



Ensayo de Grado

**PRINCIPALES VULNERABILIDADES, AMENAZAS Y RIESGOS EN
SEGURIDAD FÍSICA, DE ALGUNAS INSTALACIONES DE EDUCACIÓN
SUPERIOR EN LA CIUDAD DE BOGOTÁ**

**Presentado por:
SERGIO GUACANEME MEDINA¹**

**Presentado a:
Coronel ra. Jorge Isaza, MBA-PhD
Docente Asignatura Seminario de Investigación**

**Tutor Temático
Dr. Daniel Jiménez**

**FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y
SEGURIDAD**

**Programa DE ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD
BOGOTA D.C.
2023**

¹ Profesional en Relaciones Internacionales y Estudios Políticos, Actualmente Analista de Riesgos e Investigaciones en Colvisseg Ltda.

Resumen

La seguridad física en instalaciones de educación superior es una labor ardua, dada por la complejidad, de resguardar personas y activos de la gran variedad de amenazas, internas y externas. Entonces surge la pregunta, ¿Cómo podemos identificar los riesgos que pueden afectar las personas y activos?, la respuesta resulta a partir del análisis y recolección de información proveniente del contexto externo e interno (ISO 31000:2018), pasando por un breve recorrido de las instalaciones, que permitirá apreciar las principales vulnerabilidades a explotar por las amenazas, por consiguiente, los riesgos que pueden impactar la institución serán identificados; y en consecuencia, los diseños de seguridad física serán óptimos, respecto a la detección, retardo y respuesta, generando disuasión frente a las amenazas.

Palabras clave: riesgos, amenazas, vulnerabilidades, instalaciones de educación superior, seguridad física, iso 31000:2018, protección de activos.

Abstract

Physical security in higher education facilities is an arduous task, given the complexity, of protecting people and assets from a wide variety of internal and external threats. Then the question arises, how can we identify the risks that can affect people and assets? The answer arises from the analysis and collection of information from the external and internal context (ISO 31000:2018), going through a brief journey of the facilities, which will make it possible to appreciate the main vulnerabilities to be exploited by threats, therefore, the risks that can impact the institution will be identified; and consequently, physical security designs will be optimal, with respect to detection, delay and response, generating deterrence against threats.

Keywords: risks, threats, vulnerabilities, higher education facilities, physical security, iso 31000:2018, asset protection.

Introducción

Las instalaciones universitarias, son edificaciones complejas en la medida que estas cuentan con aforos numerosos, en ellos interactúan personas de variados rangos de edad, clases sociales y es en estos espacios, donde también se hayan activos de gran valor, especialmente en laboratorios, recintos de informática y almacenes; si a las variables anteriores agregamos, que a diferencia de una institución educativa básica, las universidades aumentan la complejidad, en la medida de que las actividades de la comunidad estudiantil se extienden durante la jornada nocturna (Fennelly, Marianna, 2014) y la carente cultura de seguridad, propician vulnerabilidades a ser explotadas. En suma, de los datos anteriores, las amenazas internas y externas (Timm, 2015. P.19) ven en las instituciones de educación superior, un objetivo viable en donde la detección, retardo y respuesta no son eficaces, debido, a la ausencia de diseños de seguridad física que promuevan la óptima disuasión de las amenazas, en consecuencia, la materialización de riesgos será constante. Es por esto, que el presente documento tendrá por fin, dar a conocer la principales vulnerabilidades y amenazas, que pueden conllevar a la ejecución de riesgos, definidos por la ISO 31000:2018 como el “efecto de incertidumbre sobre los objetivos” (p.1); pero, que para los efectos de este ensayo se entenderán como eventos que, al materializarse, pueden conllevar a un impacto en la integridad de las personas, activos, operación e imagen, pretendiendo con este, brindar un insumo para quienes gestionan o van a gestionar la seguridad de universidades.

