SEGURIDAD FÍSICA DE INSTALACIONES GUBERNAMENTALES:

GUÍA PARA LA ELABORACIÓN DE ANÁLISIS DE RIESGOS

SEGOB
SECRETARÍA DE GOBERNACIÓN

ESTADOS UNIDOS MEXICANOS

CNS
COMISIÓN NACIONAL DE SEGURIDAD

PROTECCIÓN FEDERAL

ÍNDICE

MENSAJE DEL COMISIONADO

El Servicio de Protección Federal es la instancia de la Administración Pública encargada de la salvaguarda de nuestra infraestructura crítica. Brinda protección a personas, bienes e instalaciones esenciales para el funcionamiento del sector gubernamental. Al mismo tiempo, se ha constituido como referente en el establecimiento de esquemas de seguridad para el sector privado. Ello se debe tanto al rigor en la capacitación de sus integrantes, como a la especialización y consistencia de sus procedimientos de operación.

La publicación de esta Guía para la Elaboración de Análisis de Riesgos es un elemento más del compromiso y profesionalismo del Servicio de Protección Federal, pues establece un estándar metodológico para la elaboración de una herramienta fundamental en la seguridad física de las instalaciones gubernamentales. Instrumentos como éste no sólo refuerzan la actuación de los elementos de este Órgano y de los encargados de seguridad de las dependencias gubernamentales, sino que también consolidan el carácter profesional, orientado por estándares técnicos, de quienes tienen a su cargo el resguardo de instalaciones físicas.

El Servicio de Protección Federal lleva a cabo, de manera permanente, esfuerzos importantes en la actualización y adecuación de sus procedimientos y protocolos, así como en las posibilidades de asesorar, compartir y divulgar estos avances con quienes desempeñan funciones de protección. En la Comisión Nacional de Seguridad esto nos llena de orgullo y satisfacción, y a la vez nos compromete a mantener el estándar de calidad y mejora constante de procesos. Confiamos en que esta Guía servirá como eje para orientar los esquemas de seguridad en instalaciones públicas y para consolidar procesos de gestión de riesgos.

Lic. Renato Sales Heredia
Comisionado Nacional de Seguridad

MARCO JURÍDICO

La presente guía base para la elaboración de análisis de riesgos se sustenta en las siguientes normas que otorgan facultades al Servicio de Protección Federal.

Constitución Política de los Estados Unidos Mexicanos
Artículo 21, párrafos 8.° y 9.°

Ley General del Sistema Nacional de Seguridad Pública
Artículos 2.°, 3.° y 7.°

Ley de Seguridad Nacional
Artículo 5.°, fracción XII, Artículo 6.°, fracción II y Artículo 26.°

Ley Orgánica de la Administración Pública Federal
Artículos 14, 17, 18 y 27.

Ley de la Policía Federal
Artículo 43, fracción IV.

Reglamento del Servicio de Protección Federal
Artículo 3, párrafos 3 y 5; Artículo 12, fracciones XIII, XX, XXI; Artículo 15, fracción VIII.

Con el fin de cumplir el Reglamento del Servicio de Protección Federal se elaboró la presente Guía para la Elaboración de los Análisis de Riesgos, que servirá como metodología y normativa para los encargados de seguridad de las dependencias gubernamentales en la elaboración del documento correspondiente.

INTRODUCCIÓN

El Plan Nacional de Desarrollo 2013-2018 enmarca la propuesta "México en Paz". En ella el ciudadano presidente de la República, Enrique Peña Nieto, instó a todas las fuerzas del orden a formar un solo frente en el diseño de una Política de Seguridad Nacional, la cual a la letra dice: "Condensa una serie de objetivos e intereses estratégicos nacionales, tales como la protección de la nación mexicana frente a las amenazas y riesgos" [...] "La realidad de nuestro país precisa identificar, dimensionar y jerarquizar los efectos de los diversos factores internos y externos que, en virtud de su dinamismo, tienen el potencial para constituirse en una amenaza o riesgo para la Seguridad Nacional".

Con base en estas premisas, la Comisión Nacional de Seguridad, a través del Servicio de Protección Federal, asume la responsabilidad de ser el agente de cambio ofreciendo, entre sus servicios y en cumplimiento de sus facultades, un diseño e implementación de un estándar metodológico para la realización del análisis de riesgos, y que como resultado de este estudio sea posible obtener información útil para la toma de decisiones en materia de seguridad física.

La presente Guía Base para la Elaboración de Análisis de Riesgos es el documento eje que puede brindar, a cualquier institución gubernamental y de seguridad, una metodología clara para identificar, analizar y evaluar las amenazas y vulnerabilidades a las que están expuestas las instalaciones con el objetivo de generar información que permita la gestión integral de riesgos.

