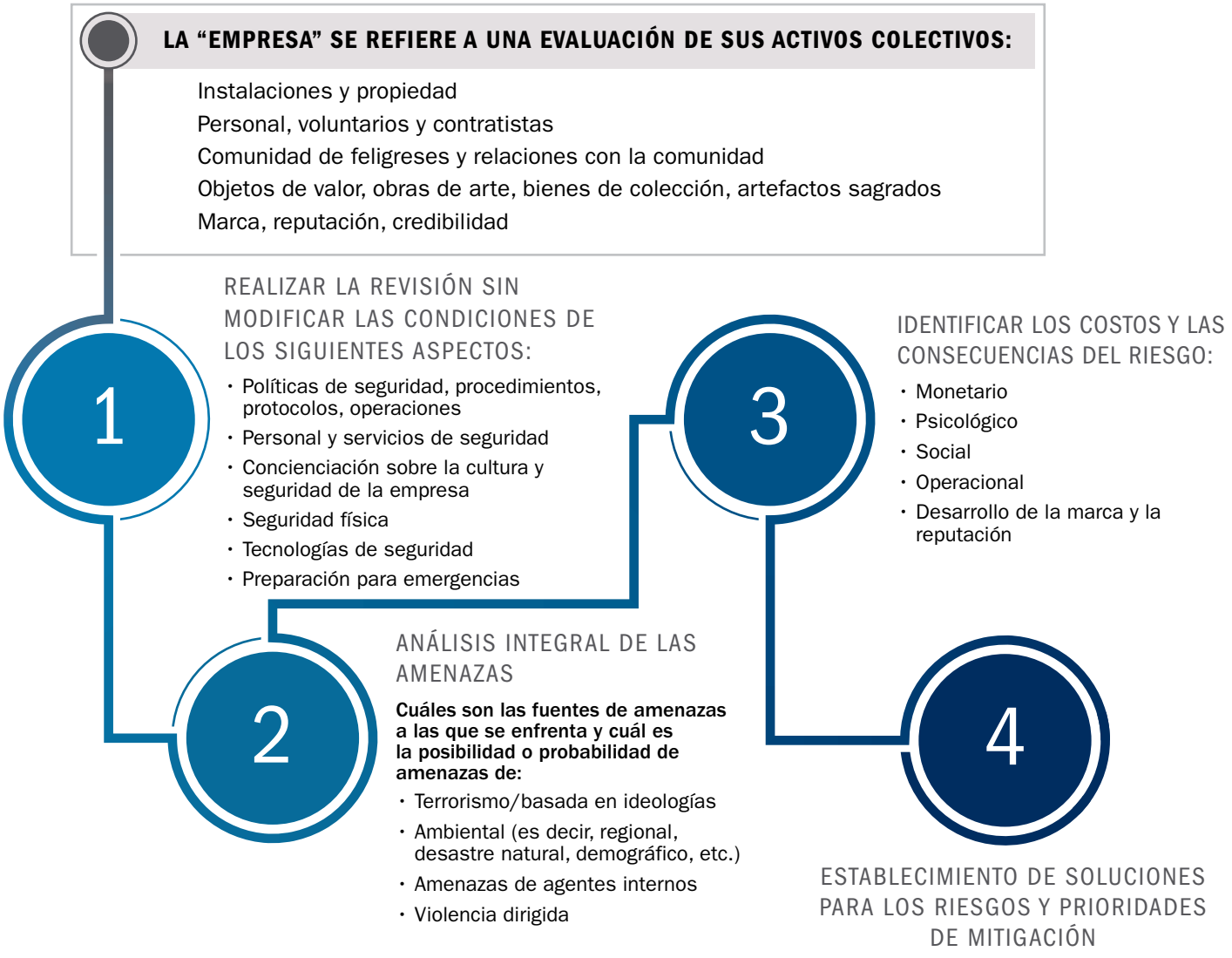
Modelo de evaluación de vulnerabilidades

El enfoque sistemático es esencial para producir una evaluación de alta calidad. Este modelo de evaluación de vulnerabilidades examina las áreas funcionales de una organización para obtener resultados que puedan evaluarse en el contexto de la viabilidad, la complejidad, los beneficios esperados, el costo y la disponibilidad de recursos.

Para mejorar este proceso, la CISA desarrolló una herramienta para la AUTOEVALUACIÓN DE LA SEGURIDAD DE LA CASA DE ADORACIÓN con una serie de preguntas diseñadas para descubrir las vulnerabilidades y áreas que deben mejorarse. Esta herramienta también puede utilizarse como una plantilla que puede adaptarse a las necesidades específicas de la organización. Como alternativa, un PSA de la CISA u otro consultor puede brindar orientación adicional para realizar la autoevaluación.

Este tipo de evaluación suele implicar la recopilación de datos e información a través de entrevistas con el personal y las partes interesadas clave, la realización de inspecciones y observaciones del sitio, la revisión de registros y materiales, como los planes de capacitación y seguridad existentes, y el análisis de registros públicos, como las estadísticas locales de delincuencia.

El aspecto más importante de una evaluación es documentar el proceso y los resultados para que el proceso en sí pueda replicarse y los datos puedan usarse para desarrollar una estrategia de seguridad.



Consideraciones clave para aprovechar el modelo de evaluación de vulnerabilidades

Patrimonio de la organización

IDENTIFICAR LAS INSTALACIONES Y PROPIEDADES

Identifique y describa sus instalaciones:

- **Identifique cada uno de los edificios de su propiedad, como el edificio principal de la HoW, la capilla, la rectoría, la escuela, el patio de recreo, el centro comunitario y el estacionamiento.**
- **Describa la cantidad, el diseño físico y la construcción de los edificios, incluido el año y el tipo de construcción, y el impacto geográfico.**
- **Defina el tipo y la cantidad de servicios que se llevan a cabo, así como el horario y la cantidad de feligreses que podrían usar cada edificio en un momento determinado. Identifique los horarios de la oficina administrativa (días y horarios). Enumere las características distintivas que podrían ayudar a identificar la propiedad de la HoW.**

*Consulte el **capítulo 5** para obtener ayuda sobre la seguridad física y los recursos asociados.*

Defina su propiedad en términos de perímetro exterior, central e interior.

- **El perímetro exterior suele incluir la instalación y los lotes del estacionamiento, los terrenos comunes exteriores, los pasillos, los patios de recreo y la fachada física de los edificios.**
- **El perímetro central es un área fluida que suele referirse a todo lo que está "en el campus", pero fuera de los edificios principales e incluye elementos exteriores, como pasillos, puertas y paredes.**
- **El perímetro interior es cualquier espacio interior, como el vestíbulo, las áreas de culto, las oficinas administrativas, la sala comunitaria, el auditorio y las aulas.**
- **Cree una lista de todos los elementos del perímetro exterior, central e interior.**

IDENTIFICAR LOS ACTIVOS Y VALORES

Identifique cualquier objeto de valor que requiera protección y el costo potencial de reposición:

- **Determine los valores de los activos, los costos para proteger los activos (mitigar el riesgo), los costos para la reposición de los activos y los costos vinculados a la reputación y existencia de la organización si se pierden los activos.**
- **Identifique los objetos de valor, como obras de arte y objetos sagrados.**
- **Asigne un costo para los objetos de valor, que pueden evaluarse simplemente como "alto", "moderado" o "bajo".**
- **Tome decisiones informadas sobre la inversión para la protección o mitigación del riesgo de cada activo.**

Realizar la revisión sin modificar las condiciones

1

REVISAR LAS PRÁCTICAS ADMINISTRATIVAS Y LOS PROTOCOLOS RELACIONADOS CON LA SEGURIDAD

Examine las operaciones diarias y los procedimientos administrativos pertinentes:

- **¿Cuáles son las prácticas en torno al acceso de los visitantes?**
  - ¿Mantiene un horario comercial regular?
  - ¿Algunos espacios se mantienen abiertos o cerrados de manera habitual?
  - ¿Existe un protocolo para recibir y examinar a los visitantes durante el culto? ¿Existe un protocolo para recibir y examinar a los visitantes fuera del horario del culto?
  - ¿Los protocolos existentes se aplican de manera consistente y se revisan periódicamente?
- **¿Cuenta con planes de acción de emergencia o de seguridad? ¿Cubren diversas situaciones, como francotiradores activos, preparación para emergencias, evacuación de emergencia, evaluación de amenazas y situaciones de seguridad escolar?**
- **¿Registró todos los procesos administrativos, procedimientos, políticas, directivas y manuales operativos? ¿Vuelve a analizar y actualizar estas políticas de manera rutinaria?**
- **¿Quién supervisa las operaciones financieras, incluidas las ofertas y los cobros? ¿Utiliza un programa informático de contabilidad? ¿Existe un sistema para realizar auditorías y supervisión?**

EXAMINAR LAS PRÁCTICAS DE RECURSOS HUMANOS

Examine las prácticas de recursos humanos:

- **¿La organización emplea personal de seguridad contratado, ya sea armado o desarmado, para brindar asistencia en las actividades y los eventos de la HoW? Si es así, ¿cuál es su función? ¿Su presencia se adapta a las preocupaciones que la seguridad suscita actualmente en la comunidad? ¿El personal de seguridad cumple con todos los requisitos de licencia, capacitación y seguro estatales y locales?**
- **¿Tiene relaciones y asociaciones formales con los funcionarios locales de orden público o los servicios de emergencias que tienen autoridad en su jurisdicción? ¿Se reúne con ellos con frecuencia para intercambiar información y colaborar en torno a las prioridades de seguridad y mitigación de riesgos?**

Consulte el capítulo 4 para obtener información sobre las prácticas de recursos humanos.

- **¿Qué protocolos de evaluación previa al empleo sigue? ¿Los empleados y voluntarios están sujetos a investigaciones de antecedentes, en especial aquellos que ocupan puestos sensibles, como interactuar con niños, dinero, sistemas informáticos o información confidencial?**
- **¿Los procesos actuales de evaluación previa al empleo cumplen con los estándares de práctica para los puestos de responsabilidad similares? Para obtener más información, consulte la guía de la Comisión para la Igualdad de Oportunidades en el Empleo de EE. UU. en la VERIFICACIÓN DE ANTECEDENTES.**

CONOZCA A SU GENTE Y SU CULTURA ORGANIZATIVA

Considere la actitud de su comunidad hacia los procedimientos de seguridad:

- **¿Los miembros suelen conocer las mejores prácticas de seguridad, como "Si ve algo, diga algo®" para observar e informar actividades sospechosas?**
- **¿Los líderes de la organización comparten mensajes regulares y consistentes sobre seguridad y protección, o es un tema que aún no se abordó de manera proactiva?**
- **¿El personal de la HoW o los miembros participaron en alguna capacitación formal sobre evacuaciones de emergencia, incidentes con francotiradores activos u otros eventos importantes?**
- **¿Tiene un proceso establecido para compartir inquietudes sobre actividades sospechosas o preocupantes?**
- **¿Los miembros de la HoW y la comunidad circundante apoyan una estrategia de seguridad que incluye posibles mejoras de seguridad?**
- **¿Qué amenazas o vulnerabilidades les preocupan a los miembros?**
- **¿Cómo se alinean los valores y las iniciativas organizativas, como el apoyo a las poblaciones vulnerables y la provisión de alimentos, refugio y apoyo social en la comunidad, con las perspectivas sobre las medidas de seguridad?**

Consulte el capítulo 4 para obtener información sobre la cultura organizativa.

Análisis integral de las amenazas

2

EVALUAR EL AMBIENTE DE AMENAZA

Establezca un conocimiento como la base de referencia del ambiente de amenaza:

- **Considere factores tales como el perfil público y la visibilidad de la organización en la comunidad y la región.**
  - Por ejemplo, comprender si las opiniones o creencias ideológicas, sociales o políticas vinculadas a la organización o a los líderes de la HoW podrían incurrir en un alto nivel de atención y riesgo.

- **Analice una gran variedad de amenazas (por ejemplo, terrorismo o amenazas basadas en la ideología) que se relacionen con la probabilidad de incidencia según la ubicación, la membresía, el historial de violencia y la prominencia.**
  - No todos los actos de violencia dirigida se basan en la ideología. Algunos incidentes con francotiradores activos estaban relacionados con violencia doméstica, disputas en el lugar de trabajo y crisis de salud mental.
- **Considere cómo la ubicación y la proximidad pueden incidir en su ambiente de amenaza. Por ejemplo, el grado de riesgo puede aumentar si una HoW está ubicada junto a una organización que suele ser el centro de atención del público o que es objeto de violencia o vandalismo.**

COMPRENDER EL ALCANCE TOTAL DEL RIESGO COMIENZA CON:

- **Identificar o enumerar cada tipo de amenaza o riesgo.**
- **Calificar y clasificar la probabilidad de ocurrencia y el impacto (p. ej., baja probabilidad/alto impacto).**

Identificación de las consecuencias y los costos relacionados con el riesgo

IDENTIFICACIÓN DE LAS CONSECUENCIAS Y LOS COSTOS RELACIONADOS CON EL RIESGO

Realice un análisis de riesgos para identificar con claridad las consecuencias asociadas con los riesgos identificados, que pueden incluir lo siguiente:

- **Pérdidas tangibles, como dinero, propiedad y objetos de valor.**
- **Daños sociales, emocionales, interpersonales y psicológicos que puedan interrumpir las operaciones y la continuidad del negocio de la HoW.**
- **Impacto en la marca, la credibilidad o la reputación de la HoW entre las partes interesadas y en toda la comunidad.**

DETERMINAR LA TOLERANCIA AL RIESGO

Analice la tolerancia de la comunidad al riesgo:

- **Participe en conversaciones sinceras sobre la tolerancia para cada riesgo identificado. Las perspectivas relacionadas con los factores de riesgo, la tolerancia al riesgo y la mitigación del riesgo pueden evolucionar con el tiempo. Por lo tanto, el proceso para evaluar el riesgo y determinar la tolerancia al riesgo debe ser flexible.**

ESTIMAR LA PROBABILIDAD DE QUE OCURRA UN RIESGO

Considere una serie de posibles situaciones y resultados:

- **Para cada riesgo, estime la probabilidad de que ocurra la amenaza y compárela con el costo y el impacto potenciales asociados con ese riesgo.**
  - Se pueden utilizar metodologías de riesgo más complicadas. Esta calificación ayudará a priorizar sus estrategias de mitigación y brindará información para la planificación de seguridad.
  - Los riesgos con una alta probabilidad de ocurrencia y los costos asociados deben clasificarse como de alta prioridad en la estrategia general de seguridad.
- **Las soluciones de mitigación pueden correlacionarse con los riesgos de la siguiente forma:**
  - Necesidad alta de mitigación
  - Necesidad moderada de mitigación
  - Necesidad baja de mitigación

Resumen

En este capítulo se proporciona un marco para diseñar y realizar una evaluación integral de la vulnerabilidad. Las casas de adoración pueden personalizar estas herramientas y recomendaciones para evaluar el patrimonio de la organización y los valores asociados, identificar el ambiente de amenaza, analizar las soluciones de riesgo y mitigación, y comprender las consecuencias asociadas con las amenazas identificadas. En última instancia, la amplitud y profundidad de la evaluación de las vulnerabilidades se basa en los recursos, la viabilidad y la urgencia con la que necesita abordar los problemas de seguridad. Los resultados de la evaluación deben orientar los análisis sobre la priorización de acciones específicas que darán forma a la estrategia de seguridad de la organización, incluida la forma en que se puede implementar esa estrategia.

4 Desarrollo del nivel de preparación y resiliencia de la comunidad

Introducción

Las personas son el activo más importante que debe proteger en la casa de adoración (HoW) y su mejor protección contra posibles amenazas. Este capítulo se centra en las personas que conforman la comunidad de la HoW y los cambios relativamente simples en la forma en que opera su HoW, de manera interna y dentro de la comunidad en general, que pueden mejorar su nivel de seguridad general.

El comportamiento humano, las relaciones interpersonales y los valores de la comunidad desempeñan una función importante en la seguridad. Con las herramientas adecuadas, las personas pueden ser la primera línea de defensa para identificar los comportamientos y las actividades sospechosos.

En este capítulo se describen una serie de políticas y programas que se pueden implementar con una inversión de capital mínima. A continuación, encontrará secciones que abarcan programas internos que las HoW individuales pueden implementar de forma independiente, políticas especializadas para considerar a medida que desarrolla el programa de seguridad general y formas de conectarse con toda la comunidad para fomentar la concienciación general, la preparación y la resiliencia.

A fin de cuentas, el desarrollo de una cultura de seguridad y responsabilidad es una de las mejores formas para que las casas de adoración se preparen y respondan a cualquier posible acto de violencia dirigida.

Figura 12. La comunidad de las casas de adoración

Una casa de adoración debe considerar a todas las personas que interactúan con la organización en el plan de seguridad.

Mejores prácticas para la comunidad de las HoW

Esta sección se centra en los programas generales que las casas de adoración pueden implementar de forma individual para mejorar su nivel de seguridad. Las HoW influyen en muchas vidas y todas las personas, desde el clero, el personal y los voluntarios hasta los feligreses y visitantes, desempeñan una función, como se muestra en la figura 12.

El objetivo general es crear un entorno en el que los líderes y miembros estén alertas a las posibles amenazas o problemas, conozcan los canales adecuados de notificación y sepan qué hacer en

una emergencia. Los entrenamientos y simulacros de rutina salvaron vidas y son, a menudo, la mejor manera de reforzar esas lecciones. Los siguientes programas e iniciativas ayudarán a preparar a su comunidad para distintas situaciones y están destinados a la casa de adoración como un todo.

Desarrollo de la cultura de seguridad

Las casas de adoración pueden mejorar su seguridad manteniendo una cultura organizativa basada en un sistema compartido de valores y objetivos de seguridad. El liderazgo de una organización puede guiar a los miembros para que adopten estos valores compartidos al:

- **Orientar los objetivos de seguridad con los valores fundamentales de la organización** y proporcionar mensajes consistentes sobre los protocolos de seguridad y protección como un valor comunitario compartido.
- **Establecer expectativas comunitarias** relacionadas con la seguridad y la facilitación activa de la comunicación, la transparencia y la capacidad de respuesta.
- **Implementar un proceso claro de intercambio de información** que les permita a los miembros de la comunidad informar incidentes o comportamientos preocupantes, al tiempo que proporciona comentarios oportunos después de evaluar el informe y garantizar que se mantenga la confidencialidad.
- **Brindar capacitación,** ya sea de manera interna o aprovechando fuentes externas, como los asesores de seguridad preventiva (PSA) de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) y sus recursos en Internet, y ofrecer oportunidades de aprendizaje continuo de manera regular.
- **Documentar todos los protocolos de seguridad** en políticas y pautas escritas y garantizar que se compartan con la comunidad de manera temprana y con frecuencia.