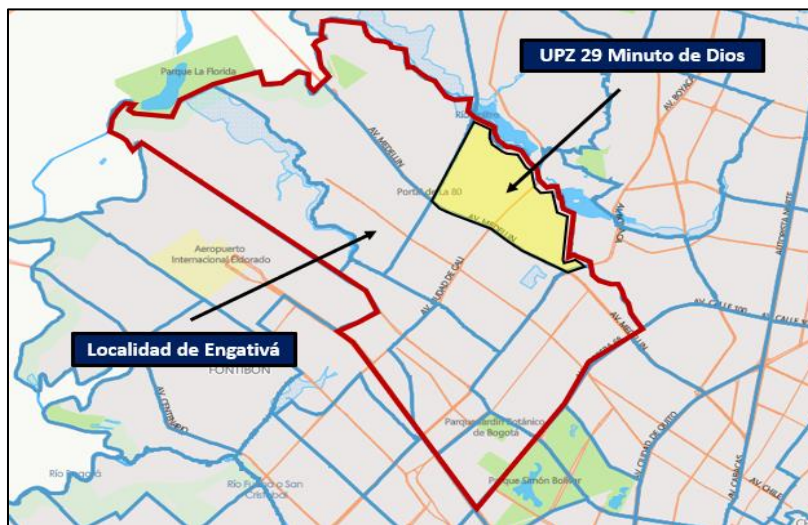
Vulnerabilidades y Amenazas en instalaciones Universitarias

Como lo indica Timm (2015) “La seguridad es la prevención de pérdidas. ¿Cómo podemos proteger, es decir, prevenir daños a los estudiantes, el personal y los visitantes?” (p.3), dicha pregunta puede ser resuelta a partir de la correcta identificación de las vulnerabilidades, entendidas como debilidades a ser explotadas (ASIS, 2003) y amenazas concernientes a una instalación de educación superior, cabe aclarar, que las amenazas son aquellos individuos o grupos de individuos que cuentan con la intención y la capacidad de materializar riesgos (ASIS, POA, 2012). El proceso de identificación de vulnerabilidad, se caracteriza por reconocer aquellas debilidades en términos de seguridad física, mediante las cuales un adversario puede explotar, y, por consiguiente, ocasionar la materialización de riesgos que conlleven a un resultado indeseado, generando afectaciones a las personas, activos, imagen y operación (NFPA 730, p. 13, 2006). En ese orden de ideas, las vulnerabilidades pueden hallarse en las diferentes áreas de la instalación, tales como: el entorno, perímetros, controles de acceso y espacios interiores (ASIS, POA, 2012), entre otras.

Entorno de la instalación

En el entorno, entendido como “el perímetro de emplazamiento y sus alrededores” (ASIS, POA, 2012. p. 76), una manera de identificar vulnerabilidades es a partir de la georreferenciación; pero, antes de explicar cómo es posible identificar vulnerabilidades en el entorno, es importante dar a conocer como esta, facilita la identificación de las principales entidades de apoyo cercanas (Policía, Bomberos, Hospitales), además que permite, medir distancias y tiempos de respuesta, frente a la consolidación de los riesgos; en ese orden de ideas, una instalación universitaria cuyas entidades de apoyo se encuentran lejanas, representa una vulnerabilidad a ser contemplada durante el análisis del contexto externo. Por