La metodología de esta guía está basada en los estándares internacionales de gestión de riesgos, buenas prácticas y los conocimientos de personal especializado en la materia para medir la exposición de los activos ante ataques terroristas, agresiones contra la infraestructura física o delitos cuyo propósito sea desestabilizar las operaciones y su continuidad.

OBJETIVO

El presente documento es una Guía para la Elaboración de Análisis de Riesgos en materia de seguridad física de instalaciones gubernamentales mediante una metodología específica y consta de las siguientes fases:

- Fase I. Identificación de activos
- Fase II. Análisis de activos y amenazas
- Fase III. Evaluación de riesgos
- Fase IV. Mitigación del riesgo

Actividades previas

Antes de proceder a la elaboración de un análisis de riesgos la instancia evaluadora deberá asegurarse de que se cubran los requisitos administrativos, operativos y legales necesarios para que los resultados cuenten con la validez adecuada.

Requerimientos

La institución que elabora el análisis de riesgos deberá contar con personal certificado por alguna dependencia o institución reconocida.

El inicio del análisis requiere integrar lo que se conoce como la célula de análisis de riesgos. Ésta la componen personal de la institución que requiere el análisis de riesgos y de la institución que lo elabora.

Desarrollo

El análisis de riesgos deberá realizarse conforme el proceso descrito en el siguiente diagrama, considerando cada una de las fases:

Fase I. Identificación de activos

Un activo es aquella persona, objeto, proceso o propiedad que en caso de sufrir daño puede desestabilizar el funcionamiento de la instalación, y dada su importancia para las organizaciones requieren de medidas especiales de prevención o protección para salvaguardarlos y evitar una consecuencia indeseable.

Los activos que se protegen en una instalación gubernamental pueden clasificarse en:

- **Personas.** Todo aquel individuo, empleado, proveedor, contratista o visitante que se encuentra dentro de la instalación
- **Procesos.** Secuencia de actividades que se realizan en la institución con el fin de lograr algún resultado específico; en éstos se incluyen productos y servicios
- **Infraestructura y equipos.** Instalaciones, equipos y objetos necesarios para cumplir con los objetivos de una institución
- **Información.** Datos, archivo, documentos, informes o sistemas de cómputo que permiten el funcionamiento de la institución

Marcha Exploratoria de Seguridad (MES)

Es el recorrido físico de la instalación por la célula de análisis con el objetivo de identificar los activos de la institución y sus posibles amenazas.

La MES consta de cuatro pasos:

a) Reunión de apertura

En esta reunión se identifican los participantes y se establecen los objetivos del recorrido y el procedimiento con el que se realizará.

b) Recorrido

Éste permite identificar y verificar los activos. Al mismo tiempo, se evalúan las condiciones en las que se encuentra su seguridad.

El recorrido de la instalación se realizará de la siguiente manera:

1. Revisión de entorno de los inmuebles
2. Revisión del perímetro
3. Revisión de las barreras físicas
4. Revisión del sistema de control de acceso
5. Revisión de pasillos y áreas de la instalación (comedor, estacionamiento, almacenes, etcétera)
6. En conjunto, el requirente y los analistas validarán los activos que fueron identificados (zonas estériles, oficinas prioritarias, helipuertos, subestaciones, plantas de emergencia, almacenes de productos, edificios, personas, etcétera)
7. Verificación de procesos y protocolos de seguridad, en caso de que existan
8. Verificación del funcionamiento de los equipos, mecanismos y dispositivos de seguridad
9. Obtención de información complementaria de hechos que hayan violentado la seguridad en las instalaciones

Como producto de este recorrido se deberá obtener la siguiente información.

1. **Identificación de activos.** Detección de aquello que debe cuidarse y protegerse
2. **Problemática de seguridad.** Condiciones o hechos capaces de vulnerar o poner en riesgo los activos
3. **Hechos de perjuicios.** Datos duros y estadísticas que intervengan en los procesos de seguridad Esta información puede apoyarse en los índices de inseguridad de la zona o con los datos de problemas de seguridad de los que se tengan antecedentes en las instalaciones
4. **Fortalezas de la seguridad.** Conocimiento a fondo de todos los sistemas de seguridad existentes, por ejemplo: una orden general de operaciones (OGO) para la protección de los activos; protocolos o procedimientos de seguridad por escrito y bien definidos; equipos y controles de seguridad existentes; barreras físicas y su estado, etcétera
5. **Experiencias de seguridad.** Cuál ha sido la experiencia y principal problemática en los sistemas de seguridad actuales

c) Entrevistas

El objetivo de las entrevistas con los diferentes actores que pudieran tener relación con la seguridad del inmueble y sus habitantes es obtener mayor información respecto a la seguridad física y la tecnología que operan en la instalación. Pudiera ser necesaria la petición complementaria de datos.

d) Reunión de cierre de la MES

El líder de la célula y el contratante dan por finalizada la MES recapitulando los activos que se protegerán y sobre los cuales se realizará el análisis y evaluación correspondiente. En este punto deberá elaborarse una lista de los activos que se protegerán y que firmarán el requirente y el líder de la célula de análisis de riesgos.