LA SEGURIDAD EN LA PRÁCTICA

EL CAMINO HACIA LA VIOLENCIA

Entre los posibles indicadores de que un individuo está en el CAMINO HACIA LA VIOLENCIA se incluyen los siguientes:

- **Comportamientos cada vez más erráticos, inseguros o agresivos**
- **Sentimientos hostiles de injusticia o maldad percibida**
- **Uso nocivo de drogas y alcohol**
- **Marginación o distanciamiento de amigos y colegas**
- **Cambios en el rendimiento laboral**
- **Cambios repentinos y dramáticos en la personalidad o en la vida hogareña**
- **Dificultades financieras**
- **Litigios civiles o penales pendientes**
- **Conflictos que se pueden observar con amenazas o planes de retribución**

Concienciación e identificación temprana

Para enfrentar o aliviar una amenaza, debe ser consciente de ella. Es fundamental involucrar a los miembros de la comunidad en la identificación temprana y la presentación de informes. Las casas de adoración pueden considerar una variedad de actividades y aprovechar numerosos recursos del Departamento de Seguridad Nacional (DHS) para brindarles a las personas las herramientas necesarias para detectar, disuadir y mitigar las amenazas:

- **Comparta el VIDEO *Pathway to Violence* (Camino hacia la violencia) y la HOJA INFORMATIVA de la CISA con el personal y la congregación. El DHS publicó varios recursos sobre cómo comprender las señales de advertencia de una persona que puede resultar violenta.**

- **Enséñele al personal acerca de los distintos FACTORES DE RIESGO E INDICADORES que podrían señalar un posible comportamiento violento.**
- **Implemente programas de capacitación para aumentar el conocimiento sobre las señales de advertencia temprana en las comunicaciones o el comportamiento.**
- **Familiarícese con LOS INDICADORES Y EJEMPLOS DE LAS NOTIFICACIONES DE ACTIVIDADES SOSPECHOSAS (SAR).**
- **Esté al tanto de las conversaciones dentro de su comunidad, en especial, cuando se trata de la actividad en Internet. Identifique y notifique las actividades sospechosas a las autoridades correspondientes, ya que esto es crucial para investigar las amenazas con credibilidad y tomar las medidas de mitigación adecuadas.**

Si ve algo, diga algo®

Promover la concienciación y la identificación temprana es una de las formas más importantes de interrumpir una posible amenaza. La campaña "SI VE ALGO, DIGA ALGO® ", que se muestra en la figura 13, puede ayudar a brindar información para los miembros sobre cómo estar alerta ante actividades sospechosas y notificarlas a través de los canales apropiados.

El DHS ofrece una variedad de productos para educar a los ciudadanos, que incluyen una infografía de "RECONOCER LAS SEÑALES", una TARJETA DE BOLSILLO imprimible y el "VIDEO DE CONCIENCIACIÓN PÚBLICA SI VE ALGO, DIGA ALGO® ".

Los visitantes del sitio web "Si ve algo, diga algo® " también pueden ver una serie de videos y "ACEPTAR EL DESAFÍO" y poner a prueba su capacidad de observación para detectar actividades sospechosas.

Figura 13. Las "5 preguntas clave" de la campaña Si ve algo, diga algo®

Las "5 preguntas clave" (quién, qué, cuándo, dónde y por qué) representan información importante que debe comunicar cuando se comunique con los funcionarios locales de orden público o con una persona con autoridad.

Fuente de la imagen: https://www.dhs.gov/see-something-say-something

El poder de un hola

La CISA recomienda que las casas de adoración implementen un programa sólido de bienvenida como un componente clave de la estrategia de seguridad general, centrado en el "PODER DEL HOLA".

Si se usa con eficacia, las palabras correctas pueden ser una herramienta poderosa. Con solo decir "hola" puede generar una conversación informal con personas desconocidas que ayudará a determinar por qué visitan la HoW y si representan una amenaza. El enfoque de **OBSERVAR, INICIAR UN HOLA, SOPESAR POR EL RIESGO Y OBTENER AYUDA (OHNO, por sus siglas en inglés)** ayuda a los feligreses a observar y evaluar actividades sospechosas y obtener ayuda cuando sea necesario.

OBSERVAR: Identifique conductas sospechosas, como tomar fotos o filmar las instalaciones o características de seguridad, usar lenguaje abusivo que una persona razonable podría encontrar amenazante o merodear un lugar sin una explicación razonable.

INICIAR UN HOLA: Interactúe con las personas que observa en el espacio. Reconocer una amenaza potencial puede actuar como elemento disuasorio y mitigar el riesgo.

SOPESAR EL RIESGO: Pregúntese si el comportamiento que observa es amenazante o sospechoso. ¿El individuo actúa de una manera que sugiere que tiene una razón legítima para estar allí o de una manera que despertaría sospechas en una persona razonable?

OBTENER AYUDA: Si cree que la persona representa una amenaza real, no intervenga; pida ayuda a la administración o a los funcionarios de orden público. Comunique sus preocupaciones a través de los canales apropiados en su HoW y siempre llame al 9-1-1 si se trata de una emergencia.

Todos los miembros de la comunidad tienen el poder de iniciar diálogos y detectar y notificar comportamientos sospechosos. A veces, un "hola" es suficiente.

LA SEGURIDAD EN LA PRÁCTICA

PUESTA EN PRÁCTICA DEL PODER DE UN HOLA

Sonría, haga contacto visual y preséntese antes de hacer las siguientes preguntas:

- **"Hola, ¿cómo está?"**
- **"¿Puedo ayudarle en algo hoy?"**
- **"¿Cómo puedo ayudarle?"**
- **"Bienvenido, ¿es la primera vez que viene?"**
- **"¿Busca algo o a alguien en particular?"**
- **"Permítame acompañarlo al lugar o llevarlo a la persona que busca".**
- **"Estaré aquí en caso de que necesite ayuda".**

Correr, ocultarse, luchar

A veces, la detección temprana no basta para prevenir un incidente; las casas de adoración deben preparar a sus miembros para que sepan cómo actuar en caso de un ataque. Los casos de atacantes activos son impredecibles y evolucionan rápidamente. Algunos de estos ataques terminan antes de que los funcionarios de orden público lleguen al lugar, por lo que las personas deben estar preparadas tanto mental como físicamente para hacer frente a la situación.

Si se trata de un atacante armado, como un francotirador activo, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) sugiere que los ciudadanos deben CORRER, OCULTARSE O LUCHAR.

Correr, ocultarse o luchar implica evaluar rápidamente la situación y determinar la forma más razonable de proteger su vida en función de su ubicación y de las circunstancias. En cualquier escenario, puede tener una de tres opciones:

1. CORRER: Si hay una ruta de escape accesible, intente evacuar las instalaciones.

- Tenga en mente una ruta y plan de escape.
- Deje atrás sus pertenencias.
- Mantenga sus manos a la vista y siga las instrucciones de la policía.

2. OCULTARSE: Si no es posible evacuar, busque un escondite donde sea menos probable que el atacante lo encuentre.

- Escóndase en un área fuera de la vista del francotirador.
- Bloquee la entrada a su escondite y cierre las puertas.
- Silencie su teléfono celular (incluido el modo de vibración).
- Permanezca en silencio.

3. LUCHAR: Como último recurso, y solo si su vida corre peligro inminente, intente desestabilizar o incapacitar al atacante.

- Actúe con la mayor agresión física posible.
- Improvise armas o lance objetos al atacante.
- Actúe de manera decisiva... su vida depende de ello.

Los líderes de la HoW deben compartir el VIDEO DE LAS OPCIONES A CONSIDERAR con todos los miembros de la comunidad para asegurarse de que estén familiarizados con las diferentes opciones durante un posible ataque.

LA SEGURIDAD EN LA PRÁCTICA

CORRER, OCULTARSE, LUCHAR

En más de la mitad (n=13) del total de casos de asaltos a mano armada (n=20), los feligreses respondieron corriendo o escondiéndose cuando comenzó el ataque. Algunos pudieron escapar por las puertas de salida, mientras que otros se escondieron en baños, armarios o debajo de los muebles. En un caso, los feligreses cerraron todas las puertas exteriores tras oír el alboroto afuera e impidieron que el atacante ingresara.

En el 45 por ciento (n=9) de los estudios de caso de asalto a mano armada (n=20), los miembros de la congregación o los testigos intentaron enfrentar, distraer o desarmar al perpetrador. Algunas víctimas confrontaron al atacante usando el entrenamiento estándar contra atacantes activos, algunas a costa de sus vidas; otras arrojaron libros, sillas o muebles. Muchos de estos intentos frenaron al atacante lo suficiente como para permitir que otros escaparan a un lugar seguro.

Servicios de salud mental y asistencia social

Algunos incidentes de violencia dirigida se derivan de crisis de salud mental y presentan señales de advertencia que indican que una persona puede ser un peligro para sí misma y para los demás. No todas las crisis de salud mental conducen a la violencia; sin embargo, las HoW deben estar al tanto de las señales que indican que una persona está en crisis y puede estar en el camino hacia la violencia.

Las casas de adoración se encuentran en una posición única que les permite identificar problemas de salud conductual e intervenir antes de que la situación se intensifique. Los líderes de las HoW suelen ser el primer punto de contacto en tiempos de crisis, actuando como consejeros o fuente de consuelo para personas y familias durante tiempos difíciles. Las HoW pueden promover una cultura de cuidado mejorando la concienciación sobre la salud mental y facilitando la búsqueda de ayuda. Considere la posibilidad de poner en práctica las siguientes opciones de intervención y asistencia para fortalecer la resiliencia de la comunidad:

- **Conozca la INFORMACIÓN BÁSICA SOBRE LA SALUD MENTAL, incluidas las posibles señales de advertencia de que alguien necesita ayuda.**
- **Concientice a su comunidad acerca de la salud mental y fomente un diálogo abierto sobre temas de salud mental y bienestar.**
- **Identifique a los miembros de la comunidad que puedan estar en crisis y póngalos en contacto con los servicios de apoyo.**
- **Desarrolle un sistema para identificar y difundir información a los miembros que no han asistido recientemente a los servicios religiosos.**
- **Revise las mejores prácticas para líderes religiosos proporcionadas a través del sitio web del Departamento de Salud y Servicios Humanos de los EE. UU., MENTALHEALTH.GOV.**
- **Complete la capacitación en Internet sobre CÓMO ABORDAR EL RIESGO DE COMPORTAMIENTO VIOLENTO EN LOS JÓVENES proporcionada por la Administración de Salud Mental y Abuso de Sustancias (SAMHSA, por sus siglas en inglés) del Departamento de Salud y Servicios Humanos de los EE. UU.**

LA SEGURIDAD EN LA PRÁCTICA

DESESCALADA

Cuando un hombre armado vestido con equipo táctico amenazó a los feligreses en una iglesia de Texas, el pastor intervino y se colocó entre el hombre armado y los feligreses. El pastor utilizó su experiencia como especialista en intervención en crisis con jóvenes con problemas y delincuentes para calmar la situación hablando con el hombre armado, quien huyó y fue arrestado al día siguiente.

- **Ofrezca programas de capacitación en desescalada para el personal, los voluntarios y los miembros interesados como una herramienta potencial.**
- **Realice capacitaciones periódicas sobre los procedimientos de cierre y para situaciones de francotirador activo.**
- **Enseñe a los miembros y al personal a identificar actividades sospechosas y establezca claramente los mecanismos de notificación.**

- **Identifique los puntos de contacto que pueden brindar apoyo especializado, como salud mental, prevención del suicidio, violencia doméstica, maltrato infantil, trata de personas y abuso de sustancias.**
  - Identifique proveedores de atención médica cercanos utilizando la herramienta de la SAMHSA en FINDTREATMENT.GOV.
  - Identifique la Agencia para la Salud Mental de su estado utilizando EL LOCALIZADOR DE SERVICIOS DE TRATAMIENTO PARA LA SALUD CONDUCTUAL de la SAMHSA.
- **Evalúe la posibilidad de establecer relaciones con proveedores especializados de la comunidad que puedan servir como recurso para las mejores prácticas y posibles referencias.**

Políticas especializadas y planificación a largo plazo

La planificación es una etapa importante en el desarrollo de una estrategia de seguridad integral. Una vez que haya implementado algunas de las mejores prácticas generales, es hora de comenzar a planificar una serie de escenarios específicos y los posibles riesgos, amenazas y resultados de cada uno. En esta sección se destacan algunas de las políticas más especializadas que deben tener en cuenta los líderes y los coordinadores de seguridad de las HoW a medida que se desarrolla su programa de seguridad.

Planificación para emergencias y respuesta ante incidentes

La planificación para emergencias debe ser una parte crucial de cualquier programa de seguridad e implica determinar cómo responderá su organización a un escenario o incidente específico. Los planes de acción de emergencia (EAP, por sus siglas en inglés) pueden ayudar a preparar a su HoW para cualquier situación de emergencia al proporcionar una guía para la respuesta ante incidentes. La CISA tiene un CONJUNTO DE RECURSOS para la planificación de la gestión de incidentes y la respuesta ante estos. Al crear un EAP, las casas de adoración pueden tener en consideración las siguientes opciones:

- **Consultar la GUÍA DE LA AGENCIA FEDERAL PARA EL MANEJO DE EMERGENCIAS (FEMA, POR SUS SIGLAS EN INGLÉS) PARA DESARROLLAR PLANES DE OPERACIÓN EN EMERGENCIAS DE ALTA CALIDAD PARA LAS CASAS DE ADORACIÓN (junio de 2013). Esta guía presenta las medidas concretas que se pueden tomar antes, durante y después de un incidente para reducir el impacto sobre la propiedad y el número de víctimas mortales. Muchas HoW también pueden beneficiarse de la capacitación sobre el SISTEMA DE MANDO DE INCIDENTES (ICS, POR SUS SIGLAS EN INGLÉS) que ofrece la FEMA.**
- **Determinar cómo continuará funcionando su HoW en cualquier tipo de emergencia. READY.GOV ofrece una serie de productos en el PAQUETE DE PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO que se pueden adaptar a las necesidades específicas de su HoW.**
- **Desarrolle su propio EAP utilizando LA PLANTILLA Y LA GUÍA DEL PLAN DE ACCIÓN DE EMERGENCIA EN UNA SITUACIÓN DE FRANCOTIRADOR ACTIVO de la CISA o la PLANTILLA PERSONALIZABLE PROPORCIONADA POR EL CENTRO DE PREPARACIÓN Y RESPUESTA DE LOS CENTROS PARA EL CONTROL Y LA PREVENCIÓN DE ENFERMEDADES (CDC, POR SUS SIGLAS EN INGLÉS).**

Estos recursos cubren solo algunas de las eventualidades previstas por una estrategia de seguridad completa e integral. Para obtener recursos de planificación adicionales, consulte EL APÉNDICE 1.

Es fundamental que el equipo de seguridad y los miembros de la comunidad sepan cómo responder si ocurriera un ataque. La mejor manera de lograr esto es asegurándose de que los miembros de la comunidad conozcan bien el EAP y realicen capacitaciones y simulacros sobre procedimientos de emergencia con regularidad.

Prácticas de seguridad del personal

Unas sólidas prácticas de seguridad del personal pueden garantizar que todos los empleados y voluntarios tengan una buena conducta y mantengan estándares de integridad y confiabilidad. Las casas de adoración, como todas las empresas y organizaciones, deben revisar periódicamente las prácticas de seguridad del personal para garantizar que se alineen con las prácticas comerciales estándar y respondan a la evolución de las amenazas:

- **Haga una lista de los puestos críticos basándose en las funciones y responsabilidades.**
  - ¿Existen operaciones comerciales que requieran un mayor nivel de escrutinio del personal?
  - Considere, por ejemplo, incluir al personal que tiene contacto con niños, desempeña funciones financieras, gestiona o conserva información personal identificable (PII, por sus siglas en inglés) y tiene acceso a sistemas de tecnología de la información (IT, por sus siglas en inglés).
- **Haga una lista de los puestos que deberían requerir o actualmente requieren una investigación de antecedentes y desarrolle e implemente políticas de descalificación automática del empleo según la naturaleza de cada puesto.**
  - ¿Se lleva a cabo un proceso de evaluación previa al empleo para los puestos críticos (personal, voluntarios y contratistas)? De no ser así, ¿qué recursos serían necesarios para implementar este proceso?
  - ¿Se realizan autoevaluaciones periódicas, revisiones formales o actualizaciones de la investigación de antecedentes para estos puestos?

Amenazas de agentes internos

La CISA define a un *agente interno* como cualquier persona que tiene o ha tenido acceso autorizado o conocimiento de los recursos de una organización, incluido el personal, las instalaciones, la información, los equipos, las redes y los sistemas. En pocas palabras, esta es una persona en la que la organización y los miembros de la comunidad confían. Una amenaza de agentes internos es la posibilidad de que un agente interno utilice su acceso a información privilegiada o conocimiento especial para dañar a dicha organización a través de la violencia, el espionaje, el sabotaje, el robo o los medios cibernéticos.

Incluir un programa de mitigación de amenazas de agentes internos como parte de una sólida estrategia de seguridad puede ayudar a aumentar la cantidad de empleados y miembros de la comunidad que se preocupan por la seguridad, reforzar una cultura de responsabilidad compartida y protección de activos, permitir la identificación temprana de amenazas, y proteger la reputación de una organización. La CISA recomienda que las organizaciones desarrollen su propia definición de amenaza de agentes internos en función de la naturaleza única de su HoW, sus valores y los recursos que consideran que están en mayor riesgo.

Un programa efectivo de mitigación DE AMENAZAS DE AGENTES INTERNOS tiene las siguientes características:

1. **SE ADAPTA** a la misión, la cultura, los activos críticos y el panorama de amenazas propios de la casa de adoración.
2. **CONSTRUYE UNA CULTURA DE NOTIFICACIÓN Y PREVENCIÓN**, como se indica en la guía de la CISA sobre cómo **RECONOCER Y NOTIFICAR COMPORTAMIENTOS ANÓMALOS**, que refuerza la inversión positiva que hacen las HoW en el bienestar de su gente, al tiempo que mejora la resiliencia general y la eficacia operativa.

3. **EMPLEA UN ENFOQUE EN CAPAS** que contempla la variedad de roles y funciones que ofrece la HoW.
4. **APLICA EL MARCO DE "RECONOCER Y NOTIFICAR" Y "EVALUAR Y RESPONDER"** para detectar, prevenir y mitigar las amenazas de agentes internos (parte del Proceso de evaluación de vulnerabilidades descrito en el capítulo 3).
5. **ESTABLECE UNA CULTURA PROTECTORA Y DE APOYO** para proteger las libertades civiles y mantener la confidencialidad.
6. **AYUDA A LAS ORGANIZACIONES A PROPORCIONAR UN ENTORNO SEGURO Y SIN AMENAZAS** en el que las personas que podrían representar una amenaza son identificadas y reciben ayuda antes de que sus acciones puedan causar daño.

Para obtener más información, consulte LOS RECURSOS PARA LA MITIGACIÓN DE AMENAZAS DE AGENTES INTERNOS de la CISA.

Procedimientos de notificación

Los programas de prevención y las campañas de concienciación para "conocer las señales" son más efectivos cuando las comunidades saben qué hacer si se identifica una posible preocupación o amenaza, y requieren una reflexión deliberada por parte del personal directivo para garantizar la rendición de cuentas y definir claramente los canales de notificación apropiados. Las casas de adoración deben detallar y comunicar claramente los estándares y mecanismos de notificación y garantizar que todos los miembros de la comunidad, especialmente los miembros del equipo de seguridad, estén familiarizados con los protocolos de la organización.