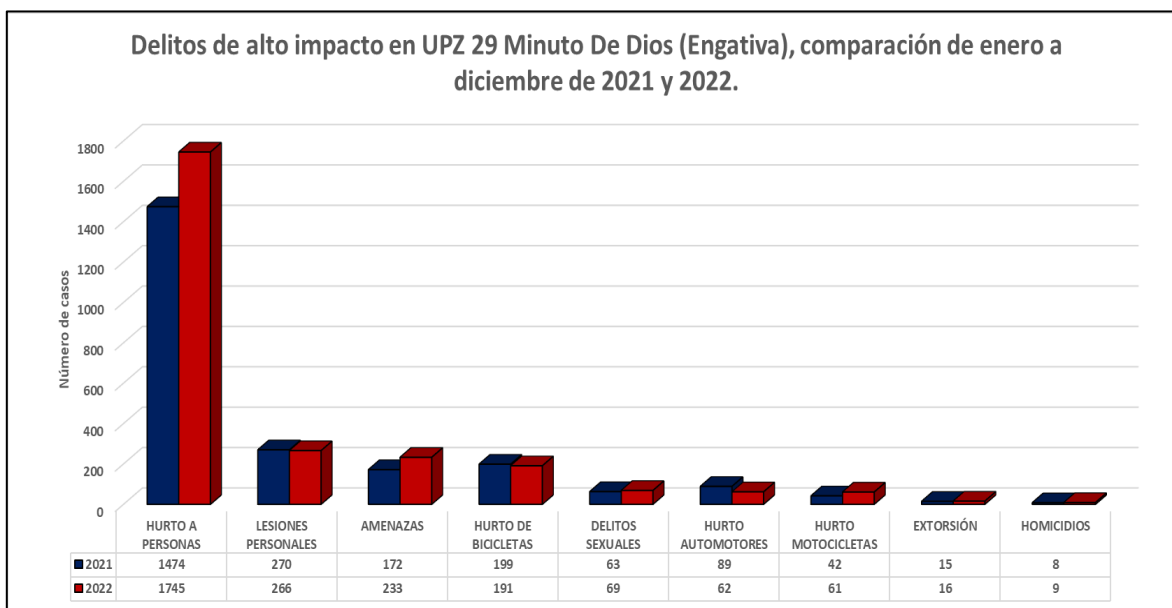
otra parte, si la edificación se localiza próxima a entidades del gobierno, puede representar una vulnerabilidad latente para la efectucción de riesgos como el terrorismo o vandalismo, dado que, las edificaciones pueden verse afectadas de manera indirecta. De la misma forma, la geolocalización permite identificar la posición espacial para el desarrollo y análisis de las estadísticas delictivas en el entorno. Las cuales son importantes, en la medida que permite estudiar de manera objetiva las dinámicas en el contexto externo a la edificación, ahora bien, en el caso de Bogotá la mejor forma de desarrollarlas, no es a partir de la localidad, en primer lugar, porque la extensión geográfica nos aleja de la objetividad de las mismas y, en segundo lugar, la identificación de riesgos asociados a las facilidades educativas, no será clara. Es por esto, que la forma óptima de analizar los delitos, es en razón de las Unidades de Planeamiento Zonal (UPZ), debido a que la extensión geográfica que está siendo analizada se reduce notablemente, como puede apreciarse en la siguiente comparación:



Fuente: Imagen extraída y modificada a partir del portal web de Mapas Bogotá, disponible en: <https://mapas.bogota.gov.co/#>

Teniendo clara la dimensión geográfica para analizar las estadísticas delictivas, se procede a extraer y reconocer las mismas, en donde se resaltarán aquellos delitos cuyo incremento puedan representar una vulnerabilidad a explotar por las amenazas del entorno.

Como se aprecia en la siguiente grafica elaborada con información sustraída de la Secretaría de Distrital de Seguridad, Convivencia y Justicia de Bogotá:



Fuente: Elaboración propia a partir de datos de la secretaria Distrital de Seguridad Convivencia y Justicia, de Bogotá.

Como se pudo valorar en el caso anterior, correspondiente a las estadísticas delictivas de la UPZ 29 el Minuto de Dios, situada en la localidad de Engativá, durante el periodo comprendido entre enero a diciembre del 2021 y 2022, se registró una tendencia al alza en los delitos de alto impacto de esa zona. En razón de ello, el análisis de las estadísticas a partir de la UPZ permite distinguir objetivamente el comportamiento de los delitos de: extorsión, homicidios, hurto en diferentes modalidades (personas, automotores, motocicletas), lesiones personales, secuestro y terrorismo. Delitos que pueden influir especialmente en el entorno de la instalación; sin embargo, el alcance puede extenderse incluso al interior de las edificaciones a resguardar.

Del mismo modo, si en el entorno durante las horas pico de ingreso y salida de estudiantes, existe la carencia en la presencia de autoridades, la probabilidad en la

materialización de riesgos que afecten a la comunidad estudiantil incrementa, especialmente el hurto calificado (CPC, art. 240) comúnmente conocido como atraco (ver imagen 3).

Imagen. 3



Fuente: Fotografía de casuística, autorizada para uso por el área de Riesgos de Colviseg Ltda.