Nota: Durante esta etapa no se emiten juicios ni resultados.

Fase II. Análisis de activos y amenazas

Identificación de activos

Con la información obtenida, el personal de análisis de riesgos deberá elaborar una tabla de activos, los cuales pueden clasificarse de la siguiente manera:

1. Personas
2. Procesos
3. Infraestructura y equipos
4. Información

Ejemplo de la clasificación:

ID activo	Tipo activo	Activo
1	Personas	Funcionarios
2	Personas	Personal administrativo
3	Personas	Visitantes
4	Instalaciones	Barda perimetral
5	Equipos	Site
6	Equipos	Subestación
7	Bienes o equipo	Equipo de cómputo
8	Productos	Producto terminado
9	Información	Bases de datos
10	Materiales	Materia prima
11	Instalaciones	Cristales de fachada

Una vez que se han listado los activos, la célula de análisis de riesgos deberá identificar todas las amenazas a las que puede estar expuesto el activo.

Identificación de amenazas

Las amenazas, por su origen, se clasifican en tres tipos:

a) Amenazas naturales

Aquellas generadas por fenómenos naturales y, por tanto, ajenos a la voluntad humana.

- Geológicas
- Hidrometeorológicas
- Biológicas

b) Amenazas sociales

Conductas antisociales o antijurídicas que implican una negación total del sistema de normas y leyes; sus consecuencias afectan la vida, los bienes y el ambiente; por ejemplo:

- Ataque
- Asalto
- Sabotaje
- Destrucción
- Intrusión
- Pérdida o robo
- Secuestro
- Colusión
- Extorsión
- Huelga
- Etcétera

c) Amenazas imprevistas o por accidentes

Éstas se derivan de las condiciones anormales de los sistemas, procesos o planes; se incluyen accidentes, procedimientos peligrosos, fallas en la instalación que pueden causar muerte, lesiones, daños, enfermedades u otros impactos sobre la salud; pérdida de medios de sustento y de servicios; afectaciones sociales, económicas y ambientales.

- Incendios
- Explosiones
- Accidentes
- Colapso
- Falla
- Etcétera

Notas:

a) Para los fines de esta guía, los análisis de riesgos de seguridad física en instalaciones gubernamentales sólo se tomarán en consideración las amenazas de tipo social y que estén relacionadas con la operación de la instalación evaluada. Con referencia a las amenazas consideradas dentro del rubro de protección civil, se deberá tener en consideración lo estipulado en la ley correspondiente para coadyuvar y deslindar responsabilidades

b) Respecto a la protección de la información de las instituciones, el análisis de riesgos no incluirá las amenazas ni los sistemas de protección a este activo. Esto debido a que cada dependencia cuenta con expertos en seguridad de la información y con sus normas y políticas de seguridad informática

Para cada activo se debe elaborar una tabla con las amenazas a las que puede estar expuesto. Esto se podrá determinar con base en las experiencias del pasado y con el apoyo de los índices de criminalidad de la zona en la que se ubican los inmuebles.

A continuación se muestra un ejemplo de algunas de las principales amenazas a las que están expuestos los activos.

Ejemplo de la tabla de amenazas

Id activo	Tipo activo	Activo	Amenazas
1	Personas	Servidores públicos o visitantes	Secuestro
			Agresiones
			Atentado
			Robo
			Espionaje
			Colusión
			Fraude
			Evasión
			Asalto
2	Instalaciones	Estacionamiento edificio sede	Intrusión de personas
			Introducción de objetos prohibidos
			Extracción de bienes
		Edificio sede	Vandalismo
			Daño a cristales
			Amenaza de bomba
		Subestación eléctrica	Robo
			Daño
			Sabotaje
3	Equipo	Site de cómputo	Atentado
			Sabotaje
			Robo
			Daño
		Reactor	Vandalismo
			Bloqueo por manifestantes
			Falla eléctrica
			Falla de suministro de agua
5	Procesos	Atención a público, control de	Falla eléctrica
			Bloqueo a la salida
		accesos de visitantes y empleados	Bloqueo de accesos
			Daño a equipo e instalaciones
			Atentado terrorista

Fase III. Evaluación de riesgos

La operación de una instalación gubernamental implica riesgos; es decir, la posibilidad de que los activos sean amenazados. Por ello, es necesario evaluar la probabilidad de que esto ocurra y los efectos que tendría en el funcionamiento de la operación en las instalaciones. Mediante la evaluación se podrán definir las prioridades de protección para los activos.