Estos procesos deben incluir una evaluación confiable y oportuna, la notificación a través de los canales apropiados y la adopción de medidas inmediata de acuerdo con las leyes, políticas y regulaciones. En algunos casos, las notificaciones pueden mantenerse a nivel interno e involucrar al equipo de seguridad o al personal directivo de la HoW. En otros casos, se recomienda comunicar sus preocupaciones a los funcionarios de orden público o las autoridades federales. Para asegurarse de que los miembros y el personal tengan las herramientas necesarias para saber qué, cuándo y cómo notificar una posible amenaza, considere los siguientes factores:

- **Realizar la CAPACITACIÓN EN SEGURIDAD DEL SECTOR PRIVADO sobre la notificación de actividades sospechosas (SAR, por sus siglas en inglés) para comprender mejor cómo notificar actividades sospechosas e integrar la notificación en la cultura de su organización. Aunque está dirigido a los organismos gubernamentales, 10 MANERAS DE INTEGRAR LA NOTIFICACIÓN DE ACTIVIDADES SOSPECHOSAS EN LAS OPERACIONES DE SU ORGANIZACIÓN también ofrece una guía útil para las HoW.**
- **Familiarizarse con la INICIATIVA NACIONAL SAR (NSI, POR SUS SIGLAS EN INGLÉS), que proporciona un proceso estandarizado para identificar y notificar actividades sospechosas.**
- **Utilizar la campaña "SI VE ALGO, DIGA ALGO®" y sus recursos para crear una estrategia interna de notificación adaptada a la cultura y la estrategia de seguridad de su organización.**
- **Identificar a las personas dentro de su organización que pueden servir como contactos de confianza para notificar actividades sospechosas.**
  - Asegúrese de que estas personas estén capacitadas en todos los protocolos de seguridad.

› Comunique esta estructura de notificación a la comunidad para que sepan a quién contactar en caso tengan preocupaciones sobre la seguridad.

- **Establecer procedimientos claros para recibir, evaluar y actuar en función de las notificaciones de los miembros de la comunidad.**

  › Explique cómo documentar la notificación, tratar las cuestiones de confidencialidad, determinar la probabilidad de riesgo/impacto, notificar a los funcionarios de orden público o a los funcionarios de salud mental (si corresponde) y realizar una evaluación adicional según sea necesario.

- **Distribuir entre el personal y los miembros de la comunidad el folleto de la NSI sobre la SEGURIDAD PARA LOS EVENTOS RELIGIOSOS Y LAS HoW.**

Participación de la comunidad en general

Las casas de adoración desempeñan una función vital en las relaciones y la cohesión de la comunidad, y esa función puede ser una fuente de fortaleza a la hora de mejorar el nivel de seguridad de su HoW. Algunas HoW sirven como lugares de reunión para grupos cívicos y grupos de apoyo, espacios para eventos, lugares de entretenimiento, lugares de votación electoral y refugios comunitarios. Otras se esfuerzan por establecer conexiones significativas con los vecinos y otras HoW de la comunidad.

La participación de toda la comunidad es un recurso importante para mejorar la concienciación general sobre las posibles amenazas, aumentar la resiliencia y construir alianzas externas, todo lo cual fortalecerá su nivel de seguridad general.

Planificación de eventos

Si bien las HoW están diseñadas para dar la bienvenida a los que no son miembros, ciertos tipos de eventos pueden aumentar el riesgo. Las consideraciones de seguridad relacionadas con la participación de la comunidad y la planificación de eventos deben incluir:

- **Desarrollar e implementar prácticas de seguridad específicas para las actividades que no sean de adoración que se lleven a cabo en la propiedad. Para más información, consulte las mejores prácticas descritas en la Guía de acción de REUNIONES EN MASA: CONCIENCIACIÓN EN MATERIA DE SEGURIDAD PARA BLANCOS FÁCILES Y LUGARES CONCURRIDOS.**
- **Identificar y evaluar continuamente las vulnerabilidades y los riesgos potenciales durante las actividades que no sean de adoración y mejorar los procedimientos de seguridad según sea necesario.**
- **Considerar la posibilidad de incorporar procedimientos de control del público para evitar la presencia de artículos prohibidos en las instalaciones durante eventos especiales e incorporar las mejores prácticas descritas en la GUÍA DE MEJORES PRÁCTICAS PARA EL CONTROL DEL PÚBLICO y LA GUÍA DE PROCEDIMIENTOS PARA EL CONTROL DE BOLSOS EN LUGARES PÚBLICOS.**
- **Gestionar las visitas y controlar el número de asistentes a eventos especiales con boletos u hojas de registro.**
- **Considerar la posibilidad de ponerse en contacto con los funcionarios locales de orden público colaboradores o los asesores de seguridad preventiva (PSA) de la CISA para que ayuden a planificar la seguridad en eventos importantes, como festividades religiosas, o siempre que se tenga previsto realizar grandes reuniones.**

Participación de la comunidad

Un enfoque de seguridad basado en la comunidad incluye actividades de difusión de información y concienciación. Como parte de una estrategia de seguridad más amplia, considere tomar medidas que promuevan la resiliencia comunitaria:

- **Participar en campañas de concienciación pública para instruir a la comunidad, dar forma al discurso público y fomentar la comprensión, la tolerancia y la aceptación.**
- **Nombrar voluntarios y seleccionar miembros de la comunidad para que participen en capacitaciones y talleres presenciales avanzados, como el PROGRAMA DEL EQUIPO COMUNITARIO DE RESPUESTA EN EMERGENCIAS (CERT, POR SUS SIGLAS EN INGLÉS), LA PREPARACIÓN CONTRA FRANCOTIRADORES ACTIVOS, atacantes activos y mitigación de la toma de rehenes.**
- **Practicar ejercicios y simulacros de entrenamiento de rutina en toda la comunidad con los funcionarios locales de orden público, los servicios de gestión de emergencias, las empresas cercanas y otras HoW.**
- **Patrocinar y facilitar cursos para la comunidad sobre primeros auxilios básicos y reanimación cardiopulmonar.**

Las organizaciones con base de fe de la comunidad pueden formar asociaciones para mejorar el intercambio de información, aumentar la resiliencia e incrementar la seguridad. Considere la posibilidad de crear estructuras y relaciones formales o informales y desarrollar grupos interreligiosos dentro de la comunidad para compartir conocimientos y recursos sobre seguridad:

- **Establezca relaciones con otras HoW en la misma zona geográfica.**
  - Evalúe la posibilidad de crear grupos formales de diálogo interreligioso.
  - Coordine con el Servicio de Relaciones Comunitarias del Departamento de Justicia para organizar un FORO SOBRE LA PROTECCIÓN DE LOS LUGARES DE ADORACIÓN con socios comunitarios interreligiosos.
- **Cree un espacio privado y compartido en las redes sociales u otro espacio de comunicación para colaborar con otras HoW en su zona y centralizar el intercambio de información.**
  - Identifique las amenazas creíbles procedentes de las comunicaciones entre pares, la información compartida, la actividad en Internet y las redes sociales, e informe a los funcionarios de orden público según corresponda.
  - Realice un seguimiento y notifique las amenazas recientes que surgen en Internet.
- **Organice un evento de PREPAREATHON en su comunidad para fomentar la preparación y la resiliencia de la comunidad.**

Alianzas estratégicas

Cultivar y mantener relaciones con los principales socios de la comunidad y el personal de respuesta es fundamental para reforzar la estrategia de seguridad de su organización. Las coaliciones comunitarias sólidas ayudan a promover los objetivos compartidos para identificar amenazas, mitigar riesgos y mejorar la seguridad pública. Mantener un diálogo continuo con los funcionarios locales de orden público y los servicios de gestión de emergencias también puede mejorar la preparación y permitir una mejor coordinación de la respuesta ante incidentes.

Las alianzas estratégicas pueden incluir los departamentos locales de policía, bomberos y servicios de emergencia médica, así como organizaciones regionales y estatales. Considere las siguientes medidas para fomentar estas relaciones importantes:

- **Identifique a quienes colaboran a nivel local con la supervisión del personal de respuesta de su organización, incluidos:**
  - los funcionarios locales de orden público competentes;
  - el Departamento de Bomberos local más cercano y la unidad de respuesta médica de emergencia;
  - el centro de traumatología del hospital más cercano;
  - cualquier otro servicio de emergencia médica cercano, incluidos los recursos de salud mental.
- **Establezca relaciones con los funcionarios locales de orden público y el personal de respuesta a través de actividades de alcance comunitario.**
  - Realice recorridos por las instalaciones y comparta los planos de construcción para familiarizarse con la propiedad. Haga un seguimiento con versiones actualizadas si se realizan cambios importantes en la propiedad y el terreno.
  - Revise los protocolos de seguridad y dirija/participe en sesiones de capacitación formales e informales.
  - Aproveche los eventos sociales comunitarios para crear conexiones entre el personal de respuesta y los vecindarios a los que atienden.

LA SEGURIDAD EN LA PRÁCTICA

ALIANZAS DE ENLACE PROFESIONAL

- **¿Cuál es el tiempo de respuesta a su HoW?**
- **¿Han realizado un recorrido por sus instalaciones?**
- **¿Han acudido a su HoW en el pasado? Si es así, ¿para qué?**
- **¿Se les ha proporcionado un dibujo arquitectónico/plano de planta de sus instalaciones?**
- **¿Han realizado capacitaciones en su HoW? ¿Lo harían, si se les invitara?**
- **¿Qué servicios de instrucción y capacitación en seguridad pública pueden ofrecer?**

- **Identifique su organización local o regional de gestión de emergencias utilizando la HERRAMIENTA DE READY.GOV. Comuníquese con la oficina más cercana y suscríbase a las alertas si se ofrecen.**
- **Identifique su OFICINA REGIONAL DE LA CISA más cercana y establezca relaciones con los PSA regionales de la CISA. Consulte LA HOJA INFORMATIVA DE PSA de la CISA para obtener información adicional sobre los servicios proporcionados a través de este programa regional.**
- **Si su HoW está ubicada en una instalación federal o cerca de ella, póngase en contacto con el SERVICIO DE PROTECCIÓN FEDERAL del Departamento de Seguridad Nacional (DHS, por sus siglas en inglés).**
- **Dialogue con los funcionarios de orden público federales para conocer los recursos de planificación y capacitación y comprender con mayor detalle los procesos de notificación de actividades sospechosas y la respuesta ante incidentes.**
- **Involucre a su centro de fusión regional en la monitorización e investigación de amenazas.**

Resumen

El comportamiento humano, las relaciones interpersonales y los valores de la comunidad tienen un enorme impacto en la eficacia de los programas de prevención, preparación y mitigación de riesgos. Las HoW que fomentan una cultura de cuidado y responsabilidad compartida estarán bien preparadas para responder a las amenazas actuales y emergentes, y las herramientas que se presentan aquí pueden ayudarle a encontrar el enfoque que mejor se adapte a las necesidades de su HoW y de la comunidad más amplia a la que atiende.

5 Protección para las instalaciones

Introducción

El propósito de cualquier programa de seguridad y protección es identificar el riesgo potencial lo antes posible, determinar el mejor plan de acción y minimizar o interrumpir el riesgo antes de que genere daños corporales o materiales. Como se explica en el capítulo 4, puede abordar muchos problemas modificando las políticas, las prácticas y los comportamientos dentro de su casa de adoración (HoW) individual, con una inversión de capital mínima. Sin embargo, gestionar algunas vulnerabilidades puede requerir cambios físicos en las estructuras y terrenos de sus instalaciones. En este capítulo se presentan algunas de las opciones para mejorar la seguridad física, así como su impacto potencial.

Un ambiente acogedor no es un ambiente indefenso.

Para enmarcar las diferentes áreas de vulnerabilidad y responsabilidad, piense que su propiedad está dividida en tres zonas distintas: *perímetro exterior*, *perímetro central* y *perímetro interior*. Una estrategia de seguridad efectiva debe abarcar toda el área de la HoW, desde el extremo más alejado de la propiedad hasta la zona más interna del santuario. La mayoría de los planes de seguridad comienzan en el perímetro exterior y avanzan hacia el perímetro central y el interior. Las características de seguridad en cada zona deben estar completamente integradas y considerar las vulnerabilidades y los riesgos interconectados entre zonas. Este sistema de zonas también proporciona un marco para implementar programas de seguridad, como la gestión de tráfico o los anfitriones.

Las opciones de mitigación de riesgos analizadas en este capítulo van desde la organización de los patrones de tráfico, la plantación de setos, la instalación de vallas e iluminación, la videovigilancia por circuito cerrado de televisión (CCTV, por sus siglas en inglés) y el perfeccionamiento de los controles de acceso a los edificios. Juntas, estas opciones respaldan un enfoque en capas que abarca todas las vulnerabilidades y los riesgos de seguridad física identificados y considera una serie de posibles escenarios de amenazas.

La posibilidad de agregar o mejorar la seguridad física puede parecer desalentadora, tanto por el costo como por la reticencia a “fortalecer” o “endurecer” un edificio diseñado para ser abierto y acogedor. La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) enfatiza que hay muchas opciones disponibles a considerar, algunas de las cuales requieren una inversión de capital mínima. Muchas HoW también son elegibles para recibir subvenciones federales y estatales para compensar el costo de las mejoras, y los líderes de las HoW y equipos de seguridad pueden aprovechar los otros recursos gratuitos proporcionados por la CISA y otras agencias federales descritas en esta guía para desarrollar un plan de mejora de la seguridad física adaptado a sus necesidades.

FINANCIAMIENTO A TRAVÉS DE SUBVENCIONES

En respuesta a los ataques dirigidos a las casas de adoración, algunos Gobiernos estatales y locales han aprobado leyes para crear oportunidades de financiación para apoyar las mejoras de seguridad. Asegúrese de verificar cuáles podrían ser aplicables a su HoW específica.

A nivel federal, el Departamento de Seguridad Nacional (DHS), la Agencia Federal para el Manejo de Emergencias (FEMA) y el Congreso están incrementando el financiamiento a través de subvenciones para ayudar a las HoW a realizar mejoras en materia de seguridad. La FEMA ofrece el PROGRAMA DE SUBVENCIONES DE SEGURIDAD SIN FINES DE LUCRO, que brinda "oportunidades de apoyo financiero para realizar mejoras de seguridad física y otras actividades para organizaciones sin fines de lucro elegibles que corren un alto riesgo de sufrir un ataque terrorista y que están ubicadas en un área urbana designada por la Iniciativa de Seguridad del Área Urbana (UASI, por sus siglas en inglés) bajo el Programa de Subvenciones UASI del DHS". Las organizaciones sin fines de lucro elegibles pueden presentar una solicitud a través de la AGENCIA ADMINISTRATIVA ESTATAL. El personal de la Dirección de Programas de Subvenciones de la FEMA también está dispuesto a trabajar con las HoW en la preparación para emergencias y la elaboración de presupuestos para ayudar a las HoW a planificar mejoras de seguridad. Para obtener más información, visite www.fema.gov/grants.

Perímetro exterior

Identificar el área total de responsabilidad de su HoW, el límite en el borde más lejano de la propiedad, es un elemento crítico en el proceso de planificación y será diferente para cada casa de adoración. Lo más importante es definir este *perímetro exterior* en términos de tamaño, elementos de protección existentes (p. ej., barreras, vallas, puertas e iluminación) y riesgos observados, si los hubiera.

El perímetro exterior suele ser la primera oportunidad para abordar una vulnerabilidad o mitigar un ataque, y el espacio que ocupa cada HoW presentará sus propios desafíos y circunstancias únicos. En algunos casos, esta área puede incluir un gran campo para eventos deportivos o actividades al aire libre. En otros, el perímetro exterior puede incluir un estacionamiento de la superficie, que puede o no tener vallas, iluminación, monitorización u otras características de seguridad. Algunas HoW pueden tener estacionamiento en la calle, mientras que otras pueden usar instalaciones de estacionamiento de varios pisos que no están afiliadas a la organización.

LA SEGURIDAD EN LA PRÁCTICA

SEGURIDAD A TRAVÉS DEL DISEÑO

La FEMA ha publicado orientaciones detalladas sobre cómo el diseño de las instalaciones y los edificios puede ayudar a mitigar el riesgo y los daños de un ataque.

DISEÑO URBANO Y DEL EMPLAZAMIENTO PARA LA SEGURIDAD: ORIENTACIONES CONTRA POSIBLES ATAQUES TERRORISTAS (2007)
Serie de gestión de riesgos

MANUAL DE REFERENCIA PARA MITIGAR POSIBLES ATAQUES TERRORISTAS CONTRA EDIFICIOS (2011)
Serie de protección de edificios e infraestructura

Una vez que el equipo de planificación de seguridad ha definido el perímetro exterior, puede identificar las vulnerabilidades, identificar las posibles soluciones de mitigación de riesgos y priorizar las soluciones en función de la probabilidad, el impacto y el costo. Las casas de adoración, en particular aquellas que están pensando en realizar nuevas construcciones o renovaciones, pueden encontrar información útil en el concepto de Prevención de la delincuencia a través del diseño ambiental (CPTED, por sus siglas en inglés), que se centra en cómo el entorno construido puede influir en el comportamiento humano. Incluso soluciones

sutiles y rentables, como cambios en el paisajismo para mejorar la visibilidad o el uso de jardineras y bolardos de concreto para controlar el acceso, pueden tener un impacto significativo y maximizar el retorno de la inversión.

Una consideración especial para el perímetro exterior es la amenaza de ataques vehiculares. En general, los ataques vehiculares se dividen en dos categorías: embestidas de vehículos y artefactos explosivos improvisados transportados por vehículos (VBIED, por sus siglas en inglés). Es más probable que ambos tipos de ataques con vehículos ocurran cerca del perímetro exterior. Si bien la investigación descrita en el capítulo 1 no identificó ningún VBIED utilizado para atacar una casa de adoración, los estudios de caso incluyeron dos ataques de embestidas de vehículos. La gestión de los patrones de tráfico y la participación de voluntarios, anfitriones, personal de seguridad o funcionarios de orden público para dirigir el tráfico, especialmente durante las horas pico, pueden ayudar a identificar actividades sospechosas. Instalar barreras, como jardineras o bolardos de concreto, también puede crear una zona de "distanciamiento" para ayudar a proteger a los feligreses.

Mientras evalúa los cambios a realizar en el perímetro exterior, considere algunas de las siguientes opciones:

OPCIONES PARA EL PERÍMETRO EXTERIOR

Características de seguridad	Tipos	Beneficios y recursos
ILUMINACIÓN		
	• Alumbrado solar • Alumbrado público programado	• Disuade a los posibles atacantes o intrusos. • Ilumina todas las áreas para que el personal y los feligreses puedan recorrer los estacionamientos y los terrenos de manera segura.
	Una iluminación adecuada y estratégicamente colocada a lo largo del perímetro exterior y en todo el terreno puede impedir el acceso no autorizado y mejorar la seguridad del personal y los feligreses. Las opciones van desde alumbrado solar con iluminación nocturna hasta alumbrado público estándar controlado por un temporizador o un interruptor de encendido/apagado.	
VALLAS/PUERTAS		
	• Barrera visual • Barrera sólida • Diseño de paisajismo	• Limita el acceso a los terrenos e instalaciones de personas no afiliadas a la HoW. • El estilo de las vallas también puede ofrecer una estética visual.
	Las vallas y puertas perimetrales presentan diferentes estilos y funciones que van desde simples barreras visuales para distinguir los límites de la propiedad hasta diseños que impiden o limitan la entrada a los terrenos. Las vallas y las puertas también pueden conectarse a los sistemas de control de acceso, iluminación y videovigilancia de los edificios.	
CCTV (VIDEOVIGILANCIA)		
	• Solo grabación • Monitorización activa sin respuesta • Monitorización activa con respuesta	• Admite la monitorización de comportamientos sospechosos y ofrece funciones de advertencia temprana y alertas. • Disuade a los intrusos. • Elimina los puntos ciegos. • CONSIDERACIONES SOBRE LA PLANIFICACIÓN: ATAQUES COORDINADOS COMPLEJOS
	Antes de instalar un sistema de vigilancia por CCTV, evalúe si esta tecnología se alinea con la estrategia, las necesidades y la capacidad de seguridad general. El CCTV se puede implementar de diversas formas: desde un sistema de grabación no monitoreado hasta un sistema monitoreado activamente por personal de seguridad contratado e integrado en un plan de respuesta ante incidentes.	