Por lo que respecta a la proximidad a espacios públicos como parques y la poca presencia de autoridades, es preciso denotar la posibilidad de que amenazas como Grupos de Delincuencia Común Organizada (GDCO) puedan ofrecer sustancias prohibidas (alucinógenos, depresores, narcóticos, estimulantes, alucinógenos, marihuana, análogos y de prescripción) a la comunidad estudiantil, de hecho, la presencia de bares en cercanías a universidades sumado al incremento del accionar delictivo relacionada con lesiones personales, culminan con la presencia constante de las lesiones “el que cause a otro daño en el cuerpo o en la salud” (CPC, art. 111), este hecho, aunque no afecta los activos de la instalación, resultan perjudiciales al buen nombre y reputación de los centros educativos.

Continuando con la relación entre las estadísticas delictivas y el entorno, es importante considerar la proximidad con áreas como: riachuelos, quebradas, lotes baldíos y demás áreas cuya vista al público sea escasa; en estos casos, el incremento en los delitos

sexuales, sumado a la presencia de estos entornos geográficos próximos a la instalación, carentes de iluminación y fuera del campo de vista de transeúntes, catalizan la consolidación de eventos conocidos como violaciones y atracos en el entorno, hechos que notablemente afectan la integridad de la comunidad estudiantil y prestigio del centro educativo. Otro factor a ser considerado en los entornos, es el análisis del contexto externo, de hecho, si analizamos el historial de los eventos de seguridad en instalaciones que realicen la misma actividad económica, podemos conocer algunas vulnerabilidades que, de igual forma, podrían facilitar la materialización de eventos no deseados en contra de las personas y los activos al interior de complejo a custodiar.

Perímetros de la instalación

ASIS define las barreras perimetrales como “la capa de protección más exterior de un sistema de protección física, son diseñadas para dejar fuera de una zona al personal no autorizado” (POA, 2012, p.287), a su vez, una barrera perimetral permite:

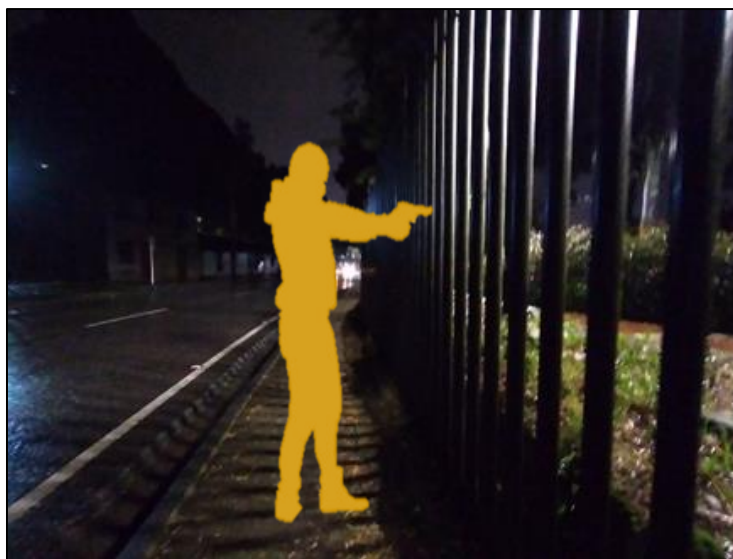
El acoplamiento de barreras vehiculares y de personas en un perímetro, en el interior y junto al sistema de detección perimetral, demora al intruso en el punto de detección, mejorando la función de evaluación. • Retrasar al intruso en el perímetro puede permitir a la fuerza de respuesta interceptar al intruso cerca del punto de la alarma. Sin la demora, el intruso probablemente habrá dejado el punto de alarma cuando la fuerza de respuesta llegue. • Hacen que sea posible proteger un lugar cuyos activos están almacenados en varios edificios de un sitio fácilmente penetrable. • Las barreras vehiculares alrededor del perímetro de un sitio (dentro de los sensores perimetrales) pueden obligar a un intruso a recorrer a pie y transportar las herramientas y armas que necesite (ASIS, POA, 2012, p. 287).