El analista de riesgos deberá describir para cada activo las posibles amenazas **(A)**, sus vulnerabilidades **(V)** y su impacto **(I)**. Podrá hacerlo mediante las siguientes tablas de valoración:

Tablas de evaluación

a) Amenaza (A)

Se obtiene de la cantidad de veces que el activo se ha visto expuesto a una amenaza o de qué tan probable es que esto suceda. Esta información se obtiene del histórico de eventos o la experiencia del analista de riesgos.

Valor	Nivel	Definición de criterio
1	Nunca	Nunca
2	Muy bajo	Muy rara vez
3	Bajo	Algunas veces
4	Alto	Varias veces
5	Muy alto	Muy seguido

b) Vulnerabilidad (V)

Se obtiene evaluando qué tan cuidado está el activo o que tan accesible resulta para los posibles perpetradores.

Valor	Nivel	Definición de Criterio
1	Muy difícil	Medidas de seguridad suficientes y eficaces. Inaccesible para el agresor.
2	Difícil	Medidas de seguridad satisfactorias. De difícil acceso para los agresores.
3	Moderado	Medidas de seguridad mínimas. Accesible con algo de seguridad.
4	Fácil	Medidas de seguridad mínimas y fallan los controles. Accesible con seguridad deficiente.
5	Muy fácil	No existen medidas. Accesible y sin seguridad.

c) Impacto (I)

Determina la gravedad del daño o hurto de los activos con base en criterios de evaluación definidos por el analista y el requirente.

Valor	Nivel	Definición de criterio
1	Insignificante	Pérdida de confianza en la institución.
2	Leve	Daño a la infraestructura de la instalación.
3	Grave	Interrupción del funcionamiento de la instalación.
4	Crítico	Daño a la imagen del país, daños, ambientales, lesiones graves, etcétera.
5	Catastrófico	Pérdida de vidas, peligro de salud, riesgos de seguridad nacional

Nota: Se pueden crear o utilizar tablas ya definidas por otras metodologías, como Carver, Hazop, etcétera, y se determinará la criticidad del riesgo de acuerdo con el resultado general de cada tabla de impacto.

Evaluación del riesgo

La evaluación del riesgo se obtiene al multiplicar los valores: amenaza (A), vulnerabilidad (V) e impacto (I).

$$ER = A \times V \times I$$

#	Tipo de activo	Riesgo	Amenaza (A)	Vulnerabilidad (V)	Impacto (I)	ER (A)(V)(I)
1	Personas	Funcionarios-Secuestro	2	2	5	20
2	Personas	Personal-Robo	4	4	3	48
3	Equipo	Servidor-Daños	4	3	5	60
4	Equipo	Subestación–Sabotaje	2	4	4	32
5	Instalación	Bloqueo entrada	5	4	3	60
6	Instalación	Amenaza de bomba	5	2	5	50

Nivel de aceptabilidad

La definición del nivel de aceptabilidad del riesgo de cada activo requiere comparar el resultado total del producto de ER = A × V × I con la tabla siguiente:

La siguiente tabla permite obtener el nivel de aceptabilidad:

Valores	Nivel de aceptabilidad	Prioridad de intervención
De 51 a 125	Inadmisible	Atención inmediata
De 26 a 50	Inaceptable	Atención a corto plazo
De 6 a 25	Tolerable	Atención a mediano plazo
De 1 a 5	Aceptable	Mejora continua

El resultado quedaría como sigue:

#	Tipo de activo	Riesgo	Amenaza (A)	Vulnerabilidad (V)	Impacto (I)	ER (A)(V)(I)	Nivel
1	Personas	Funcionarios-Secuestro	2	2	5	20	Tolerable
2	Personas	Personal-Robo	4	4	3	48	Inaceptable
3	Equipo	Servidor-Daños	4	3	5	60	Inadmisible
4	Equipo	Subestación-Sabotaje	2	4	4	32	Inaceptable
5	Instalación	Bloqueo entrada	5	4	3	60	Inadmisible
6	Instalación	Amenaza de bomba	5	2	5	50	Inaceptable

Esto permite definir la prioridad de intervención en la protección de un activo de acuerdo con sus amenazas y vulnerabilidades, así como el tipo de controles que permitirán la mitigación del escenario.