OPCIONES PARA EL PERÍMETRO EXTERIOR

Características de seguridad	Tipos	Beneficios y recursos
LA GESTIÓN DEL TRÁNSITO		
	• Puertas/Bolardos • Senderos/Señalización • Estacionamiento para visitantes • Anfitriones, voluntarios, funcionarios de orden público	• Establece el flujo de personas y vehículos. • Admite funciones de advertencia temprana y permite la vigilancia visual no intrusiva. • CISA, GUÍA DE ACCIÓN ANTE LA EMBESTIDA DE VEHÍCULOS • CISA, HOJA INFORMATIVA DEL CURSO DE DETECCIÓN DE VBIED
	Un proceso de gestión del tráfico controlado protege a todos los miembros de la comunidad de accidentes y ataques vehiculares al limitar el flujo del tráfico con puertas, bolardos, conos de tráfico, señalización o personal que dirige el tráfico. Las personas que apoyen este proceso deberán estar claramente identificadas con un chaleco o uniforme de alta visibilidad. En algunas circunstancias, los funcionarios locales de orden público pueden brindar ayuda.	
COMUNICACIÓN DE EMERGENCIA		
	• Postes de llamada de emergencia (cabina de alerta de antipánico)	• Posibilidad de ponerse en contacto con el personal de seguridad de la HoW o los funcionarios de orden público en caso de emergencia. • Minimiza el riesgo en áreas alejadas de los edificios principales en instalaciones más grandes.
	Identifique las áreas de la propiedad alejadas de los edificios principales donde una cabina de llamadas de emergencia podría ser útil, como un estacionamiento distante, un sendero o un jardín de oración. Los equipos informáticos de todo tipo requerirán mantenimiento y pruebas regulares.	
PAISAJE		
	• Retiro de maleza • Instalación de elementos paisajísticos	• Mejore la visibilidad eliminando la maleza excesiva. • Retire cualquier material inflamable.
	Asegúrese de mantener la propiedad y los terrenos en buen estado. Elimine cualquier maleza o elemento del paisaje que obstruya la visibilidad o represente un peligro potencial. Considere instalar elementos paisajísticos, como jardineras grandes, que pueden servir para dirigir el tránsito o disuadir el acceso no autorizado.	

Perímetro central

El *perímetro central* es un área fluida y suele incluir todo lo que está “en el campus” pero fuera del edificio principal. Por ejemplo, las paredes y las puertas exteriores del edificio principal se considerarían parte del perímetro central, al igual que cualquier edificio anexo o espacios como áreas de juegos o áreas de picnic. Los edificios adicionales, como una escuela, una rectoría o una residencia en el lugar, se consideran parte del perímetro central, pero requieren consideraciones de seguridad distintas separadas del edificio principal de la HoW. Varios estudios de caso en el capítulo 1 revelaron vulnerabilidades potenciales relacionadas con la seguridad del perímetro central, con atacantes que se desplazan o inician el ataque en esta zona. Los edificios del perímetro central deben describirse detalladamente durante la evaluación de las vulnerabilidades para que alguien que no esté familiarizado con el lugar, como el personal de respuesta o un consultor de seguridad externo, pueda visualizar rápidamente la propiedad y agilizar las acciones de respuesta ante emergencias.

El perímetro central es a menudo donde convergen muchos tipos diferentes de vulnerabilidades y amenazas, y requiere un plan de seguridad multifacético para hacer frente a estas complejidades.

Otras zonas del perímetro central a tener en consideración son las zonas de picnic o parques infantiles, que serán de especial interés. Estos espacios, que suelen ser utilizados por niños, deben ser una prioridad absoluta para establecer dispositivos de control de acceso y monitorización continua, como con cámaras de CCTV o voluntarios y personal de seguridad. Si es posible, controle el acceso a esta zona con vallas o una barrera física que impida la entrada no autorizada.

Al momento de identificar y priorizar características para asegurar el perímetro central, considere las siguientes opciones:

OPCIONES PARA EL PERÍMETRO CENTRAL

Características de seguridad	Tipos	Beneficios y recursos
PUERTAS		
	• Madera, vidrio o metal • Resistente a impactos o explosiones	• Cuando están cerradas y aseguradas, las puertas disuaden a los intrusos y ayudan a controlar el flujo de personas y el acceso. • Los anfitriones capacitados estratégicamente ubicados pueden ayudar a identificar comportamientos sospechosos.
	Determine el número de entradas y cuándo se utilizan. ¿De qué material son (madera, metal o vidrio)? ¿Cómo se aseguran (cerradura y llave o tarjeta de acceso)? ¿Tienen alarmas? Evalúe si un atacante podría bloquear o encadenar las puertas para evitar el escape durante una emergencia.	
VENTANAS		
	• Con alarmas • Con cerraduras	• Cuando están cerradas y aseguradas, las ventanas disuaden a los intrusos. • Las ventanas también proporcionan una salida de emergencia.
	Las ventanas pueden permitir la entrada no autorizada, especialmente en el nivel del suelo, pero también proporcionan una salida de emergencia si las puertas están obstruidas. Evalúe si se pueden bloquear y asegurar, pero también si se pueden abrir fácilmente en caso de que sea necesario. ¿El vidrio tiene un material de protección de fibra? ¿Tienen alarmas?	
CCTV (VIDEOVIGILANCIA)		
	• Solo grabación • Monitorización activa sin respuesta • Monitorización activa con respuesta	• Admite la monitorización y las alertas de comportamientos sospechosos, incluida la función de advertencia temprana. • Disuade a los intrusos. • Elimina los puntos ciegos.
	Las zonas que requieren cobertura pueden ser entradas exteriores, pasillos exteriores muy transitados o puntos ciegos. El CCTV en el perímetro central se puede implementar con o sin monitorización con un plan de respuesta como se indicó anteriormente en la sección sobre CCTV en el perímetro exterior.	
CONTROL DEL ACCESO		
	• Cerradura y llave estándar • Acceso electrónico	• Limita el acceso a las personas autorizadas y se puede ajustar a los horarios de la HoW.
	Las opciones incluyen el control básico con cerraduras y llaves, aparatos electrónicos más sofisticados que utilizan tarjetas o llaveros de acceso, y programas informáticos integrados con horarios y niveles de acceso asignados.	

OPCIONES PARA EL PERÍMETRO CENTRAL

Características de seguridad	Tipos	Beneficios y recursos
ALARMAS CONTRA INTRUSOS		
	• Colocada en puertas y ventanas	• Alerta rápidamente de la presencia de un intruso al personal de seguridad, los funcionarios de orden público u otros servicios de emergencia.
	Evalúe el costo frente al retorno de la inversión, las necesidades de seguridad de la organización y las funciones que se adaptan a la propiedad y las instalaciones, como los sensores de movimiento.	
GENERADOR ELÉCTRICO DE EMERGENCIA		
	• Con gas natural • Con combustible diésel • Vida útil mínima: 24 horas	• Admite servicios de emergencia, como tecnología de la información (IT), detección de incendios, control de acceso, sistema de CCTV y otras funciones de seguridad conectadas.
	Los generadores eléctricos de emergencia garantizan el funcionamiento de los sistemas críticos en caso de emergencia, como la iluminación para evacuación, los ascensores, la calefacción, la ventilación y el aire acondicionado (HVAC, por sus siglas en inglés) y las rejillas de retorno de aire fresco. Un atacante puede aprovechar la confusión y la angustia generadas por los cortes de energía para causar más daños o lesiones. Las rejillas de retorno de aire fresco deben estar por encima del nivel del suelo para evitar la manipulación del sistema de HVAC. La infraestructura expuesta debe estar cubierta, protegida con cubiertas metálicas cerradas y monitoreada por CCTV.	
PAISAJISMO		
	• Retiro de maleza • Instalación de elementos paisajísticos	• Mejore la visibilidad eliminando la maleza excesiva. • Retire cualquier material inflamable.
	Asegúrese de mantener la propiedad y los terrenos en buen estado. Elimine cualquier maleza o elemento del paisaje que obstruya la visibilidad o represente un peligro potencial. Considere instalar elementos paisajísticos, como jardineras grandes, que pueden servir para dirigir el tránsito o disuadir el acceso no autorizado.	

Perímetro interior

El santuario, o *perímetro interior*, será sin duda la zona más importante a proteger porque es donde se ubicará su recurso más importante: su gente. En la mayoría de los casos, este será el edificio principal, pero las estructuras adicionales, como las escuelas, las rectorías o las residencias, tendrán sus propios perímetros internos que pueden incluir habitaciones para niños, oficinas administrativas, salas de oración u otras áreas comunes.

De los 37 actos de violencia dirigida examinados en el capítulo 1, el 43 por ciento (n=16) ocurrió dentro del perímetro interior o santuario. Al ser el lugar donde suele reunirse la mayor cantidad de gente, por lo general, los ataques dentro del perímetro interior representan el mayor número de víctimas mortales. Con el fin de proteger a su gente, la zona del perímetro interior requiere el más alto nivel de escrutinio, control y monitorización.

Las medidas de seguridad enfocadas en el perímetro interior deben ser lo más detalladas posible. Los miembros del equipo de seguridad deben tener funciones y responsabilidades claramente definidas. Todos los miembros de la congregación deben conocer las capacitaciones básicas de seguridad identificadas en el capítulo 4 y comprender los protocolos para la evacuación de emergencia o escenarios de atacantes activos. Para consideraciones especiales relacionadas con las medidas de seguridad para escuelas y guarderías, consulte el capítulo 6.

La seguridad del perímetro interior generalmente incluye las siguientes características:

OPCIONES PARA EL PERÍMETRO INTERIOR

Características de seguridad	Tipos	Beneficios y recursos

SANTUARIO

- Zona principal de adoración
- Mayor congregación de personas
- Programa de preparación contra francotiradores activos

- Capacitación de feligreses sobre los procedimientos de emergencia
- CISA, PREPARACIÓN CONTRA FRANCOTIRADORES ACTIVOS

El santuario es una de las áreas más importantes que hay que proteger y debe ser un aspecto central en el proceso de planificación de la seguridad. La gestión de incidentes y los planes de acción de emergencia deben centrarse en el santuario y los servicios que se realizan allí.

RECEPCIÓN/GESTIÓN DE VISITANTES

- Las personas son el mayor recurso de seguridad de una HoW
- El poder de un hola
- Capacitación en identificación de actividades sospechosas

- Permite la identificación rápida de actividades, correo o llamadas telefónicas sospechosos.
- Ayuda a controlar el flujo de visitantes de la HoW y gestionar el acceso.
- CISA, EL PODER DE UN HOLA

Considere la posibilidad de implementar un sistema de gestión de visitantes. En el caso de las HoW que cuentan con personal administrativo o de recepción, realice la capacitación adecuada e implemente procedimientos de seguridad detallados, incluida una lista de visitantes autorizados/preseleccionados, la notificación y la selección, la gestión del correo y las llamadas telefónicas y la notificación de actividades sospechosas. Asegúrese de que todos los visitantes conozcan las salidas de emergencia.

CONTROL DEL ACCESO

- Cerradura y llave estándar
- Acceso electrónico

- Limita el acceso a las personas autorizadas y se puede ajustar a los horarios de la HoW.

Las opciones incluyen el control básico con cerraduras y llaves, aparatos electrónicos más sofisticados que utilizan tarjetas o llaveros de acceso, y programas informáticos integrados con horarios y niveles de acceso asignados.

HABITACIONES PARA NIÑOS/ESCUELA

Consulte el capítulo 6.

HABITACIÓN DE REFUGIO EN EL LUGAR

- Habitación sin ventanas con puertas que se cierran con llave u otro espacio interior seguro

- Ofrece una habitación segura para esconderse durante una situación de francotirador activo.
- MANUAL DE REFERENCIA PARA MITIGAR POSIBLES ATAQUES TERRORISTAS CONTRA EDIFICIOS
- GESTIÓN DE RIESGOS: UNA GUÍA PARA MITIGAR POSIBLES ATENTADOS TERRORISTAS CONTRA EDIFICIOS

Identifique un refugio en el lugar o “habitaciones seguras” que se puedan usar durante condiciones climáticas peligrosas o durante un incidente, como una situación de francotirador activo. Estos lugares deben ser habitaciones sin ventanas y con puertas que cierren con llave. El personal y los visitantes deben conocer la ubicación y comprender el propósito de estas habitaciones. Las capacitaciones pueden ayudar a preparar al personal para guiar a los miembros a estos lugares en caso de emergencia. Los planes de refugio en el lugar deben contemplar situaciones climáticas graves, como tornados o incidentes con materiales peligrosos donde respirar el aire exterior podría suponer una amenaza.

OPCIONES PARA EL PERÍMETRO INTERIOR

Características de seguridad	Tipos	Beneficios y recursos
PRIMEROS AUXILIOS/AED		
	• Comprado en tienda • Ofrecido por profesionales	• El personal y los feligreses tienen las herramientas necesarias para responder rápidamente en una emergencia. • USTED ES LA AYUDA HASTA QUE LLEGUE LA AYUDA
	Los equipos de socorro, como los botiquines de primeros auxilios y los desfibriladores externos automáticos (AED, por sus siglas en inglés), se deben guardar en lugares claramente señalizados y verificar periódicamente para garantizar que los suministros estén completos y no han caducado. Los AED se deben probar y recibir mantenimiento para que funcionen correctamente. Se puede contratar a empresas que ofrezcan este servicio.	
SISTEMAS DE ALARMA Y EXTINCIÓN DE INCENDIOS		
	• Comprado en tienda • Ofrecido por profesionales	• Alerta rápidamente al personal de seguridad, Departamento de Bomberos u otros servicios de emergencia en caso de incendio.
	Los detectores de incendios y humo, junto con los sistemas de extinción de incendios, deben cumplir las normas estatales, del condado y municipales. La mayoría de los edificios se someten a inspecciones de los sistemas de emergencia antes de recibir un permiso de ocupación. Todas las HoW deben tener detectores de humo y fuego que funcionen y que cumplan con la normativa. Estas alarmas deben inspeccionarse anualmente para garantizar su pleno funcionamiento. Los extintores de incendios deben colocarse en todos los edificios y estar bien señalizados para facilitar el acceso en caso de emergencia. Estos también deben ser inspeccionados y recibir mantenimiento conforme a las normas locales.	

Resumen

Dividir el área de responsabilidad de su casa de adoración en un perímetro exterior, central e interior ofrece un marco útil para organizar sus programas de seguridad y contemplar las actualizaciones o modificaciones que podrían ser necesarias para mejorar la seguridad física. Su evaluación de vulnerabilidades ayudará a facilitar el proceso de identificación de vulnerabilidades y riesgos y priorizar cualquier cambio que considere necesario de la manera más eficiente y rentable posible.

6 Consideraciones sobre la seguridad en guarderías y escuelas

Introducción

Proporcionar a los niños un espacio seguro para aprender y desarrollarse es un valor fundamental en las comunidades de todo el país. Las escuelas y las guarderías son particularmente vulnerables a la violencia dirigida, por lo que muchas han implementado sólidos programas de seguridad en los últimos años. La amenaza de la violencia escolar es aún mayor en las escuelas K-12, los programas de verano, las guarderías, los programas de estudios religiosos y extracurriculares, y los programas de atención de fin de semana afiliados a las casas de adoración. Garantizar entornos seguros para los niños y los educadores es esencial, y las casas de adoración (HoW) deben priorizar la planificación de la seguridad para las escuelas o las guarderías teniendo en cuenta el alcance total de las vulnerabilidades y los riesgos asociados. Las orientaciones que se ofrecen aquí se basan en los ELEMENTOS FUNDAMENTALES de la seguridad escolar desarrollados por el Departamento de Seguridad Nacional (DHS) y detallados en SchoolSafety.gov.

Evaluación de las instalaciones

Comience por evaluar el lugar y las necesidades de la comunidad afiliada a la escuela o guardería, como la cantidad de alumnos y profesores, la cantidad de entradas y salidas, y la cantidad de aulas. Esto permitirá realizar una evaluación más precisa y elaborar planes de seguridad adaptados para salvaguardar de manera efectiva las instalaciones. Para agilizar este proceso, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) recomienda utilizar evaluaciones sin costo, incluida la GUÍA Y HERRAMIENTA DE EVALUACIÓN DE ESCUELAS K-12 de la CISA, o la APLICACIÓN SITE ASSESS DEL CENTRO DE PREPARACIÓN Y GESTIÓN DE EMERGENCIAS PARA ESCUELAS (REMS, POR SUS SIGLAS EN INGLÉS) administrada por el Departamento de Educación de EE. UU.

SchoolSafety.gov brinda a los centros educativos herramientas para mantener un ambiente seguro para niños y educadores. Los recursos están organizados a lo largo del proceso de preparación: **PREVENIR, PROTEGER Y MITIGAR, RESPONDER Y RECUPERARSE**. El personal de la escuela y la guardería puede realizar una autoevaluación para recibir un plan de acción personalizado con los próximos pasos a tomar y acceder a una variedad de valiosos recursos, capacitaciones y subvenciones adaptadas.

No existe un enfoque único para el cuidado y la educación de los niños. Sin embargo, el Gobierno y el sector privado ofrecen muchos recursos para ayudar a las HoW a desarrollar e implementar medidas de seguridad en las escuelas y las guarderías de acuerdo con los estatutos locales. Estos incluyen recursos sobre políticas de seguridad escolar, seguridad física, clima escolar, técnicas de salud conductual, capacitaciones y oportunidades de financiación. Los asesores de seguridad preventiva (PSA) de la CISA también ofrecen evaluaciones profesionales en el sitio.