Ahora bien, los perímetros son esa barrera física entre la instalación y el entorno, de ahí que el correcto funcionamiento, facilita desincentivar al adversario de su probable objetivo. Respecto a estas áreas de la instalación, en su mayoría, las barreras perimetrales están compuestas por muros de mampostería, malla eslabonada, rejas en acero inoxidable o en aluminio, cerca viva, cercas en alambre de púas (estacas de madera situadas a 2 mts, con 4 líneas de alambre de púas), barreras naturales (ríos, montañas, acantilados etc.) o simplemente limitan con otras edificaciones; a mi modo de ver, la principal falencia en las barreras perimetrales es la falta de diseño en el sistema de protección física, en donde es posible apreciar, que los mismos en la mayoría de ocasiones no contemplan la amenaza base del diseño (Design Base Threat, DBT por sus siglas en inglés) y han sido desarrollados sin contemplar los tipos de amenazas, capacidades de estas y los modos de operación, a los cuales un complejo se encuentra expuesto (ASIS, POA, 2012, p. 27).

En segundo lugar, se haya la falta de mantenimiento preventivo y correctivo, lo que, durante el desarrollo de los estudios de seguridad, me ha permitido apreciar: aperturas en las mallas, reparaciones rudimentarias con alambre dulce y en algunos casos la vegetación próxima a la barrera perimetral, oculta los defectos de la misma como ranuras a nivel del suelo, que expone las infraestructuras físicas a la intrusión “ingreso no autorizado a una instalación” (González, 2017, p. 13) este ingreso de puede dar por escalamiento, descenso, ruptura, excavación o al mismo nivel (González, 2017). De hecho, algunas barreras perimetrales no contemplan el nivel de riesgo de la facilidad y se definen alturas y características erradas o simplemente se definen con base en criterios subjetivos de algunas personas con funciones de gestión de seguridad de las mismas.

Las barreras impiden también, que los transeúntes observen al interior de la instalación y la interacción dentro de la misma, de ahí que, si una barrera perimetral permite visualizar hacia el interior, las amenazas podrán identificar los activos y vulnerabilidades sobre ellos, que puedan ser explotadas. En un caso en particular, las barreras se encontraban conformadas por una cerca de tubos metálicos, con una separación aproximada de 10 cm que facilitaban visualizar al interior, además, el espacio entre ellos permitía ingresar un brazo entre la barrera; cabe resaltar que, del otro lado de la barrera (a no más de un metro), la comunidad estudiantil hacía uso de un sendero para desplazarse al interior del centro educativo. En consecuencia, este tramo de la barrera, resultó ser utilizado por los delincuentes para mediante intimidaciones con arma de fuego, hurtar los objetos personales de los alumnos (ver imagen 4).

Imagen 4.



Fuente: Fotografía de casuística modificada, autorizada por el área de Riesgos de Colviseg Ltda.

Además de lo anterior, la ausencia de medidas de retardo como concertinas, cercas eléctricas, alambre de púas, son coadyuvantes de la intrusión, por escalamiento (González, 2017). De igual modo, la inexistencia de herramientas electrónicas que permitan detectar de

manera oportuna intentos de intrusión, afecta directamente en los tiempos de respuesta del personal de seguridad. Al respecto Mary Lynn García (2008) opina:

El objetivo del sistema es proteger los activos de robo o sabotaje por un adversario malévolo. Para que un sistema sea eficaz en este objetivo, hay que empezar por saber que estamos bajo ataque (DETECCIÓN), a continuación, mantener al adversario lejos de los objetivos (RETARDO), permitiendo así que el tiempo de respuesta, de fuerza para interrumpir o detener el adversario (RESPUESTA) (P. 7).

Considerando que la relación entre tiempos de detección y respuesta son indirectamente proporcionales, en donde: a menor tiempo de detección mayor será el tiempo disponible de respuesta; por el contrario, si el tiempo de detección es superior, el tiempo disponible de respuesta será menor (García, 2008).

Por lo tanto, la carencia de iluminación perimetral optima, sistema de detección de intrusión y sistemas de videovigilancia con analítica de video, son vulnerabilidades que elevan la probabilidad respecto a la materialización de riesgos a través de estos espacios. Otro aspecto a valorar en los perímetros, es la necesidad de adquirir servicios de binomio canino, los cuales permiten al centro educativo, proyectar corredores seguros para la comunidad estudiantil.

Controles de Acceso

Por control de acceso, la NFPA 730 del 2006, lo define como: “El monitoreo o control del tráfico a través de puntos de acceso de un área protegida por identificación del solicitante y aprobación de entrar o salir” (p. 10).