A continuación se detalla la descripción de los niveles de aceptabilidad:

Nivel	Descripción
Aceptable	• La seguridad es adecuada. • Cuentan con los equipos para operar; son adecuados, suficientes y redundantes. • Cumple con un programa de mantenimiento predictivo y existe un programa de renovación tecnológica. • Lo protocolos se aplican correctamente; se actualizan conforme a nuevas amenazas y se realizan simulacros. • La probabilidad de materializarse una amenaza es muy baja.
Tolerable	• La seguridad es adecuada. • Cuenta con los equipos para operar; son adecuados y suficientes. • Cumple con un programa de mantenimiento. • Los protocolos se aplican correctamente. • La probabilidad de materializarse una amenaza es baja.
Inaceptable	• La seguridad no es la adecuada. • Cuenta con los controles para operar, pero éstos no cumplen con la cantidad ni calidad de equipo requerido; su estado no es óptimo. • Los protocolos de operación son insuficientes y no están por escrito. • La probabilidad de daño es alta.
Inadmisible	• La seguridad está en riesgo. • Cuenta con los controles para operar, pero éstos no cumplen con la cantidad ni calidad de equipo suficiente; su estado no es óptimo. • No hay protocolos de operación por escrito. • La probabilidad de daño es muy alta.

Prioridad de intervención

Después de la valoración de los riesgos, la prioridad de intervención se obtiene del valor total del producto de (A)(V)(I), en donde los riesgos se ordenan de forma ascendente tomando en cuenta el resultado.

#	Activo	Riesgo	Amenaza (A)	Vulnerabilidad (V)	Impacto (I)	ER	Nivel
3	Equipo	Servidor-Daños	4	3	5	60	Inadmisible
5	Instalación	Bloqueo entrada	5	4	3	60	Inadmisible
6	Instalación	Amenaza de bomba	5	2	5	50	Inaceptable
2	Personas	Personal-Robo	4	4	3	48	Inaceptable
4	Equipo	Subestación-Sabotaje	2	4	4	32	Inaceptable
1	Personas	Funcionarios-Secuestro	2	2	5	20	Tolerable

En el documento de análisis de riesgos se debe presentar de manera clara, específica y objetiva la propuesta de solución a la problemática de seguridad que se ha detectado. A esto se le conoce como mitigación de riesgos, y debe establecerse entre los integrantes de la célula, el requirente y los especialistas en seguridad encargados de proteger los activos.

Fase IV. Mitigación del riesgo

El personal de análisis de riesgos y los especialistas en seguridad deben diseñar un sistema integral de seguridad para proteger los activos y así disminuir los riesgos detectados. Este sistema deberá establecer acciones de disuasión, prevención, detección, retraso, reacción y coordinación; en él se deben incluir:

- ✓ **Estructurales o físicos.** Barreras, diseños, mallas, ventanillas, protecciones, etcétera
- ✓ **Tecnológicos.** Software especializado, circuito cerrado de TV, rayos X en accesos, accesos automatizados, control de paquetes, etcétera

- ✓ **Procesos.** Programa integral de seguridad, políticas de seguridad, protocolos, procedimientos, consignas, capacitación, etcétera
- ✓ **Personas.** Personal de seguridad, monitoristas, caninos, etcétera

Estructurales o físicos

Una serie de condiciones físicas que deben cumplir los inmuebles para funcionar de manera segura; es decir, es necesario que existan barreras físicas para delimitar, retardar, disuadir y proteger las instalaciones.

Las barreras perimetrales ofrecen cierto grado de disuasión física, psicológica y legal para los intrusos.

Propósitos de la barrera perimetral:

- Delinear los límites
- Encaminar a las visitas hacia los puntos legales de ingreso
- Disuadir y demorar a los intrusos ilegales

La emisión de criterios de funcionalidad de las barreras físicas existentes demanda determinar si cumplen con el cometido para el que fueron instaladas, considerando que son fortalezas complementarias para la delimitación y protección perimetral, controlar accesos, resguardo de áreas internas, bloquear físicamente y retardar la entrada de personas no autorizadas, etcétera.

Las barreras físicas para la seguridad de los inmuebles es uno de los elementos fundamentales en la evaluación de los riesgos y las vulnerabilidades. En todo momento es imperativo considerar la existencia de normas oficiales que se deben cumplir para garantizar el buen funcionamiento de las barreras físicas instaladas.

Dentro de las barreras más comunes se tienen:

- Tendido de alambre de púas
- Cercas simples
- Cercas para uso duro
- Muros o paredes
- Muros con alambre de púas
- Muros con remate de concertina
- Etcétera

Tecnológicas

Las medidas de seguridad con apoyo tecnológico son todas aquellas dotadas de dispositivos y sistemas que coadyuvan en la detección, protección, vigilancia, evaluación y reacción; por tanto, tienen como meta apoyar las funciones de los elementos de seguridad. En ningún caso un artefacto sustituye a las personas.

Los equipos tecnológicos de los sistemas de seguridad deberán cumplir las normativas aplicables, nacionales e internacionales. También es altamente recomendable centralizar la información generada y que los equipos utilicen una plataforma de gestión, condición que permite el intercambio de datos entre todos los equipos utilizados.