Procedimientos y protocolos

Un conjunto adecuado de procedimientos y protocolos es esencial para prevenir y responder a las amenazas. Considere la posibilidad de establecer un plan de acción de seguridad escolar y UN PLAN DE OPERACIÓN EN EMERGENCIAS (EOP, por sus siglas en inglés), y asigne funciones de seguridad a personal específico para prepararse ante una serie de amenazas a una escuela o guardería. Las medidas de seguridad deben abordar las consideraciones de seguridad física y conductual, así como las políticas institucionales. Un proceso de planificación completo debe incluir los siguientes pasos:

- **Cree un PLAN DE ACCIÓN DE SEGURIDAD ESCOLAR personalizado para determinar los próximos pasos importantes que ayudarán a proteger su escuela.**
- **Analice las vulnerabilidades de las políticas actuales, como la falta de información, la falta de orientaciones o las prácticas obsoletas, y coteje esta lista con las mejores prácticas para identificar áreas donde se pueden necesitar nuevos procedimientos o mejoras.**
- **Complete el curso en Internet sobre el DESARROLLO DE PLANES DE OPERACIÓN EN EMERGENCIAS (EOP) K-12 101 para obtener más información sobre cómo crear un EOP eficaz y un plan de implementación.**
- **Utilice la GUÍA INTERINSTITUCIONAL PARA DESARROLLAR PLANES DE OPERACIONES ESCOLARES DE EMERGENCIA DE ALTA CALIDAD para establecer los principios fundamentales y seguir el proceso de planificación de seis pasos.**
- **Utilice LAS ESTRATEGIAS DE RECUPERACIÓN y la lista de recursos del DHS para facilitar la elaboración de un plan de recuperación sólido.**

Es importante considerar la incorporación de las siguientes políticas en los planes de seguridad:

- **Políticas para recoger y dejar a los niños**
- **Políticas para tutores de menores o personas con responsabilidad legal sobre un menor, aparte de los padres**
- **Políticas para supervisar el recreo e implementar medidas de seguridad física adecuadas**
- **Protocolos en caso de conflictos domésticos**
- **Protocolos para visitantes y personas sospechosas en la propiedad o sus alrededores**
- **Protocolos ante un incidente activo en otro edificio de la propiedad**

Seguridad física

Las consideraciones de seguridad física para las escuelas y guarderías incluyen vulnerabilidades adicionales, como patios de recreo, aulas y áreas designadas para dejar y recoger a los niños. Las casas de adoración deben alinear la planificación de la seguridad física con las recomendaciones más generales proporcionadas en el capítulo 5 y adaptadas a los riesgos asociados con estos elementos únicos. Las HoW deben considerar la posibilidad de tomar las siguientes precauciones adicionales:

- **Evaluar la situación actual de la seguridad física de la escuela/guardería con la ayuda de un PSA de la CISA, los recursos de SchoolSafety.gov o utilizando la ENCUESTA DE SEGURIDAD ESCOLAR DEL DHS para identificar brechas en las características físicas y el equipo, y priorizar las actualizaciones.**
- **Utilizar la aplicación móvil segura Site Assess del CENTRO DE PREPARACIÓN Y GESTIÓN DE EMERGENCIAS PARA ESCUELAS (REMS, POR SUS SIGLAS EN INGLÉS) para evaluar la seguridad y recibir una lista de tareas personalizada.**
- **Implementar mejoras de seguridad dentro de los diversos perímetros, como se describe en PARTNER ALLIANCE FOR SAFER SCHOOLS: PAUTAS DE SEGURIDAD Y PROTECCIÓN PARA ESCUELAS K-12.**
- **Evaluar la implementación de LAS ESTRATEGIAS DE SEGURIDAD FÍSICA recomendadas por SchoolSafety.gov.**

Clima escolar

Ofrecer a los alumnos una variedad de sistemas de apoyo social, emocional y conductual puede fortalecer su carácter y permitirles conectar con sus compañeros y educadores de manera más significativa. Estos sistemas pueden mejorar el clima escolar y prevenir la violencia, al mismo tiempo que apoyan la salud mental y capacitan a los alumnos para hablar cuando algo parece sospechoso o peligroso. Un informe del Servicio Secreto de EE. UU. (USSS, por sus siglas en inglés) de 2019 reveló que el 80 % de los atacantes escolares exhibieron previamente un comportamiento que causó preocupación tanto por la seguridad pública como por la seguridad del atacante.[1] Proporcionar al personal y a los alumnos de la HoW un entorno seguro que anime a todos a notificar comportamientos preocupantes ayuda a disminuir la probabilidad de violencia a través de una intervención temprana. Para que este enfoque tenga éxito, las escuelas no solo deben priorizar el clima escolar, sino también proporcionar orientación sobre los mecanismos de notificación disponibles. Las HoW pueden utilizar los siguientes recursos para mejorar el clima escolar general dentro de las escuelas y las guarderías afiliadas:

- **Revisar PRINCIPIOS RECTORES: UNA GUÍA PARA MEJORAR EL CLIMA ESCOLAR para aprender sobre los tres principios críticos para fomentar un clima escolar positivo.**
- **Utilizar las GUÍAS DE ACCIÓN PARA MEJORAR EL CLIMA ESCOLAR para evaluar las cinco acciones clave para mejorar el clima escolar. Cada paso proporcionará medidas, qué hacer y qué no hacer, y preguntas a considerar.**
- **Visitar los recursos sobre el CLIMA ESCOLAR en SchoolSafety.gov para acceder a recursos temáticos adicionales y opciones disponibles de subvención.**

---

1 Centro Nacional de Evaluación de Amenazas, Protecting America's Schools: *A U.S. Secret Service Analysis of Targeted School Violence* (Protección de las escuelas estadounidenses: análisis de la violencia escolar dirigida del Servicio Secreto de EE. UU.) (2019), Servicio Secreto de EE. UU., Departamento de Seguridad Nacional de EE. UU., https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf.

Salud conductual

Promover la salud conductual de los alumnos, así como del cuerpo docente y el personal, como se describe en el capítulo 4, es un paso importante hacia la prevención de la violencia en las escuelas. El éxito social y académico de los alumnos que luchan con problemas de salud mental y conductual suele verse afectado también. Por ejemplo, una encuesta de 2017 concluyó que aproximadamente el 20 % de los alumnos de 12 a 18 años han sufrido acoso escolar.[2] El acoso escolar es un hecho común que puede afectar gravemente la salud física y mental, y ha sido un factor en algunos casos de violencia escolar. Las HoW pueden ayudar a crear entornos más seguros en sus escuelas y guarderías utilizando los recursos disponibles para identificar comportamientos preocupantes e implementando medidas para mejorar la salud mental y física de los alumnos.[3] Tenga en cuenta las siguientes medidas y recursos para identificar y abordar comportamientos amenazantes o preocupantes antes de que puedan conducir a la violencia:

- **Realizar una evaluación de amenazas conductuales para identificar posibles actividades sospechosas y mejorar el apoyo a la salud conductual.**
  - Un equipo multidisciplinario comprometido que incluya y esté respaldado por profesionales calificados de una variedad de disciplinas debe realizar esta evaluación. El equipo debe incluir, como mínimo, un administrador escolar, un consejero de salud mental y un oficial de recursos escolares.
  - Una vez que se completa la capacitación y se establecen roles claros, el equipo debe crear planes, políticas y procedimientos integrales por escrito para el proceso de evaluación de amenazas conductuales, incluido un proceso para evaluar las amenazas y los comportamientos preocupantes notificados.
  - El equipo debe revisar continuamente las amenazas y otros comportamientos preocupantes notificados para identificar áreas de intervención y mitigación.
  - Puede utilizar la herramienta MEJORA DE LA SEGURIDAD ESCOLAR CON EL MODELO DE EVALUACIÓN DE AMENAZAS del USSS para encontrar orientaciones y recursos detallados para crear equipos, realizar evaluaciones de amenazas y crear políticas y procedimientos para las escuelas.
- **Completar el Perfil de salud mental escolar de la EVALUACIÓN DE LA SALUD Y EL RENDIMIENTO ESCOLAR para obtener una descripción general de los servicios y sistemas de salud mental existentes. Esta descripción general ayudará a identificar brechas y contribuirá al seguimiento a nivel nacional de los sistemas de salud mental en las escuelas.**
- **Realizar la EVALUACIÓN DE LA CAPACIDAD DE PREVENCIÓN DEL ACOSO ESCOLAR Y EL PAQUETE DE CAMBIOS para determinar la capacidad de su escuela para prevenir el acoso en siete áreas.**
  - Tras la evaluación, utilice el Portafolio de prevención del acoso escolar para revisar los impulsores basados en evidencia para la prevención del acoso escolar a fin de mejorar las capacidades actuales.

---

2 "Facts About Bullying" (Datos sobre el acoso escolar). StopBullying.gov, Departamento de Salud y Servicios Humanos de los EE. UU., 12 de agosto de 2020, https://www.stopbullying.gov/resources/facts#stats.

3 "Bullying and Cyberbulling" (Acoso escolar y ciberacoso), SchoolSafety.gov, Departamento de Seguridad Nacional de EE. UU., https://www.schoolsafety.gov/prevent/bullying-and-cyberbullying.

Capacitación

La capacitación, los ejercicios y los simulacros son esenciales para crear un ambiente en el que el personal de la escuela y la guardería pueda ayudar a prevenir y responder a situaciones de emergencia. Los alumnos deben recibir capacitaciones sobre las mejores prácticas para mantenerse a salvo durante incidentes, como condiciones climáticas peligrosas o una situación de francotirador activo. Comprender las políticas, las funciones y los procedimientos ayuda a optimizar los esfuerzos de respuesta y mitigar el riesgo de resultados negativos. Las HoW pueden tener en cuenta las siguientes estrategias para capacitar al personal escolar y garantizar que las políticas, los procesos y los procedimientos se mantengan actualizados:

1. Capacitar a los administradores y al personal de la escuela en todos los aspectos del EOP y el plan de implementación con los siguientes pasos:
    A. Capacitar al personal sobre las funciones y responsabilidades dentro del EOP.
    B. Designar a un miembro del personal para coordinar y ejecutar los ejercicios del EOP.
    C. Realizar ejercicios anuales con todo el personal para practicar los procedimientos del EOP. Incluir a socios de la comunidad cuando corresponda.
    D. Evaluar los planes actuales mientras se realizan ejercicios de capacitación para actualizar el EOP en consecuencia.[4]
2. Enviar una SOLICITUD DE CAPACITACIÓN REMS para recibir capacitación presencial gratuita sobre el desarrollo del EOP y estrategias de resiliencia.
3. Completar ejercicios de simulación autodirigidos para alumnos y miembros del cuerpo docente utilizando los KITS DE EJERCICIOS PARA PRINCIPIANTES DEL PROGRAMA DE RESILIENCIA DEL CAMPUS del DHS.
4. Utilizar los principios de la guía del PROGRAMA DE EVALUACIÓN Y EJERCICIOS DE SEGURIDAD NACIONAL para desarrollar, ejecutar y evaluar programas de ejercicios adicionales. La guía debe utilizarse de acuerdo con las prioridades organizacionales para las iniciativas y políticas de seguridad escolar.
5. Revisar LAS CAPACITACIONES, LOS EJERCICIOS Y LOS SIMULACROS que se ofrecen en SchoolSafety.gov para obtener estrategias y recursos adicionales.

---

4 "Training, Exercises, and Drills" (Capacitaciones, ejercicios y simulacros). SchoolSafety.gov, Departamento de Seguridad Nacional de los EE. UU., https://www.schoolsafety.gov/respond-and-recover/training-exercises-and-drills.

Recursos de financiamiento

Las escuelas HoW sin fines de lucro pueden ser elegibles para recibir las subvenciones que se describen a continuación tras presentar una solicitud a su organismo adjudicador estatal (SAA, por sus siglas en inglés) o directamente de la entidad adjudicadora:

- **PROGRAMA DE SUBVENCIONES DE SEGURIDAD SIN FINES DE LUCRO**
  - Financia mejoras de seguridad para organizaciones sin fines de lucro con un alto riesgo de sufrir un atentado terrorista.
- **PROGRAMA DE PREVENCIÓN DE LA VIOLENCIA ESCOLAR (SVPP, POR SUS SIGLAS EN INGLÉS)**
  - Ayuda a mejorar la seguridad de las escuelas en la jurisdicción del beneficiario a través de programas de seguridad escolar basados en evidencias.
- **PROGRAMA DE ALUMNOS, PROFESORES Y FUNCIONARIOS (STOP, POR SUS SIGLAS EN INGLÉS) CONTRA LA VIOLENCIA ESCOLAR: SOLUCIONES TECNOLÓGICAS Y DE EVALUACIÓN DE AMENAZAS PARA ESCUELAS MÁS SEGURAS**
  - Mejora los esfuerzos para reducir los delitos violentos mediante la creación de equipos de evaluación de amenazas escolares, el uso de tecnología para notificar de forma anónima actividades sospechosas relacionadas con la violencia en las escuelas y la creación y la mejora de los Centros Estatales de Seguridad Escolar.
- **PROYECTO DE RESPUESTA DE EMERGENCIA ESCOLAR A LA VIOLENCIA (SERV, POR SUS SIGLAS EN INGLÉS)**
  - Financia servicios relacionados con la educación a corto y largo plazo para agencias educativas locales (LEA, por sus siglas en inglés) e instituciones de educación superior (IHE, por sus siglas en inglés) para apoyar la recuperación tras un suceso violento o traumático que haya perturbado el entorno de aprendizaje.
- **PROGRAMA E-RATE**
  - Permite que las escuelas y bibliotecas públicas accedan de manera rentable a tecnologías que refuerzan las infraestructuras de red y preparan para las futuras necesidades educativas.

Para conocer las oportunidades adicionales de subvención, visite SchoolSafety.gov.

Resumen

Las escuelas y guarderías afiliadas a las casas de adoración comparten muchas de las mismas características y vulnerabilidades que otras instalaciones similares en todo el país, con un nivel de riesgo adicional debido a las afiliaciones con base de fe. Las HoW con tales instalaciones deben ser conscientes en todo momento de estos desafíos y amenazas únicos a la hora de desarrollar e implementar políticas de seguridad sólidas para proteger a los alumnos y maestros y salvaguardar su entorno de aprendizaje.

7 Ciberseguridad

Introducción

Internet ha permitido que las comunidades con base de fe se conecten de formas nunca antes vistas. Muchas casas de adoración (HoW) emplean tecnologías como los servicios de transmisión en vivo y la creación de una comunidad a través de portales en Internet. Esta conectividad permite un gran acceso, pero también abre la puerta a amenazas nuevas y emergentes. Los ciberdelincuentes buscan constantemente nuevos blancos y vulnerabilidades que aprovechar y las HoW no son inmunes.

Las organizaciones con base de fe son vulnerables a los ciberataques debido al tipo de información a la que acceden y almacenan; se las considera blancos fáciles debido a su tamaño y a la percepción de que carecen de protecciones cibernéticas. Como parte de sus operaciones comerciales estándar, las organizaciones con base de fe recopilan y almacenan grandes cantidades de información personal y financiera de feligreses, donantes y empleados. Esta información personal identificable (PII) puede utilizarse para cometer robos de identidad, sustraer fondos de cuentas bancarias e identificar blancos para su posterior explotación. Además de los ciberdelincuentes motivados por el beneficio económico, los perpetradores pueden atacar a las HoW por razones ideológicas. En cualquier de los dos casos, un ciberataque puede dañar la reputación de una HoW de maneras que son difíciles de superar, lo que posiblemente interfiere con la misión general de la institución.

La ciberseguridad debe tratarse como una extensión de otros planes de seguridad y contingencia.

Tipos de ciberataques

Si bien los ciberdelincuentes pueden emplear varios métodos, el análisis de incidentes realizado para este informe reveló que las HoW son particularmente vulnerables a los siguientes tipos de ataques:

Explotación financiera

Al igual que cualquier organización que maneja dinero, las HoW están en riesgo de sufrir explotación financiera. Muchas organizaciones con base de fe ahora recolectan donaciones a través de plataformas móviles o en Internet, lo que crea nuevas vulnerabilidades y oportunidades de explotación. La explotación financiera puede estar vinculada a una variedad de métodos nefastos, incluidas las intrusiones en la red que resultan de la suplantación de identidad y los programas malignos.

Programa de chantaje

Un número cada vez mayor de ciberdelincuentes utilizan programas de chantaje, un tipo de programa informático diseñado para denegar el acceso a un sistema informático o a los datos hasta que se pague una cantidad, para atacar blancos fáciles como hospitales y gobiernos municipales. En ataques de este tipo, los ciberdelincuentes acceden a redes vulnerables y cifran los archivos antes de exigir el pago.

Desfiguración del sitio web

Otra vulnerabilidad potencial se presenta en forma de desfiguración del sitio web, en la que un ciberdelincuente accede a una red o servidor web y cambia o reemplaza el contenido de este con su propia información. Estos ataques, en los que suele emplearse lenguaje o imágenes de odio, buscan causar miedo y socavar los esfuerzos de una comunidad para crear un diálogo interreligioso. Las comunidades con base de fe son cada vez más víctimas de ataques de desfiguración de sitios web.

Creación de una cultura de preparación cibernética

Reducir el riesgo cibernético requiere un enfoque integral y en varias capas, muy parecido al utilizado para abordar las amenazas físicas. Las HoW deben incorporar la resiliencia cibernética en cualquier plan de seguridad que aborde la preparación institucional y de los feligreses. La gestión del riesgo cibernético requiere que las HoW desarrollen prácticas de seguridad sólidas y una *cultura de preparación cibernética* fomentando la higiene cibernética básica y la protección de datos en toda la organización.

Como el asesor de riesgos de la nación y el principal organismo civil encargado de salvaguardar el ciberespacio de la nación, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) es responsable de desarrollar la capacidad nacional de defensa contra los ciberataques. La CISA se dedica a desarrollar y proporcionar a las comunidades con base de fe una serie de recursos destinados a capacitar a las HoW para mitigar una variedad de amenazas cibernéticas. HoW de todos los tamaños pueden utilizar los recursos y consejos que se describen a continuación para realizar cambios con el fin de tener una presencia más segura en Internet.

La CISA ofrece experiencia directa en ciberseguridad y recomienda desarrollar relaciones con sus ASESORES DE CIBERSEGURIDAD (CSA, POR SUS SIGLAS EN INGLÉS) regionales para reforzar la preparación en ciberseguridad, la mitigación de riesgos y las capacidades de respuesta ante incidentes.

LA SEGURIDAD EN LA PRÁCTICA

CREACIÓN DE UNA CULTURA DE PREPARACIÓN CIBERNÉTICA

6 elementos esenciales de una cultura de preparación cibernética

Usted	Impulsa la estrategia, la inversión y la cultura de ciberseguridad.
Su personal	Desarrolla conciencia sobre seguridad y vigilancia.
Sus sistemas	Protegen los activos y las aplicaciones críticos.
Sus ambientes	Asegúrese de que solo tienen acceso a su lugar de trabajo digital las personas autorizadas.
Su información	Realice copias de seguridad y evite la pérdida de información fundamental para las operaciones.
Sus acciones en momentos de estrés	Limitan los daños y aceleran el restablecimiento de las operaciones normales.

Para obtener más información, consulte: ELEMENTOS CIBERNÉTICOS ESENCIALES DE LA CISA

ASESORES DE CIBERSEGURIDAD (CSA) DE LA CISA

¿QUIÉNES SON?	Personal regional de la CISA que ofrece asistencia y apoyo de primera línea para ayudar a preparar y proteger a las partes interesadas frente a las amenazas de ciberseguridad.
¿DÓNDE SE ENCUENTRAN?	Están distribuidos en las diez regiones CISA de los Estados Unidos.
¿QUÉ HACEN?	Involucran a las entidades del sector privado y los gobiernos estatales, locales, tribales y territoriales (SLTT, por sus siglas en inglés) mediante asociaciones y actividades de asistencia directa, como reuniones en el sitio, facilitación de grupos de trabajo y coordinación y apoyo ante incidentes.
¿CUÁL ES SU OBJETIVO?	Promover la preparación en materia de ciberseguridad, la mitigación de riesgos y las capacidades de respuesta ante incidentes, y crear canales de comunicación entre el público y los programas cibernéticos del Departamento de Seguridad Nacional (DHS).