Los controles de acceso resaltan en la medida de que, a través de estos, son ingresados y extraídos la mayoría de los activos de la instalación de forma autorizada y no autorizada, de igual forma, es a través de estos que se materializa el contrabando (ASIS, POA, 2012, p. 239); entiéndase por contrabando, “cualquier elemento que sea prohibido en un área” (ASIS, POA, 2012, p. 251). De este modo, las funciones de un control de acceso son:

Permitir la entrada y salida sólo de personas autorizadas • Detectar e impedir la entrada o salida de material de contrabando (armas, explosivos, herramientas no permitidas o activos críticos) • Entregar información al personal de seguridad para facilitar la evaluación y la respuesta (ASIS, POA, 2012, p. 239).

Al respecto, los objetivos de un control de acceso varían en función del ingreso o salida; en razón del ingreso, los objetivos son autorizar o negar el acceso de personas e impedir el ingreso de elementos no autorizados, como armas, explosivos o sustancias prohibidas, por su parte, durante la salida la extracción no autorizada de activos es la principal labor.

Ahora bien, los controles de acceso a su vez se clasifican entre peatonales y vehiculares, en relación a los primeros, la mayor dificultad es poder realizar la identificación, registro, validación, denegación o acceso, para posteriores controles a profundidad, de los alumnos, empleados, visitantes y contratistas. Conforme a los controles de acceso permiten el ingreso y salida de las instalaciones, resultan especialmente vulnerables durante las horas pico de ingreso y salida de estudiantes, de este modo, la carencia de sistemas para el control de accesos, facilita el ingreso de delincuentes bajo la fachada de estudiantes o falsos aspirantes, porque no existen herramientas tecnológicas, procedimientos y personal capacitado, sumado a esto, el esquema de seguridad durante las horas pico, resulta siendo

sobrepasado por la ausencia de personal suficiente para controlar los ingresos y salidas. Del mismo modo, si el filtro de acceso no cuenta con registro fotográfico, la capacidad disuasiva termina siendo opacada por la experticia de la delincuencia, que saca provecho del acceso fácil, para posterior consolidar eventos de inseguridad como el hurto externo (entiéndase por hurto externo, el ingreso autorizado de delincuentes que aparentan ser visitantes o aspirantes) al interior de estas; sin embargo, es importante resaltar que la implementación de registro fotográfico no garantiza la efectividad del control de acceso, cuando se realiza de manera manual y exclusivamente por un vigilante con funciones de control de ingreso. Sumado a lo anterior, la necesidad de implementar medidas tecnológicas en estos espacios, como sistemas de control de activos con tecnología RFID, que permitan detectar de manera oportuna los intentos por extraer de manera no autorizada activos de la instalación.

No menos importante, es un diseño óptimo del sistema de videovigilancia, que permita evitar puntos ciegos y, además, sirva como herramienta tecnológica que facilite tener un control de las personas de las escenas y de las actividades, que se están y se desarrollan al interior de las edificaciones, adicional, un diseño óptimo del sistema de videovigilancia facilita las labores investigativas, posterior a ejecución de riesgos. Otra vulnerabilidad a comentar, producto de mi experiencia, es que no se cuentan en algunos casos, con controles de acceso exclusivos para proveedores o contratistas que requieran realizar labores de adecuación física.

Por su parte, los controles de acceso vehicular en su mayoría cuentan con herramientas de acceso electrónicas que se enfocan en las credenciales de la persona que conduce el vehículo; pero, carecen de mecanismos de identificación de los vehículos, motocicletas y bicicletas que son ingresados. Al mismo tiempo, la precaria cobertura del

sistema de videovigilancia en estos espacios, dificulta tener un control de las personas que conducen los vehículos y acompañantes, el registro de las placas de y el estado en que son ingresados.