Los sistemas que deberán interactuar por medio de una plataforma de gestión pueden ser, entre otros:

- Sistema de videovigilancia
- Sistema de sensores de movimiento
- Sistema automatizado de cierre de puertas
- Sensores de alertamiento
- Control de accesos automatizado por medio de equipos biométricos
- Inspección no intrusiva (arcos detectores de metales) y detección (túneles de rayos X)
- Plataformas de gestión
- Otros sistemas

Procesos

Éstos brindan pautas escritas básicas empleadas para garantizar la eficacia operativa del plan integral de seguridad.

- Definen las políticas de seguridad de la institución
- Establecen la guía para el manejo de la seguridad
- Resuelven conflictos o incidentes de seguridad
- Garantizan la seguridad de las instalaciones

Las políticas y los procedimientos son la primera medida de seguridad de un sistema de protección física efectivo; brindan la orientación necesaria para realizar los operativos de los elementos de seguridad, desplegar la tecnología de seguridad y evaluar la eficacia general de las medidas de seguridad.

Una vez que se formulan las políticas y los procedimientos, éstos deben probarse y revisarse en forma continua. Esta revisión brinda a los responsables de la seguridad la capacidad para identificar problemas antes de emprender una acción y además permite la práctica y el conocimiento de los procedimientos.

Las políticas serán cumplidas al establecer los procedimientos correspondientes para detectar y prever cualquier riesgo; un procedimiento menciona una serie de tareas, pasos y actividades que permiten cumplir con una meta o consigna.

Cada instalación requiere de sus procedimientos específicos; sin embargo, existen varios que pueden estandarizarse; por ejemplo, los controles en:

- Acceso peatonal
- Acceso de paquetes
- Revisión de pertenencias
- Ingreso de equipo de cómputo
- Ingreso de paquetes
- Acceso vehicular
- Acceso a áreas restringidas
- Revisión de áreas controladas
- Vigilancia de helipuertos
- Vigilancia de subestaciones y plantas de energía
- Etcétera

Estos procedimientos pueden considerarse estandarizados y es posible replicarlos en cualquier instalación.*

Otro de los elementos fundamentales para garantizar la efectividad del personal de seguridad en una instalación son los protocolos sistemáticos de operación. Éstos incluyen las acciones que en necesario seguir ante determinados acontecimientos, como:

- Amenaza de bomba
- Manifestación
- Bloqueo de accesos o salidas
- Agresión a personal o funcionarios
- Robo
- Sismo
- Incendio
- Terrorismo
- Secuestro
- Toma de rehén o rehenes
- Etcétera

* Se recomienda consultar el Manual de Procedimientos Estandarizados del Servicio de Protección Federal de la CNS.

Existen también procedimientos complementarios y de apoyo para la seguridad, los cuales dependen del tipo de instalaciones con las que se cuenta; por ejemplo, se tienen los de:

- Operación de barreras perimetrales, puentes o puertas especiales
- Iluminación
- Sistemas de detección de intrusos
- Videovigilancia
- Control de cerrojos y llaves
- Filtros o esclusas para control del ingreso
- Custodia y ubicación de activos protegidos
- Etcétera

Personas

La respuesta de los elementos de seguridad depende de que se cuente con los planes tácticos adecuados, el trabajo en equipo, el conocimiento de los procedimientos y su capacitación. Los especialistas en análisis de riesgos y de seguridad deberán, de manera constante, comprobar el funcionamiento de los planes de respuesta del personal de seguridad. Para verificar tales planes se recomienda realizar simulacros en los que se observe de manera especial el conocimiento y la coordinación de los elementos de seguridad.

El despliegue y actuación del personal de seguridad siempre deben ser resultado del estudio y análisis de riesgos. Esto permitirá definir de manera precisa las funciones y consignas de los integrantes del cuerpo de seguridad de la institución, además de que la vigilancia y protección se realice acorde con los activos que deben protegerse.

Los principales objetivos de los elementos de seguridad en la protección perimetral de un inmueble son disuasión, prevención, detección, evaluación, demora y reacción.