Higiene cibernética

Las organizaciones deben construir una cultura de preparación cibernética desde cero, lo que puede requerir un cambio de mentalidad. La higiene cibernética supone implementar niveles básicos de ciberseguridad y mejorar la concienciación general sobre el riesgo entre el personal, los voluntarios y los feligreses para mejorar la resiliencia y mitigar los efectos de una posible intrusión o ataque. La ciberseguridad es cada vez más importante ya que nuestra cultura sigue dependiendo de la cibertecnología y los beneficios que ofrece, y es una consideración importante para organizaciones de todos los tamaños y ubicaciones.

Las HoW deben priorizar el conocimiento de los conceptos clave de ciberseguridad y adoptar las mejores prácticas del sector, y la mayoría de los proveedores de servicios de Internet están listos para ayudar a resolver muchas vulnerabilidades comunes. Además de los pasos descritos en la GUÍA DE RECURSOS DE CIBERSEGURIDAD, existen varios enfoques de sentido común que las organizaciones con base de fe pueden utilizar para crear una cultura de ciberseguridad:

- **Consultar los ELEMENTOS CIBERNÉTICOS ESENCIALES de la CISA para obtener información importante sobre la preparación cibernética de las organizaciones.**
- **Mantenerse al día sobre las actualizaciones de seguridad y habilitar las actualizaciones automáticas siempre que sea posible.**
  - COMPRENDER LOS PARCHES Y LAS ACTUALIZACIONES DE LOS PROGRAMAS INFORMÁTICOS
- **Suscribirse al SISTEMA NACIONAL DE CONCIENCIACIÓN CIBERNÉTICA (NCAS, POR SUS SIGLAS EN INGLÉS) para recibir alertas, informes de análisis, boletines o consejos sobre ciberseguridad.**
- **Realizar copias de seguridad de archivos y datos importantes con regularidad.**
  - Los archivos importantes que necesitan copias de seguridad y protección adicionales pueden incluir: registros financieros; listas, direcciones y PII de feligreses; registros de propiedades; archivos de empleados y voluntarios; registros de donaciones en Internet, etc.

- **Mantenerse alerta ante los correos electrónicos sospechosos y tener cuidado al abrir archivos adjuntos o enlaces (PRECAUCIÓN CON LOS ARCHIVOS ADJUNTOS AL CORREO ELECTRÓNICO).**
- **Si está disponible, habilitar la autenticación en dos fases (2FA, por sus siglas en inglés) en las cuentas de administrador del sitio web.**
- **Conocer LOS RIESGOS PARA LOS TELÉFONOS MÓVILES y realizar ajustes para proteger los dispositivos móviles afiliados a su HoW.**
- **Establecer prácticas y políticas de seguridad básicas para los empleados, como exigir contraseñas seguras, y establecer pautas de uso adecuado de Internet que detallen las sanciones por infringir las políticas de ciberseguridad de la empresa. Aplique estas políticas con coherencia.**
- **Establecer normas de conducta para la gestión y la protección de la información de los feligreses y donantes y otros datos importantes. Considere restringir el acceso o proteger con contraseña los archivos e instalar programas informáticos para proteger el sitio web y la plataforma de donaciones.**
- **Instalar programas antivirus en todas las computadoras y actualizarlo periódicamente.**

Seguridad en Internet

Internet facilita que las organizaciones con base de fe se pongan en contacto con sus miembros y con posibles nuevos miembros, mientras que las redes sociales ofrecen una forma efectiva de mantenerse conectados y compartir actualizaciones. Sin embargo, la facilidad de acceso y la informalidad también hacen que estas plataformas sean atractivas para agentes malintencionados, que pueden aprovechar la información que está fácilmente disponible. Si bien muchos sitios son benignos, las plataformas de las redes sociales se han utilizado para distribuir códigos maliciosos. Del mismo modo, la información personal publicada en las redes sociales se puede utilizar para llevar a cabo ataques de ingeniería social o para planificar ataques físicos, como a través del aprovechamiento de los horarios o planes de adoración. Incluso sin la presencia de agentes tecnológicos sofisticados, aquellos que buscan acosar o intimidar aprovechan las plataformas en Internet.

LA SEGURIDAD EN LA PRÁCTICA

ELECCIÓN DE CONTRASEÑAS SEGURAS

QUÉ HACER:

- Utilizar la contraseña más larga permitida.
- Utilizar símbolos y números.
- Utilizar diferentes contraseñas para cada cuenta.

QUÉ NO HACER:

- Utilizar palabras del diccionario.
- Utilizar contraseñas basadas en información personal.
- Compartir su contraseña.

La adopción de niveles básicos de seguridad y la concienciación pueden permitir que las HoW sigan conectándose a Internet de manera segura. Los siguientes recursos pueden ayudarle a conectarse a Internet de manera segura:

- **Implemente las mejores prácticas generales de privacidad en Internet, como se indica en la HOJA DE CONSEJOS SOBRE PRIVACIDAD EN INTERNET.**
- **Revise SEGURIDAD EN LAS REDES SOCIALES y la HOJA DE CONSEJOS SOBRE CIBERSEGURIDAD EN LAS REDES SOCIALES para comprender la variedad de amenazas asociadas con las redes sociales.**
- **Consulte las PAUTAS PARA PUBLICAR INFORMACIÓN EN INTERNET y supervise la información publicada en los sitios web de las instalaciones o en las cuentas de redes sociales, incluidos los horarios y actividades de adoración. Considere la posibilidad de publicar los horarios semanalmente, en lugar de mensualmente, o restringir la publicación de los horarios a un portal de miembros.**
- **Preste atención a lo que se envía por correo electrónico a la congregación. Mantenga actualizadas las listas de distribución para asegurarse de que solo envía correos electrónicos a los miembros actuales que necesitan la información.**
- **Haga ajustes para priorizar la socialización de forma segura.**
- **El ciberacoso puede variar en gravedad y puede indicar una tendencia hacia comportamientos más graves. Comprenda los conceptos básicos del ciberacoso y consulte CÓMO ENFRENTARSE A LOS CIBERACOSADORES para obtener información sobre cómo proteger a su comunidad.**
- **Comprenda los riesgos que supone la ingeniería social e implemente los procedimientos descritos para EVITAR ATAQUES DE INGENIERÍA SOCIAL Y SUPLANTACIÓN DE IDENTIDAD.**

Prácticas de seguridad y concienciación

Además de las mejores prácticas básicas que todas las personas y organizaciones pueden adoptar, las HoW pueden considerar la posibilidad de implementar medidas más avanzadas para mejorar la resiliencia frente a posibles incidentes cibernéticos. Un programa sólido de ciberseguridad incluirá actividades centradas en la planificación de la respuesta ante incidentes cibernéticos, la capacitación de las principales partes interesadas y el desarrollo de protocolos de notificación para identificar actividades sospechosas. La creación de un programa de ciberseguridad eficaz requiere tanto un conocimiento de las tácticas como una nueva forma de pensar. Las HoW deben considerar la posibilidad de tomar las siguientes medidas:

- **Identifique umbrales y métodos de notificación de incidentes cibernéticos, tanto internamente al director del programa de seguridad como externamente a las autoridades, consultando la tarjeta de consejos sobre CÓMO RECONOCER Y PREVENIR LA CIBERDELINCUENCIA y el sitio de la CISA para NOTIFICAR INCIDENTES CIBERNÉTICOS.**
- **Hable con otras instituciones con base de fe acerca de las medidas que están tomando para protegerse. Asegúrese de compartir la información que tiene para ayudarlas también.**
- **Suscríbase al BOLETÍN MENSUAL DE US-CERT para obtener información sobre seminarios en Internet y talleres sobre ciberseguridad, nuevas publicaciones y mejores prácticas.**
- **Realice una REVISIÓN AUTODIRIGIDA DE RESILIENCIA CIBERNÉTICA (CRR, POR SUS SIGLAS EN INGLÉS) de la CISA para evaluar las medidas de seguridad existentes e identificar las áreas de mejora.**
- **Sepa cómo comunicar y a quién involucrar durante una crisis, incluida LA NOTIFICACIÓN DE CIBERATAQUES E INCIDENTES A LA CISA y a las autoridades correspondientes.**

- **Elabore una lista detallada de inventario de datos y activos físicos y actualícela periódicamente.**
  - Incluya el fabricante, el modelo, el número de serie y la información de soporte de los equipos y programas informáticos. En el caso de los programas informáticos, incluya la versión específica que está instalada y funcionando.
  - Sepa dónde se almacenan los datos y la tecnología y quién tiene acceso a ambos.
- **Realice pruebas de vulnerabilidad en su sitio web mediante el uso de un servicio de detección de vulnerabilidades de pago o el análisis gratuito de protocolo de Internet (IP, por sus siglas en inglés) estático de la CISA para detectar vulnerabilidades y debilidades conocidas.**
- **Consulte OBSERVACIONES DE LA CISA: SOLUCIONAR LAS VULNERABILIDADES EN SISTEMAS ACCESIBLES A TRAVÉS DE INTERNET para obtener más información. Realice copias de seguridad periódicamente y evite la pérdida de información fundamental para las operaciones.**
  - Evalúe una serie de opciones para realizar copias de seguridad de datos que podrían incluir una función que respalde sus datos automáticamente.
  - Mantenga copias de seguridad en línea y fuera de línea que no estén permanentemente conectadas a las computadoras y redes que están respaldando. Esta medida reduce el riesgo de dañar una copia de seguridad.
- **Defina el comportamiento esperado en toda la organización para crear una cultura de seguridad entre el personal. Exija el cumplimiento de los acuerdos de usuario final y las políticas de ciberseguridad de la organización.**
- **Cree una red de relaciones de confianza con socios religiosos y organismos gubernamentales locales para compartir información sobre las amenazas y acceder a información oportuna sobre amenazas cibernéticas.**
- **Asista a una reunión regional dirigida por la CISA centrada en la evolución de las necesidades de gestión de riesgos cibernéticos y los recursos comunitarios disponibles para diversos sectores y regiones.**
- **Utilice el PAQUETE ESCALABLE DE EJERCICIOS TEÓRICO SOBRE CIBERSEGURIDAD (CTEP, POR SUS SIGLAS EN INGLÉS) de la CISA para elaborar y personalizar un ejercicio teórico sobre ciberseguridad acorde a su organización.**
- **Las organizaciones deben determinar su riesgo de DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL DE IDENTIFICACIÓN PERSONAL. Tras determinar este riesgo, deben seguir las mejores prácticas de la industria para evitar la divulgación.**
- **Elabore un plan integral de respuesta ante incidentes cibernéticos que se centre en la recuperación de sistemas, redes y datos de copias de seguridad conocidas y correctas y capacite al personal al respecto.**
  - Asegúrese de que este plan sea aprobado formalmente por la alta dirección de su organización para garantizar su aceptación.
  - Ponga a prueba periódicamente su plan de respuesta ante incidentes para asegurarse de que cada parte de su organización sepa cómo responder a incidentes de ciberseguridad tanto básicos como a gran escala.

Acción contra amenazas específicas

Los ciberataques se presentan de muchas maneras y cada una requiere una respuesta específica. Afortunadamente, estas contramedidas a menudo se superponen y son una parte esencial de la creación de una cultura sólida de higiene y preparación cibernética.

Programas malignos y virus

Los programas malignos y los virus son programas informáticos maliciosos diseñados para comprometer la integridad de su computadora o dispositivo móvil y dar a los atacantes la capacidad de vigilar su actividad o robar sus datos. Hay varias consideraciones importantes para protegerse a usted mismo y a su organización contra los programas malignos y las intrusiones en la red:

- **Instruya a su personal sobre los diferentes tipos de programas malignos que pueden infectar los dispositivos y las mejores prácticas para protegerlos. Lea la TARJETA DE CONSEJOS SOBRE PROGRAMAS MALIGNOS de la CISA.**
- **Mantenga todos los programas informáticos de seguridad, los navegadores web y los sistemas operativos actualizados para evitar que los atacantes se aprovechen de las vulnerabilidades conocidas.**
- **Evite hacer clic en enlaces sospechosos en correos electrónicos o publicaciones en Internet.**
- **Utilice un programa informático de seguridad para escanear el bus universal en serie (USB, por sus siglas en inglés) y otros dispositivos externos que puedan ser infectados por virus y programas malignos.**

Ataques de suplantación de identidad

Un ataque de suplantación de identidad utiliza el correo electrónico o sitios web maliciosos para infectar su máquina o recopilar datos personales y financieros. Los correos electrónicos de suplantación de identidad pueden parecer procedentes de una institución o sitio web real y solicitar información personal. Cuando los usuarios responden con la información solicitada o hacen clic en el enlace proporcionado, los atacantes pueden acceder a las cuentas. Hay varias consideraciones clave que le ayudarán a protegerse de los intentos de suplantación de identidad:

- **Familiarice a su personal con las mejores prácticas y los ejemplos de posibles correos electrónicos de suplantación de identidad descritos en la TARJETA DE CONSEJOS DE SUPLANTACIÓN DE IDENTIDAD de la CISA.**
- **Evite hacer clic en los hipervínculos de los correos electrónicos. Si es posible, escriba la URL en su barra de búsqueda.**

LA SEGURIDAD EN LA PRÁCTICA

RECONOCIMIENTO DE LOS ATAQUES DE SUPLANTACIÓN DE IDENTIDAD

¿Se trata de una suplantación de identidad?

1. ¿Parece que el correo electrónico proviene de una institución real, pero al examinarlo con más detenimiento nota ligeras modificaciones? (por ejemplo: .net en lugar de .com, faltan letras, etc.)
2. ¿El correo electrónico solicita que la información personal se envíe por correo electrónico o haciendo clic en un enlace?
3. ¿El correo electrónico le ruega que actúe rápidamente para evitar consecuencias graves?
4. Cuando pasa el cursor sobre un enlace web, ¿va a un sitio que no está relacionado con el texto?

En caso de duda, deséchelo: *si parece sospechoso, ¡bórrelo!*

- **Tenga cuidado con los correos electrónicos que ofrecen algo que suena demasiado bueno para ser verdad o que instan a actuar con rapidez.**
- **No revele información personal o financiera en un correo electrónico y no responda a solicitudes de esta información, ni siquiera a través de enlaces enviados por correo electrónico.**
- **Preste atención a la dirección de correo electrónico o la URL del sitio web proporcionados en un correo electrónico sospechoso. Los sitios web y las cuentas maliciosos pueden lucir idénticos a los sitios y correos electrónicos legítimos, pero pueden usar variaciones ortográficas o dominios diferentes.**
- **Si no está claro si una solicitud por correo electrónico es legítima, intente comunicarse con la empresa directamente o búsquela en Internet, ¡pero no use la información facilitada en el correo electrónico!**

Programa de chantaje

Los ataques con programas de chantaje usan programas malignos para denegar el acceso a sistemas o datos con fines de extorsión. Tras bloquear el acceso de un usuario a los datos o al sistema, el ciberdelincuente retiene los sistemas o los datos como rehenes hasta que se paga un rescate. Los ataques con programas de chantaje suelen dirigirse a los usuarios finales a través de correos electrónicos de suplantación de identidad y aplicaciones no seguras. La prevención es la defensa más eficaz contra los ataques con programas de chantaje, por lo que es fundamental tener en cuenta varias medidas de precaución:

- **Familiarice a su personal con el conjunto de RECURSOS CONTRA LOS ATAQUES CON PROGRAMAS DE CHANTAJE de la CISA, incluido el seminario web "Combatir los ataques con programas de chantaje" y LOS CONSEJOS DE SEGURIDAD PARA PROTEGERSE CONTRA LOS ATAQUES CON PROGRAMAS DE ESTE TIPO.**
- **Tenga cuidado al abrir archivos adjuntos de correo electrónico, especialmente si se trata de archivos comprimidos o ZIP.**
- **Para obtener información sobre cómo proteger las redes de su organización y cómo responder a un posible ataque con programas de chantaje, consulte la GUÍA DE ATAQUES CON PROGRAMAS DE CHANTAJE, un recurso integral centrado en el cliente con las mejores prácticas y formas de prevenir, proteger y responder a un ataque con programas de chantaje.**
- **Implemente un programa de concienciación y capacitación. Debido a que los usuarios finales son los objetivos, los empleados y otras personas que acceden a la red deben ser conscientes de la amenaza que implican los ataques con programas de chantaje y de cómo se llevan a cabo.**
- **Asegúrese de que todas las aplicaciones y sistemas operativos se actualicen regularmente con los últimos parches de seguridad.**
- **Instale y actualice regularmente los programas informáticos antivirus, los servidores de seguridad y los filtros de correos electrónicos para reducir el tráfico de red malicioso.**
- **Configure servidores de seguridad para bloquear el acceso a direcciones IP maliciosas conocidas que se pueden encontrar en las ALERTAS Y PRODUCTOS ANALÍTICOS de NCAS.**

Desfiguración del sitio web

La desfiguración de un sitio web ocurre cuando un atacante toma el control de un sitio web público. En los últimos años, las HoW han sufrido un número creciente de desfiguraciones de sitios web. Estos tipos de ataques suelen incluir imágenes y lenguaje perturbadores con el objetivo de infundir miedo en una comunidad específica y dañar la reputación del sitio web y su propietario. Los ataques

a los sitios web puede amenazar su integridad, así como la confidencialidad de cualquier información vinculada a él. Para una organización con base de fe, esto puede ser extremadamente perturbador y vergonzoso. Hay varias medidas importantes que las HoW pueden tomar para protegerse contra los ciberataques a través de sitios web:

- **Familiarice a su personal con los aspectos básicos de LA SEGURIDAD DEL SITIO WEB.**
- **Examine los servicios proporcionados por el proveedor de alojamiento de sitios web de su organización y contáctelo para analizar la implementación de medidas de seguridad según los servicios proporcionados.**
- **Cambie todos los nombres de usuario y contraseñas predeterminados proporcionados por el registrador de dominios y el sistema de nombres de dominio (DNS, por sus siglas en inglés), ya que generalmente están disponibles en Internet y se pueden usar en un ataque.**
- **Actualice periódicamente las contraseñas de todas las cuentas en los sistemas que pueden realizar cambios en el registro DNS o el sitio web de su organización.**
- **Revise de manera habitual los registros DNS y del registrador de todos los dominios. Consulte PERSPECTIVAS CIBERNÉTICAS DE LA CISA: MITIGAR LA MANIPULACIÓN DE LA INFRAESTRUCTURA DNS para obtener más información.**
- **Haga cumplir la autenticación multifactorial (MFA, por sus siglas en inglés) para todos los usuarios autorizados y administradores de sitios web.**
- **Habilite el registro y audite periódicamente los registros del sitio web para detectar acontecimientos sobre seguridad o sobre accesos indebidos. El acceso inusual o sospechoso debe investigarse más a fondo.**
- **Realice inspecciones periódicas para detectar vulnerabilidades y corrija las críticas y altas. Consulte OBSERVACIONES CIBERNÉTICAS DE LA CISA: SOLUCIONAR LAS VULNERABILIDADES EN SISTEMAS ACCESIBLES A TRAVÉS DE INTERNET para obtener más información.**

Resumen

Las HoW no son inmunes a los ciberataques. Una forma importante de proteger su organización es estar atento a los incidentes de ciberseguridad y notificar los que detecte. La CISA ofrece varios servicios de fácil acceso para ayudar a las organizaciones de todos los tamaños a prepararse y responder a los incidentes cibernéticos:

- **Si ocurre un incidente en su organización, considere notificar cualquier intento de suplantación de identidad, ataque con programas malignos o vulnerabilidades identificadas a través de la HERRAMIENTA SEGURA DE NOTIFICACIÓN o el SISTEMA DE NOTIFICACIÓN DE INCIDENTES de la CISA.**
- **La CISA analiza ataques con programas malignos, mensajes de suplantación de identidad y vulnerabilidades de sitios web o programas informáticos para proporcionar información práctica que ayude a los ciudadanos a protegerse mejor en el futuro.**
- **La CISA sugiere notificar de cualquier actividad que considere que cumple con los criterios de un incidente o ataque de suplantación de identidad. La política de la CISA es preservar la confidencialidad de toda la información específica de su organización, a menos que usted autorice la divulgación de dicha información.**

Lograr una cultura de preparación cibernética requiere una nueva forma de pensar sobre la ciberseguridad y una inversión para priorizar la higiene cibernética básica. Comprender los conceptos básicos de la ciberseguridad e incorporar las mejores prácticas sencillas puede marcar una diferencia significativa a la hora de proteger sus instalaciones contra ciberataques perjudiciales. Los empleados y voluntarios deben recibir capacitación sobre estas mejores prácticas y procedimientos y saber cómo reconocer y actuar ante actividades sospechosas durante una crisis cibernética. La ciberseguridad debe tratarse como una extensión de otros planes de seguridad y contingencia.