Espacios interiores

Por áreas interiores se entenderán todos aquellos espacios que se encuentran posterior a los perímetros, de igual forma, los espacios interiores se clasifican en zonas sin restricciones, zonas controladas y zonas restringidas, en concreto ASIS International (2012) define:

- 1) Zonas sin restricciones. Ciertas áreas de una instalación deben estar absolutamente libres para el ingreso de personas durante las horas estipuladas para su respectivo uso. El diseño de zonas sin restricciones debe estimular a las personas a llevar a cabo sus actividades y poder salir del establecimiento sin entrar en zonas restringidas o controladas. Las zonas no restringidas pueden incluir los vestíbulos, áreas de recepción, bares, algunas oficinas administrativas o para el personal y las salas de reuniones para el público.
- 2) Zonas controladas. Para ingresar a estas zonas la persona debe tener un propósito válido. Una vez admitida, puede trasladarse de un departamento a otro sin restricciones rigurosas. Las zonas controladas pueden incluir comedores del personal, oficinas de seguridad, oficinas administrativas, áreas de trabajo y zonas de carga.
- 3) Zonas restringidas. Estas son áreas sensibles limitadas sólo al personal que está asignado a ellas. Las secciones dentro de las zonas restringidas pueden requerir de un control de acceso adicional. Los departamentos y funciones ubicadas en zonas restringidas pueden incluir bóvedas, archivos sensibles, productos químicos y medicamentos, preparación de alimentos,

salas de control, áreas mecánicas, equipamientos eléctricos y/o telefónicos, laboratorios, lavanderías, suministro de elementos esterilizados y áreas de trabajo sensibles (p. 77).

En lo que respecta a las Zonas sin Restricciones, encontraremos que, en las áreas de estacionamientos de vehículos, sumado a la poca cultura de seguridad por parte de la comunidad estudiantil, facilita la materialización de riesgos en estos espacios, siendo así, común encontrar como la comunidad estudiantil descuidan elementos personales sobre las motocicletas, como cascos sin medidas de anclaje, chaquetas, activos de valor como equipos de cómputo a la vista, maletas, incluso, las mismas llaves de los vehículos. Asimismo, en los bicicleteros de la comunidad estudiantil, la presencia de bicicletas sin asegurar o espacios insuficientes ocasionando el estacionamiento en espacios no autorizados para este fin, promueven el hurto externo e interno siendo los contratistas y visitantes la principal amenaza.

Por hurto externo se entenderá como la “Situación en que un tercero ajeno a la instalación, ingresa siguiendo los protocolos de seguridad (sin violentar) a través de los controles de accesos y hurta activos de la instalación ocultos en su cuerpo o entre morrales o bolsas.” (Área de Riesgos de Colvisseg Ltda., 2022). En contraparte, el hurto interno es el cometido por empleados, alumnos, contratistas y demás personal interno.

Por otro lado, la poca cobertura del sistema de videovigilancia en áreas verdes, áreas que, además, no están cubiertas por el esquema de seguridad o cuyas rondas son escasas, facilita que algunos alumnos hagan uso de sustancias prohibidas al interior o encuentren espacios propicios para llevar a cabo actos sexuales consensuados o no consensuados.

Zonas controladas y Zonas Restringidas

En mi opinión, las zonas controladas y zonas restringidas, son las que tienen un mayor nivel de importancia, dado que, en estos espacios yacen los activos críticos o de mayor valor de la instalación; las salas de cómputo, los laboratorios y almacenes, suelen ser el foco de concentración de activos de mayor cuantía, en ese orden de ideas, las vulnerabilidades correspondientes a estos recintos suelen ser: la nula cobertura de los sistemas de detección de intrusión y sistema de videovigilancia, evaluación y visualización de la alarma, y contramedidas redundantes en retardo. Paradójicamente, algunas edificaciones contarán con robustos sistemas de detección de intrusos, videovigilancia y barreras físicas que impidan el acceso no autorizado a estos espacios; pero, resultan ineficientes las medidas anteriores, si se carece de políticas y procedimientos para el control de cerraduras, llaves y candados. De hecho, otra vulnerabilidad enfocada en factores procedimentales, es el poco control periódico en los inventarios de activos, hecho que favorece el hurto bajo la modalidad hormiga, sin generar alertas tempranas, debido al deficiente control de activos. Al respecto:

El hurto hormiga es un delito que se comete al interior de los negocios y consiste en hurtos de activos de poco valor o en cantidades que parecen insignificantes, pero que al acumularse a lo largo del tiempo representan una gran pérdida para el negocio (NS POS, 2021, Blog).