Para que el plan integral de seguridad sea eficaz es fundamental que cada elemento funcione como es debido. Por tanto, se recomienda que en seguridad perimetral se actúe de la siguiente manera:

1. Elemento en sitio debidamente equipado (disuasión)
2. Notificar un evento (detección y evaluación)
3. Desacelerar el avance del adversario (demora)
4. Lo cual permite que las fuerzas de seguridad tengan tiempo para interceptar, detener o neutralizar al adversario (reacción)

Los criterios para la designación del personal de seguridad quedarán establecidos por:

- La identificación de los riesgos
- Los puntos estratégicos para el control del riesgo
- La cantidad de equipo electrónico que apoye la identificación de los posibles riesgos
- La cantidad objetiva de personal para controlar el riesgo
- La capacidad operativa y tiempo de reacción

Plataforma de gestión de la seguridad

En cualquier sistema de seguridad dotado de dispositivos electrónicos siempre será recomendable que cuente con el software adecuado para administrar de manera eficiente la interacción de todos los elementos involucrados en el sistema de seguridad. Una plataforma de seguridad deberá contar con la capacidad para crear cercas virtuales y el establecimiento de horarios de control, lo que permite concentrar la vigilancia en puntos y objetos específicos aprovechando mejor los recursos y disminuyendo los espacios de almacenamiento del equipo electrónico.

Plan integral de seguridad

Para garantizar la mejor operación de un sistema de seguridad es necesario:

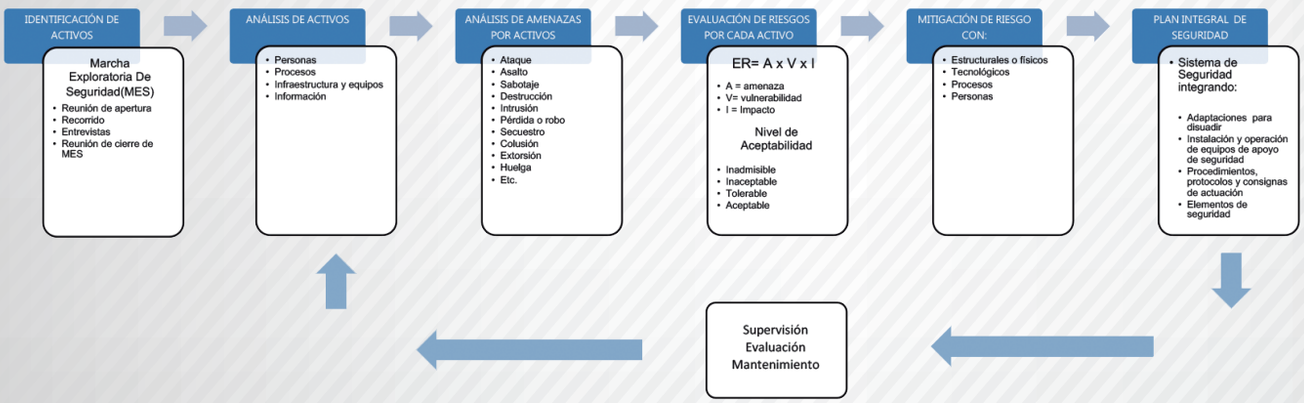
1. Identificar y conocer los activos que se protegerán
2. Conocer las posibles amenazas a las que están expuestos los activos
3. Analizar qué tan vulnerables son los activos
4. Evaluar el riesgo
5. Definir la prioridad de intervención en el cuidado de los activos
6. Diseñar los mecanismos de seguridad y protección incluyendo:
   - ✓ Las barreras físicas, modificaciones y adaptaciones para disuadir e impedir el paso de intrusos
   - ✓ La instalación y operación de equipo electrónico de apoyo para la seguridad y de ser posible una plataforma de gestión de la seguridad
   - ✓ Los procedimientos y protocolos bajo los cuales deben actuar los elementos de seguridad para garantizar la protección del inmueble y las personas. En este rubro se debe incluir la orden diaria de operaciones en la que se indica qué se debe hacer en cada punto de control de seguridad
   - ✓ El número de elementos de seguridad necesarios para cumplir la orden diaria de operaciones y la supervisión del cumplimiento de todos los procedimientos

Todo esto se obtiene a partir del análisis de riesgos y se construye al analizar sus resultados. Cuando todo ello se puede coordinar y cada elemento de seguridad conoce sus funciones y qué hacer ante eventualidades, se dice que se cuenta con un plan integral de seguridad. Este plan en una institución debe ser el medio ideal para proporcionar la mejor protección a los activos.

Existen acciones impredecibles o hechos no considerados, pero mediante coordinación, capacitación permanente y revisiones constantes podrán mitigarse mejor que si no se cuenta con un plan específico.

A continuación se presenta el "Diagrama General de Análisis de Riesgos" con todos los términos antes descritos, incluyendo la supervisión, evaluación y mantenimiento de dicho sistema.

DIAGRAMA GENERAL DE ANÁLISIS DE RIESGO



GLOSARIO DE TÉRMINOS

Activos
Es aquella persona, objeto, proceso o propiedad que en caso de sufrir daño puede desestabilizar el funcionamiento de la instalación, y dada su importancia para las organizaciones requieren de medidas especiales de prevención o protección para salvaguardarlos y evitar una consecuencia indeseable.