8 Resumen y conclusiones generales

Los ataques dirigidos a casas de adoración (HoW) son una amenaza estadísticamente infrecuente, pero real, para el pueblo estadounidense y una prioridad absoluta para el Departamento de Seguridad Nacional (DHS). En su calidad de asesor de riesgos de la nación, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) ha preparado esta guía para ayudar a las casas de adoración y organizaciones con base de fe a desarrollar una estrategia de seguridad integral para ayudar a proteger la vida y la propiedad.

En esta guía de seguridad, la CISA analizó diez años de ataques dirigidos a casas de adoración para contextualizar las recomendaciones de seguridad para toda la organización descritas en los capítulos anteriores. Los estudios de caso revisados son ejemplos de la variedad de amenazas que enfrenta una casa de adoración a diario. Desde ataques físicos, como situaciones de francotirador activo o ataques con bombas, hasta ciberataques menos visibles, una casa de adoración debe estar alerta en sus prácticas de seguridad.

La mejor manera de mitigar un posible ataque es adoptar un enfoque integral en materia de seguridad. Esto requiere asignar funciones y responsabilidades claras para tomar decisiones en materia de seguridad, planificar e implementar los procedimientos y capacidades en toda la organización. Un plan de seguridad sólido debe adaptarse a las necesidades y prioridades específicas de la casa de adoración.

Para desarrollar e implementar prácticas sólidas de seguridad, la CISA recomienda evaluar la implementación de las siguientes medidas:

- Establecer un plan de seguridad en varias capas que identifique funciones y responsabilidades claras para desarrollar e implementar medidas de seguridad.
- Crear planes de acción de emergencia, planes de continuidad del negocio y planes de respuesta ante incidentes que estén bien comunicados y se hayan puesto en práctica con el equipo de seguridad para una comprensión plena.
- Realizar una evaluación de vulnerabilidades para conocer los riesgos a los que está expuesta la casa de adoración, a partir de la cual podrá priorizar la implementación de las medidas de seguridad consecuentes.

- Fomentar la preparación y la resiliencia de la comunidad estableciendo una cultura organizacional de cuidado en la que todos los miembros y visitantes reciban el apoyo adecuado, y las amenazas creíbles se notifiquen a través de los canales identificados previamente.
- Aplicar medidas de seguridad física para controlar y proteger el perímetro exterior, medio e interior, al mismo tiempo que respeta el propósito de cada área de la casa de adoración.
- Enfocarse en la seguridad de los niños mediante la implementación de medidas de seguridad en los centros de cuidado infantil, las guarderías y las escuelas.
- Implementar las mejores prácticas de ciberseguridad para salvaguardar la información importante y prevenir un posible ciberataque.

Estas opciones de seguridad no detendrán todas las amenazas hacia una casa de adoración, pero un enfoque de seguridad integral ofrece la mejor solución para proteger a las personas y los bienes de un ataque. Las HoW deben adaptar este conocimiento a sus necesidades específicas de seguridad y, al mismo tiempo, garantizar que se mantengan los valores inherentes de apertura y bienvenida.

Proyecciones futuras

La CISA continuará trabajando con organizaciones con base de fe (FBO) para comprender el fenómeno que suponen los ataques de este tipo y brindar orientación sobre las formas de mitigar el riesgo. A medida que la CISA mira hacia el futuro, está claro que se necesitan más estudios y que algunos de los pasos tangibles más importantes serán desarrollar una definición compartida de violencia dirigida contra las HoW, desarrollar un sistema unificado de seguimiento y notificación que sirva de base para futuros análisis y planes de seguridad, y seguir vinculando a las HoW de todo el país para compartir mejor los recursos, las ideas y las soluciones.

Apéndice 1: Recursos consolidados para las casas de adoración

La guía de recursos de esta sección es una consolidación de todos los recursos proporcionados en esta guía de seguridad, organizados por capítulo y sección. Esta lista no es exhaustiva, pero ofrece información útil que se puede adaptar al plan de seguridad de cualquier casa de adoración (HoW) en función del riesgo y la prioridad.

CATEGORÍA	RECURSO
Capítulo 1: Introducción	
	DHS, Marco estratégico para contrarrestar el terrorismo y la violencia dirigida https://www.dhs.gov/publication/dhs-strategic-framework-countering-terrorism-and-targeted-violence
	FBI, Rastreador de delitos de odio https://www.fbi.gov/services/cjis/ucr/hate-crime
Capítulo 2: Determinación del enfoque integral en materia de seguridad	
Preparación para emergencias	DHS, Serie de informes sobre seguridad ciudadana en las casas de adoración https://www.cisa.gov/publication/houses-worship-hometown-security-report-series-may-2017
	DHS, Guía para elaborar planes de acción de emergencia de alta calidad para casas de adoración https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness
	CISA, Plantilla y guía del plan de acción de emergencia en una situación de francotirador activo https://www.cisa.gov/publication/active-shooter-emergency-action-plan-guide
	CISA, Video del plan de acción de emergencia en una situación de francotirador activo https://www.cisa.gov/active-shooter-emergency-action-plan-video
	CISA, Organizaciones con base de fe: Recursos de seguridad para casas de adoración https://www.cisa.gov/faith-based-organizations-houses-worship
	CDC, Plantilla del plan de acción de emergencia https://www.cdc.gov/niosh/docs/2004-101/emrgact/emrgact.pdf
	FEMA, Pautas para la elaboración de planes de emergencia https://training.fema.gov/hiedu/docs/cgo/week%203%20-%20producing%20emergency%20plans.pdf
	FEMA, Centro de Preparación Doméstica https://cdp.dhs.gov/
	FEMA, Lista de verificación del kit de emergencia https://www.fema.gov/media-library-data/1553273223562-797451b5cb0bee8d35d3e4e85e3830d6/Checklist.pdf
	FEMA, Preparación de las comunidades con base de fe https://www.fema.gov/emergency-managers/individuals-communities/faith-preparedness
	Cruz Roja Estadounidense, Lista de verificación de primeros auxilios https://www.redcross.org/get-help/how-to-prepare-for-emergencies/anatomy-of-a-first-aid-kit.html

CATEGORÍA	RECURSO
Operaciones en emergencias	CDC, Plan de comunicación de crisis https://emergency.cdc.gov/cerc/ppt/CERC_Crisis_Communication_Plans.pdf
	CISA, Preparación contra francotiradores activos https://www.cisa.gov/active-shooter-preparedness
	CISA, Talleres de preparación contra francotiradores activos https://www.cisa.gov/active-shooter-workshop-participant
	CISA, Video de Correr, ocultarse, luchar https://www.youtube.com/watch?v=W2Vqtf5KqAQ&feature=youtu.be
	CISA, Video de preparación contra francotiradores activos https://www.cisa.gov/options-consideration-active-shooter-preparedness-video
	CISA, Capacitación sobre francotiradores activos para el personal de respuesta https://www.cisa.gov/first-responder
	Ready.gov, Recursos para situaciones de francotiradores activos https://www.ready.gov/active-shooter
	Ready.gov, Recursos de capacitación https://www.ready.gov/training-0
	Ready.gov, “Usted es la ayuda hasta que llegue la ayuda” https://community.fema.gov/until-help-arrives
	“Detener el sangrado” https://www.stopthebleed.org/training
	DHS, Capacitación en artefactos explosivos improvisados https://cdp.dhs.gov/training/course/AWR-337
	CISA, Mitigación de ataques de vehículos https://www.cisa.gov/first-responder
	CISA, Capacitación sobre amenazas de agentes internos https://www.cisa.gov/training-awareness
Continuidad del negocio	Ready.gov, Paquete de planificación de continuidad del negocio https://www.ready.gov/business-continuity-planning-suite
	CISA, Guía para la recuperación tras una situación de francotirador activo https://www.cisa.gov/publication/active-shooter-recovery-guide
	CISA, Paquete de planificación de la continuidad del sector de servicios de emergencia https://www.cisa.gov/emergency-services-sector-continuity-planning-suite
	CISA, Seguridad local: conectar, planificar, capacitar, notificar https://www.cisa.gov/connect-plan-train-report
	FEMA, Programas Nacionales de Continuidad https://www.fema.gov/media-library/assets/documents/89510
	DOJ, Herramientas de ayuda para las víctimas de la violencia en masa https://www.ovc.gov/pubs/mvt-toolkit/recovery.html

Capítulo 3: Realización de una evaluación integral de la vulnerabilidad

	PSA de la CISA https://www.cisa.gov/protective-security-advisors
	CISA, Autoevaluación de la seguridad de las casas de adoración https://www.cisa.gov/publication/houses-worship-security-self-assessment
	EEOC, Guía de verificación de antecedentes https://www.eeoc.gov/background-checks

Capítulo 4: Desarrollo del nivel de preparación y resiliencia de la comunidad

CATEGORÍA	RECURSO
Gestión de amenazas	CISA, Video sobre El camino hacia la Violencia https://www.cisa.gov/pathway-violence-video
	CISA, Hoja informativa sobre El camino hacia la Violencia https://www.cisa.gov/publication/pathway-violence-fact-sheet
	DHS, Infografía de la campaña Si ve algo, diga algo® https://www.dhs.gov/see-something-say-something/recognize-the-signs
	DHS, Tarjeta de bolsillo de la campaña Si ve algo, diga algo® https://www.dhs.gov/see-something-say-something/campaign-materials
	DHS, Indicadores y factores de riesgo https://www.dhs.gov/publication/risk-factors-and-targeted-violence-and-terrorism-prevention
	CISA, Amenazas de agentes internos: Reconocer y notificar el comportamiento anómalo https://www.cisa.gov/recognize-and-report
	DHS, Si ve algo, diga algo® : Acepte el desafío https://www.dhs.gov/see-something-say-something/take-challenge
	DHS, Notificación de actividades sospechosas (SAR): Indicadores y ejemplos https://www.dhs.gov/publication/suspicious-activity-reporting-indicators-and-examples
	DHS, Capacitación de la iniciativa SAR a nivel nacional (NSI): Seguridad del sector privado https://www.dhs.gov/course/nsi-training-private-sector-security
	DHS, Cómo integrar la notificación de actividades sospechosas en las operaciones de su agencia https://www.dhs.gov/publication/10-ways-integrate-sar-your-agency-s-operations
	DHS, Iniciativa SAR a nivel nacional (NSI): Seguridad para los eventos religiosos y las casas de adoración https://www.dhs.gov/publication/safety-faith-based-events-and-houses-worship-nsi-awareness-flyer
	FBI, Información de contacto de la oficina local https://www.fbi.gov/contact-us/field-offices
	FBI, Formulario para pistas https://tips.fbi.gov/
	FEMA, Centro de recursos del Sistema de mando de incidentes (ICS) https://training.fema.gov/emiweb/is/icsresource/
Participación de la comunidad y relaciones con la comunidad	CISA, Reuniones en masa: Concienciación en materia de seguridad para blancos fáciles y lugares concurridos https://www.cisa.gov/publication/active-assailant-security-resources
	CISA, Guía de las mejores prácticas para el control del público https://www.cisa.gov/publication/patron-screening-guide
	CISA, Guía de procedimientos para el control de bolsos en lugares públicos https://www.cisa.gov/publication/public-venue-bag-search-guide
	Ready.gov, Equipo Comunitario de Respuesta en Emergencias (CERT) https://www.ready.gov/cert
	DOJ, Foro sobre la protección de los lugares de adoración https://www.justice.gov/crs/our-work/facilitation/protecting-places-of-worship
	Ready.gov, “PrepareAthon” https://www.ready.gov/prepareathon
	CISA, Programa de evaluación de la resiliencia regional (RRAP, por sus siglas en inglés) https://www.cisa.gov/regional-resiliency-assessment-program

CATEGORÍA	RECURSO
Relación de enlace profesional	Ready.gov, Información para la gestión de emergencias locales https://www.ready.gov/local
	Herramienta para identificar las regiones CISA más cercanas https://www.cisa.gov/cisa-regional-offices
	CISA, Hoja informativa sobre el Programa de asesores de seguridad preventiva (PSA) https://www.cisa.gov/publication/psa-fact-sheet
	DHS, Servicio Federal de Protección https://www.dhs.gov/topic/federal-protective-service
Servicios de salud mental y asistencia social	MentalHealth.gov, "¿Qué es la salud mental?" https://www.mentalhealth.gov/basics/what-is-mental-health
	MentalHealth.gov, Charla sobre salud mental: Información para líderes comunitarios y religiosos https://www.mentalhealth.gov/talk/faith-community-leaders
	SAMHSA, Cómo abordar el riesgo de comportamiento violento en los jóvenes https://www.samhsa.gov/sites/default/files/addressing-youth-violence.pdf
	SAMHSA, FindTreatment.gov https://www.findtreatment.gov/
	SAMHSA, Localizador de servicios de tratamiento para la salud conductual https://findtreatment.samhsa.gov/locator/stateagencies.html#.XurGoG5Fwgo

Capítulo 5: Protección para las instalaciones

Subvenciones	FEMA, Programa de Subvención de Seguridad para Organizaciones sin Fines de Lucro https://www.fema.gov/grants/preparedness/nonprofit-security
	FEMA, Tipos de subvenciones https://www.fema.gov/grants
Seguridad a través del diseño	FEMA, Diseño urbano y del emplazamiento para la seguridad https://www.fema.gov/media-library-data/20130726-1624-20490-9648/fema430.pdf
	FEMA, Manual de referencia para mitigar posibles atentados terroristas contra edificios https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf
Gestión de amenazas	FEMA, Consideraciones sobre la planificación: Ataques coordinados complejos https://www.fema.gov/media-library-data/1532550673102-c4846f270150682decbda99b37524ca6/Planning_Considerations-Complex_Coordinated_Terrorist_Attacks.pdf
	CISA, Guía de acción ante la embestida de vehículos https://www.cisa.gov/publication/active-assailant-security-resources
	CISA, TRIPwire: Guía de identificación de IED transportados por vehículos, vehículos estacionados https://www.fbiic.gov/public/2008/oct/DHSVehicleBorneIEDIdentificationGuideParkedVehicles.pdf
	Oficina del Director de Inteligencia Nacional (DNI, por sus siglas en inglés): Herramientas de primeros auxilios https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox
	CISA, Guía de seguridad y resiliencia https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience
	DHS, Manual de referencia para mitigar posibles atentados terroristas contra edificios https://www.dhs.gov/science-and-technology/bips-06fema-426-reference-manual-mitigate-potential-terrorist-attacks-against
	FEMA, Gestión de riesgos: Una guía para mitigar posibles atentados terroristas contra edificios https://www.fema.gov/media-library-data/20130726-1524-20490-7395/fema452_01_05.pdf

CATEGORÍA	RECURSO

Capítulo 6: Consideraciones sobre la seguridad en guarderías y escuelas

Recursos generales	DHS, SchoolSafety.gov https://www.schoolsafety.gov/
	Departamento de Educación (DoED, por sus siglas en inglés), Preparación y gestión de emergencias para escuelas (REMS) https://rems.ed.gov/AboutUs.aspx
	SchoolSafety.gov, Herramienta de preparación para la seguridad https://www.schoolsafety.gov/safety-readiness-tool#no-back
	REMS, Desarrollo de planes de operación en emergencias (EOP) K-12 101 https://rems.ed.gov/trainings/CourseK12EOP.aspx
	REMS, Guía para desarrollar planes de operación en emergencias escolares de alta calidad https://rems.ed.gov/docs/REMS_K-12_Guide_508.pdf
	PSA de la CISA https://www.cisa.gov/protective-security-advisors central@cisa.dhs.gov
Seguridad física	DHS, Encuesta de seguridad escolar https://doe.sd.gov/schoolsafety/documents/Security-Survey-508.pdf
	REMS, Capacitación en directo y aplicación Site Assess https://rems.ed.gov/SITEASSESS.aspx?AspxAutoDetectCookieSupport=1
	Alianza de Socios para Escuelas más Seguras (PASS, por sus siglas en inglés): Pautas de seguridad y protección para escuelas K-12 https://passk12.org/wp-content/uploads/2019/01/PASS-K-12-School-Safety-Security-Guidelines-v4.pdf
Clima escolar	DoED, Principios rectores: Una guía de recursos para mejorar el clima escolar y la disciplina https://www2.ed.gov/policy/gen/guid/school-discipline/guiding-principles.pdf
	Guía de acción para el clima escolar https://safesupportivelearning.ed.gov/scirp/action-guides
	USSS, Análisis de la violencia escolar dirigida https://www.secretservice.gov/data/protection/ntac/Protecting_Americas_Schools.pdf
	Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) StopBullying.gov https://www.stopbullying.gov/resources/facts#stats
	USSS, Mejora de la seguridad escolar con el modelo de evaluación de amenazas https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf
	Universidad de Maryland, Evaluación de la Salud y el Rendimiento Escolar (SHAPE, por sus siglas en inglés), Perfil de salud mental escolar https://www.theshapesystem.com/wp-content/uploads/2019/10/SMH_School-version-10.2.pdf
	HHS, Paquete de evaluación para la prevención del acoso escolar https://mchb.hrsa.gov/
Capacitación	REMS, Solicitud de capacitaciones en vivo https://rems.ed.gov/TA_TrainingsByRequest.aspx
	DHS, Programa de evaluación y ejercicios de seguridad nacional https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf

CATEGORÍA	RECURSO
Recursos de financiamiento	DOJ, Programa de prevención de la violencia escolar https://cops.usdoj.gov/svpp
	DOJ, Programa STOP contra la violencia escolar: soluciones tecnológicas y de evaluación de amenazas para escuelas más seguras https://bja.ojp.gov/program/stop-school-violence-program/archives
	DoED, Proyecto de respuesta de emergencia escolar a la violencia (SERV), Apoyo para la recuperación tras la violencia https://www2.ed.gov/programs/dvppserv/index.html
	DoED, Programa E-Rate: Tecnología rentable para reforzar la infraestructura de la red https://www2.ed.gov/about/inits/ed/non-public-education/other-federal-programs/fcc.html

Capítulo 7: Ciberseguridad

Higiene cibernética	CISA, Guía de recursos de ciberseguridad https://us-cert.cisa.gov/resources/smb
	CISA, Elementos cibernéticos esenciales https://www.cisa.gov/publication/cisa-cyber-essentials
	CISA, Sistema Nacional de Concienciación Cibernética (NCAS): Seguridad del sitio web https://www.us-cert.gov/ncas/tips/ST18-006
	CISA, NCAS: Precaución con los archivos adjuntos a los correos electrónicos https://www.us-cert.gov/ncas/tips/ST04-010
	CISA, Privacidad y aplicaciones para dispositivos móviles https://us-cert.cisa.gov/ncas/tips/st19-003
Seguridad en Internet	CISA, Hoja de consejos sobre la privacidad en Internet https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA, NCAS: Mantenerse seguro en las redes sociales https://www.us-cert.gov/ncas/tips/ST06-003
	CISA, Hoja de consejos sobre ciberseguridad en las redes sociales https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA, NCAS: Directrices para la publicación de información en Internet https://www.us-cert.gov/ncas/tips/ST05-013
	Alianza Nacional de Ciberseguridad, Mejores prácticas de ciberseguridad en las redes sociales https://staysafeonline.org/resource/social-media-cybersecurity-best-practices/
	CISA, NCAS: Cómo lidiar con los acosadores cibernéticos https://www.us-cert.gov/ncas/tips/ST06-005
	CISA, NCAS: Cómo evitar los ataques de ingeniería social y suplantación de identidad https://www.us-cert.gov/ncas/tips/ST04-014
Prácticas de seguridad y concienciación	CISA, Tarjeta de consejos para reconocer y prevenir la ciberdelincuencia https://www.cisa.gov/publication/stop-think-connect-toolkit
	CISA, Notificación de incidentes cibernéticos https://www.cisa.gov/reporting-cyber-incidents https://us-cert.cisa.gov/report
	CISA, Suscríbase al boletín mensual de US-CERT https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new
	CISA, Revisión de la resiliencia cibernética (CRR) https://www.us-cert.gov/resources/assessments
	CISA, Asesores de ciberseguridad (CSA) https://www.cisa.gov/csa

CATEGORÍA	RECURSO
Prácticas de seguridad y concienciación (continuación)	CISA, Observaciones: Solucionar las vulnerabilidades en sistemas accesibles a través de Internet https://www.cisa.gov/insights
	CISA, Paquete de ejercicios teóricos sobre ciberseguridad (CTEP) https://www.cisa.gov/national-cyber-exercise-and-planning-program
	DHS, Manual para salvaguardar la información de identificación personal https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information
Programas malignos y virus	CISA, Tarjeta de consejos sobre programas malignos https://www.cisa.gov/publication/stop-think-connect-toolkit
Ataques de suplantación de identidad	CISA, Tarjeta de consejos sobre la suplantación de identidad https://www.cisa.gov/publication/stop-think-connect-toolkit
Programa de chantaje	CISA, Recursos contra los ataques con programas de chantaje US-CERT https://www.us-cert.gov/Ransomware
	CISA, NCAS: Consejos de seguridad para la protección contra ataques con programas de chantaje https://www.us-cert.gov/ncas/tips/ST19-001
Desfiguración del sitio web	CISA, Perspectivas cibernéticas: Mitigar la manipulación de la infraestructura DNS https://www.cisa.gov/insights
	CISA, Observaciones cibernéticas: Solucionar las vulnerabilidades en sistemas accesibles a través de Internet https://www.cisa.gov/insights

Apéndice 2: Lista de incidentes

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
2009			
4/7/2009	**Campamento de retiro Kkottongnae**	**Cristiano**	**Temecula, CA**
John Suchan Chong, de 69 años, un empleado de mantenimiento en un retiro católico, atacó a otros residentes con una pistola en aparente represalia por los desaires percibidos. Disparó y mató a una víctima e hirió a otras tres antes ser reducido por los testigos.			
2010			
3/20/2010	**Iglesia Church of the Living God**	**Cristiano**	**Pittsburg, CA**
John Hugo Scherzberg, de 42 años, incendió una serie de iglesias porque estaba enojado y culpaba a Dios por sus circunstancias de vida.			
2011			
6/1/2011	**Catedral de San Ambrosio**	**Cristiano**	**Des Moines, IA**
Mediante un ciberataque encubierto, los piratas informáticos robaron más de $680.000 que la diócesis recaudó para ayudar a las personas sin hogar y a las mujeres maltratadas.			
2012			
1/1/2012	**Fundación Imam Al-Khoel**	**Musulmán**	**Ciudad de Nueva York, NY**
Ray Lazier Lengend, de 40 años, también conocido como Suraj Poonai, bombardeó una serie de edificios residenciales y casas de adoración, incluido un templo hindú y una mezquita, y declaró que quería “eliminar a tantos árabes como fuera posible”. Nadie resultó herido, pero los ataques causaron importantes daños materiales.			
1/12/2012	**Congregación Beth El**	**Judío**	**Paramus, NJ**
Anthony Graziano y Aakash Dalal, ambos de 19 y 20 años en el momento de sus delitos, pasaron de cometer una serie de vandalismos antisemitas a bombardear un par de sinagogas y la casa de un rabino.			
5/12/2012	**Iglesia St. Peter’s Episcopal Church**	**Cristiano**	**Ciudad de Ellicott, MD**
Douglas Franklin Jones, de 56 años, disparó y mató a un sacerdote episcopal y a un secretario de la iglesia en una disputa sobre la despensa de alimentos de la iglesia.			

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
5/20/2012	**Iglesia New Holy Deliverance Outreach Ministry**	**Cristiano**	**Axton, VA**
Jean-Claude Bridges, de 17 años, junto con un cómplice menor de edad no identificado, incendiaron una iglesia predominantemente negra. En el juicio, admitió haber atacado a la iglesia por prejuicios raciales.			
8/5/2012	**Templo Sij de Wisconsin en Oak Creek**	**Sij**	**Oak Creek, WI**
Wade Michael Page, un veterano del ejército de 40 años vinculado a organizaciones de supremacistas blancos, disparó y mató a seis personas en un templo sij. Otras cuatro personas resultaron gravemente heridas en el ataque, entre ellas un oficial que acudió al lugar; un sacerdote murió más tarde a causa de sus heridas. El francotirador resultó herido por los disparos de los oficiales que acudieron al lugar y se suicidó.			
8/6/2012	**Sociedad Islámica de Joplin**	**Musulmán**	**Joplin, MO**
Jedediah Stout, de 32 años, fue arrestada después de incendiar una clínica de Planned Parenthood. En el juicio, se declaró culpable de varios cargos de incendio intencional y confesó haber incendiado una mezquita porque no le gusta el Islam.			
9/30/2012	**Centro Islámico del Gran Toledo**	**Musulmán**	**Perrysburg, OH**
Randolph T. Linn, un camionero de 52 años y ex infante de marina, irrumpió en una mezquita fuera de horario e incendió la sala de oración, causando más de $1 millón en daños. En el juicio, Linn confesó que había estado bebiendo mucho y que estaba alterado por la cobertura informativa sensacionalista de los ataques contra militares estadounidenses en el Medio Oriente.			
10/1/2012	**Templo Kol Ami Emanu-El**	**Judío**	**Plantation, FL**
Un grupo de piratas informáticos que se hace llamar Team System Dz se apoderó del sitio web de una sinagoga durante una festividad religiosa y lo reemplazó con mensajes antisemitas y elogios a la organización terrorista Estado Islámico.			
10/24/2012	**Iglesia World Changers Church International**	**Cristiano**	**College Park, GA**
Floyd Palmer, de 51 años, disparó y mató a un voluntario de la iglesia que dirigía un servicio de oración en una megaiglesia del área de Atlanta. Se desconoce la motivación de Palmer, pero anteriormente había sido acusado de un tiroteo en una mezquita de Baltimore y tiene antecedentes de enfermedad mental.			
12/2/2012	**Iglesia First United Presbyterian Church**	**Cristiano**	**Coudersport, PA**
Gregory Eldred, un maestro de escuela de 52 años, buscó a su exesposa y la asesinó con un disparo mientras ella tocaba el órgano durante un servicio religioso. Eldred recibió cadena perpetua; su motivación sigue bajo investigación.			

2013

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
3/31/2013	**Iglesia Hiawatha Church of God in Christ**	**Cristiano**	**Ashatabula, OH**

Reshad Riddle, de 28 años, asesinó con un disparo a su padre durante un servicio religioso de Pascua e hizo declaraciones incoherentes mientras retenía a los miembros a punta de pistola. Riddle fue reducido rápidamente por los oficiales que acudieron al lugar. Un juez declaró a Riddle "legalmente demente" y lo puso bajo custodia de un sistema de atención de salud conductual.

10/8/2013	**Iglesia católica de Spring Valley**	**Cristiano**	**Spring Valley, CA**

Eugene William Volk, de 46 años, se declaró culpable de una variedad de cargos, incluidos delitos de odio e incendio premeditado, relacionados con el incendio de una iglesia que causó más de $200.000 en daños. Volk tenía un extenso historial criminal y confesó odiar la fe católica.

2014

4/13/2014	**Centro Comunitario Judío de Kansas City**	**Judío**	**Overland Park, KS**

Frazier Glen Miller, Jr., un veterano del ejército de 73 años con un largo historial de vínculos con organizaciones racistas, disparó y mató a tres personas en un centro comunitario judío y una comunidad de jubilados.

2015

6/17/2015	**Iglesia Episcopal Metodista Africana Emanuel**	**Cristiano**	**Charleston, SC**

Dylan Roof, un supremacista blanco de 21 años, disparó y mató a nueve personas durante un servicio de oración en una iglesia tradicionalmente negra. Durante su arresto, Roof declaró que su intención era iniciar una guerra racial.

9/13/2015	**Iglesia Corinth Missionary Baptist Church**	**Cristiano**	**Bullard, TX**

Rasheed Abdul Aziz, de 40 años, ingresó a una iglesia vistiendo equipo táctico completo y armado con una pistola, declarando su intención de "matar a los infieles". El pastor era un especialista experimentado en la intervención en crisis y convenció al presunto atacante para que depusiera su actitud. Fue arrestado al día siguiente.

12/11/2015	**Sociedad Islámica del Valle de Coachella**	**Musulmán**	**Coachella, CA**

Carl James Dial, de 23 años, lanzó una bomba molotov contra una mezquita poco después del mediodía. Nadie resultó herido, pero el fuego causó grandes daños materiales. Los padres de Dial lo describieron como problemático, y los investigadores creen que el ataque fue en represalia por el tiroteo masivo de 2015 en San Bernardino.

2016

1/1/2016	**Centro Islámico de Wheaton**	**Musulmán**	**Chicago, IL**

Un pirata informático desconocido o un grupo de piratas informáticos crearon un sitio web falso para una mezquita del área de Chicago y publicaron imágenes y mensajes incendiarios para provocar una reacción violenta contra los musulmanes.

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
2/28/2016	**Iglesia St. Peter's Missionary Baptist Church**	**Cristiano**	**Dayton, OH**
Daniel Schooler, de 68 años, disparó y mató a su hermano, un reverendo, durante una disputa por una demanda. En el juicio, Schooler explicó que fue a la iglesia para discutir la disputa y le disparó a su hermano en defensa propia después de que la discusión subiera de tono. Schooler tenía un extenso historial criminal y antecedentes de trastornos mentales.			
8/13/2016	**Mezquita Al-Furqan Jame Masjid**	**Musulmán**	**Ciudad de Nueva York, NY**
Oscar Morel, de 35 años, disparó y mató a dos eruditos musulmanes cuando salían de una mezquita en Nueva York. Un juez condenó a Morel a cadena perpetua, pero los investigadores no pudieron determinar la motivación.			
9/1/2016	**Iglesia Hopewell Missionary Baptist Church**	**Cristiano**	**Greenville, MS**
Andrew McClinton, de 47 años, incendió una iglesia tradicionalmente negra en Misisipi. McClinton tenía un extenso historial criminal y los investigadores concluyeron que incendió la iglesia, de la que era miembro, para encubrir actividades ilícitas.			
9/11/2016	**Centro Islámico de Fort Pierce**	**Musulmán**	**Fort Pierce, FL**
Joseph Schreiber, de 32 años, incendió una mezquita a la que asistía Omar Mateen, autor del tiroteo masivo en la discoteca Pulse en Orlando. La mezquita fue destruida. Schreiber había publicado previamente un mensaje antiislámico en las redes sociales e hizo declaraciones islamófobas en el juicio.			
2017			
1/7/2017	**Iglesia St. Stephen Presbyterian Church**	**Cristiano**	**Fort Worth, TX**
Thomas Dale Britton, de 54 años, irrumpió en una iglesia durante la noche y pasó varias horas destrozando el edificio y provocando incendios, causando daños por valor de más de medio millón de dólares. Dejó un grafiti que intentaba implicar al ISIS, pero los investigadores no pudieron determinar el motivo.			
2/17/2017	**Iglesia de San Agustín**	**Cristiano**	**Des Moines, IA**
Ashley Eckhardt, de 31 años, atacó a un diácono con un cuchillo durante un ministerio católico con los enfermos. Los testigos describieron a Eckhardt como una persona perturbada y que "gritaba sobre el diablo". El diácono sobrevivió y un juez condenó a Eckhardt a cinco años de prisión.			
6/11/2017	**Sociedad Islámica de Tampa**	**Musulmán**	**Pomona, CA**
Shaun Urwiler, un veterano de 42 años que padece de trastorno de estrés postraumático, estrelló su camión contra varios autos y luego lo estrelló contra la entrada de una mezquita, causando alrededor de $6.000 en daños. Durante su arresto, Urwiler dijo a los agentes que quería "causar un poco de caos".			

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
8/5/2017	**Centro Islámico Dar al-Farooq (DAF)**	**Musulmán**	**Bloomington, MN**
Tres hombres: Michael McWhorter, 29; Joe Morris, 23; y Michael Hari, de 47 años, intentaron bombardear una mezquita durante las oraciones de la mañana. McWhorter y Morris se declararon culpables de múltiples delitos de odio; Hari está a la espera de juicio. Los tres hombres están vinculados a organizaciones supremacistas blancas. El atentado fue parte de una ola de delitos en varios estados y tenía la intención de expulsar a los musulmanes del país.			
9/24/2017	**Iglesia Burnette Chapel Church of Christ**	**Cristiano**	**Antioch, TN**
Emanuel Kidega Samson, de 25 años, disparó y mató a una persona en el estacionamiento de la iglesia Burnette Chapel Church of Christ en Antioch, TN. Samson entró en la iglesia y continuó con el ataque. En total, Samson mató a una persona e hirió a siete antes de que los funcionarios de orden público lo detuvieran.			
11/5/2017	**Iglesia First Baptist Church**	**Cristiano**	**Sutherland Springs, TX**
Devin Patrick Kelley, de 26 años, disparó y mató a 26 personas e hirió a 20 en la iglesia First Baptist Church en Sutherland Springs, Texas. Comenzó a disparar en el estacionamiento y luego ingresó a la iglesia para continuar con el ataque. Un vecino de la iglesia con un arma de fuego legal le disparó dos veces a Bowers y persiguió al atacante en un vehículo. El vehículo de Bowers se estrelló, momento en el que se suicidó con una pistola antes de que llegara la policía.			
2018			
10/27/2018	**Sinagoga Tree of Life**	**Judío**	**Pittsburgh, PA**
Robert Gregory Bowers, de 46 años, disparó y mató a 11 personas e hirió a otras seis, incluidos 4 funcionarios de orden público que acudieron al lugar, en la Congregación Tree of Life en Pittsburgh, Pensilvania. La policía intercambió disparos con el atacante antes de detenerlo. Bowers enfrenta numerosos cargos federales y estatales, incluido cometer un delito de odio.			
11/23/2018	**Congregación Bais Yeshuda**	**Judío**	**Los Ángeles, CA**
Mohamed Mohamed Abdi, de 32 años, utilizó un vehículo para intentar atropellar a los fieles que salían de la Congregación Bais Yeshuda en Los Ángeles, California. No se reportaron víctimas. Las autoridades rastrearon y arrestaron al agresor, quien gritó insultos antisemitas durante el ataque.			
2019			
4/1/2019	**Iglesia St. Ambrose Catholic Church**	**Cristiano**	**Brunswick, OH**
Iglesia católica de San Ambrosio en Brunswick, Ohio perdió $1.75 millones de un fondo de renovación como consecuencia de un ciberataque. Los autores del crimen se hicieron pasar por la empresa constructora para piratear el correo electrónico de la iglesia. Usaron el acceso al correo electrónico para solicitar información financiera a otro empleado.			

FECHA	NOMBRE DE LA HoW	DENOMINACIÓN	CIUDAD, ESTADO
4/4/2019	**Iglesia bautista de St. Mary/Iglesia bautista de Greater Union/Iglesia bautista de Mount Pleasant**	**Cristiano**	**Port Barre; Opelousas, LA**

Holden Matthews, de 21 años, incendió cuatro iglesias en Luisiana durante varias noches. Atacó la Iglesia bautista St. Mary en Port Barre, LA y la Iglesia bautista Greater Union y la Iglesia bautista Mount Pleasant en Opelousas, LA. Matthews compartió videos e imágenes de los ataques en Internet. Matthews enfrenta cargos estatales por cometer delitos de odio.

4/27/2019	**Sinagoga Chabad of Poway**	**Judío**	**Poway, CA**

John Timothy Earnest, de 19 años, mató a una persona e hirió a tres en un tiroteo en la sinagoga Chabad of Poway. El Departamento de Policía de San Diego detuvo a Earnest aproximadamente a dos millas de la sinagoga. El ataque ocurrió el último día de la Pascua judía.

12/29/2019	**Iglesia West Freeway Church of Christ**	**Cristiano**	**White Settlement, TX**

Keith Kinnunen, de 43 años, disparó y mató a dos personas durante un servicio religioso el domingo por la mañana en una iglesia en White Settlement, Texas. Se disfrazó para llevar a cabo el ataque. Kinnunen falleció al recibir un disparo del jefe de seguridad de la iglesia.

12/29/2019	**Congregación Netzach Yisroel**	**Judío**	**Monsey, NY**

Se acusa a Grafton Thomas, de 37 años, de atacar a varias personas con un arma blanca en una celebración de Hanukkah organizada por un rabino en Monsey, Nueva York. Se le declaró no apto para ser juzgado y actualmente se encuentra en un centro de atención mental.

U.S. Department of Homeland Security

Agencia de Ciberseguridad y Seguridad de la Infraestructura

Washington, DC 20528