Analista de riesgos
Persona certificada en análisis y gestión de riesgos.

Amenaza
Probabilidad de ocurrencia o presencia de un riesgo que cause daño a un sistema; se entiende como daño una forma de destrucción.

Amenazas naturales
Aquellas generadas por fenómenos naturales y, por tanto, ajenos a la voluntad humana.

Amenazas sociales
Conductas antisociales o antijurídicas que implican una negación total del sistema de normas y leyes; sus consecuencias afectan la vida, los bienes y el ambiente.

Amenazas imprevistas o por accidentes
Aquellas derivadas de las condiciones anormales de los sistemas, procesos o en los planes; se incluyen accidentes, procedimientos peligrosos, fallas en la instalación que pueden causar muerte, lesiones, daños, enfermedades u otros impactos sobre la salud; pérdida de medios de sustento y de servicios, afectaciones sociales, económicas y ambientales.

Análisis de riesgos
Es el estudio de las causas, las fuentes de riesgo, las consecuencias y la probabilidad de que éstas ocurran.

Célula de análisis de riesgo
Equipo multidisciplinario y especializado en la identificación de riesgos, amenazas y vulnerabilidades que subsisten en torno a los activos de una instalación, y que cuenta con la capacidad técnica para emitir recomendaciones destinadas a mitigar dichos factores de riesgo.

Consigna
Orden o instrucción que se le da a un subordinado.

Perjuicio
Detrimento que una amenaza causa a un activo.

Factor de exposición (FE)
Grado en que un activo está sujeto a un evento o suceso en un periodo o lugar determinado.

Guía base
Instrumento técnico que contiene las bases metodológicas para la elaboración de los análisis de riesgos.

Impacto
Tipo y nivel de los efectos adversos causados por la ocurrencia de uno o varios riesgos, con resultados medibles para la organización; pueden provocar pérdidas y afectaciones en los activos o alterar la continuidad de las operaciones.

Instalaciones
Los inmuebles de las dependencias y entidades de la administración pública federal.

MES
Siglas de marcha exploratoria de seguridad. Es el recorrido de inspección visual y física de las condiciones del sistema integral de seguridad de la instalación y su correlación con su gestión de riesgos.

Orden general de operaciones
Orden escrita en la cual se establecen las consignas generales y específicas, y las responsabilidades del personal de seguridad, así como las estrategias de comunicación y coordinación en caso de eventos no deseados.

Personal de seguridad
Personas encargadas de la seguridad, custodia, protección y vigilancia de las instalaciones y activos de las dependencias y entidades de la administración pública federal, sean integrantes de empresas privadas de seguridad, de instituciones de seguridad pública o personal adscrito a la institución en la que prestan sus servicios.

Plan integral de seguridad
Serie de componentes diseñados para funcionar en conjunto y lograr estrategias para proteger las instalaciones. Incorpora a las personas, las tecnologías, políticas y los procedimientos para la protección contra amenazas latentes.

Procedimiento
Serie puntual de tareas, pasos y procesos necesarios para lograr un cometido de seguridad; manera en que la organización opera sus políticas.

Protocolo sistemático de operación (PSO)
Conjunto de reglas estandarizadas que permiten establecer mecanismos y formas de actuación para prevenir y enfrentar una emergencia.

Requerimiento de datos
Petición de la información necesaria a la organización solicitante para cumplir con la evaluación de los componentes funcionales de la institución.

Riesgo
Efecto de la incertidumbre sobre los personas, objetos u objetivos. Puede ser negativo, lo que será un siniestro, o positivo, lo que será un suceso.

Riesgo aceptable
Es aquel que se asume, en virtud de que su materialización no constituye un impacto importante para los activos; por lo general es inherente a la operación.

Riesgo inaceptable
Es aquel que requiere de mitigación a corto plazo, ya que puede afectar toda la operación, la continuidad de la operación bajo esta condición; requiere de la autorización de las autoridades de la institución.

Riesgo inadmisible
Los riesgos que alcanzan la calificación de inadmisibles tienen la capacidad de desestabilizar el sistema y su atención debe ser inmediata; por tanto, la responsabilidad de la continuidad de la operación bajo este nivel de riesgo sólo puede asumirla la más alta autoridad.

Riesgo tolerable
El riesgo determinado dentro de este tipo de clasificación indica que la operación no requiere suspenderse; sin embargo, debe atenderse a tiempo con acciones de mejora con el fin de evitar complicaciones.

Seguridad física
Conjunto de acciones destinadas a la protección física de los activos que se encuentran en una instalación.

Vulnerabilidad
Debilidad de los activos o de las medidas de seguridad que pueden ser aprovechadas o superadas por una amenaza para ocasionar un daño.

SERVICIO DE PROTECCIÓN FEDERAL