Dentro de las áreas restringidas de una instalación encontraremos, además, los servicios de utilidad (cuartos de bombas y generadores o plantas eléctricas, rack de comunicaciones, calderas, etc.), activos cuya intervención no autorizada pueden ocasionar daños, que, a su vez, conlleven a interrupciones en la operación. En efecto, si estos espacios no son cubiertos adecuadamente por el sistema de protección física puede resultar en eventos

no deseados. Desde luego, la principal amenaza asociada con este riesgo es la comunidad estudiantil y personal de trabajadores que, por inconformidades con la entidad educativa, encuentren en el Sabotaje una manera de afectar la instalación. En este punto, es necesario contemplar que el control de llaves en zonas controladas como las azoteas, es vital para impedir que estudiantes con problemas de diferente naturaleza puedan tomar acciones como el suicidio. Llegado a este punto, es importante recalcar que las amenazas, además de ser entendidas como individuos o grupos de individuos, que cuentan con capacidades e intenciones o motivaciones (García, 2008), debemos recalcar, que encuentran en las fallencias del sistema de seguridad física, oportunidades para materializar el riesgo, motivaciones de índole económico o personal, y finalmente una racionalización en donde la amenaza justifica dentro de su sistema de valores la materialización del riesgo (ACFE, S.F.).

Principales Riesgos en instalaciones universitarias

Posterior a realizar una encuesta a 6 jefes de seguridad de instalaciones universitarias de la ciudad de Bogotá, en la cual se indagó en los siguientes temas, indicando: las principales vulnerabilidades, amenazas y riesgos, que podían dar a conocer desde su experiencia en seguridad físicas de instituciones de educación superior. Por ende, se pudo apreciar en cuanto a las vulnerabilidades:

1. la falta de conciencia de la comunidad respecto al autocuidado de los activos personales en los espacios interiores, cataliza la materialización de riesgos;
2. No existen políticas definidas respecto a los procedimientos de seguridad durante el desarrollo de actividades multitudinarios y eventos académicos como diplomados, congresos y demás;

3. En varios puestos, las consignas de los servicios de seguridad, no son muy claras y carecen de especificación respecto al puesto (son muy generales);
4. Ausencia respecto a la presencia de la policía en los entornos de los centros académicos, y;
5. Falencias en los controles a profundidad, para el resguardo de los activos, activos sin medidas de anclaje al sitio, espacios sin cobertura de sistemas de videovigilancia y detección de intrusos, carencia en controles de acceso para zonas restringidas.

En relación con las principales amenazas, se destaca:

1. Personal externo a la comunidad educativa, que hace ingreso al complejo
2. Grupos de Delincuencia Común Organizada (GDCO), que aprovechan momentos de oportunidad;
3. Estudiantes de los complejos educativos, contratistas, visitantes y empleados; y,
4. habitantes de calle que recorren el entorno.

En razón de los principales riesgos a materializarse ya sea en el entorno, controles de acceso, perímetros o espacios interiores, los encuestados respondieron:

1) hurto externo; 2) hurto interno; 3) hurto calificado (atracos); 4) microtráfico en entornos y zonas sin restricción; 5) intrusión; 6) suplantación de miembros de la comunidad estudiantil; 7) fuga de información confidencial; 8) suicidio; 9) actos sexuales consensuados o no consensuados en espacios internos; 10) sabotaje; 11) extorsiones entre la comunidad estudiantil, basados en divulgación de fotografías íntimas; 12) actos vandálicos, producto de inconformidades de la comunidad estudiantil; y, 13) protesta social. Con base en lo anterior, es necesario recalcar, que algunos riesgos pueden originarse como producto de otros, dado

que, los riesgos - causa - como la intrusión, suplantación o hurto externo, pueden resultar en la materialización de otros riesgos – concausa – como el hurto, secuestro, sabotaje, lesiones personas, entre otros. En ese sentido, es importante analizar en el desarrollo del sistema de seguridad física, como a raíz de algunas vulnerabilidades, pueden dar cabida a la probable materialización de múltiples riesgos (González, S.F.).

Conclusiones

La identificación de vulnerabilidades en Universidades, es un proceso producto del análisis del contexto externo e interno, en donde posterior a un recorrido sobre las instalaciones, se puede determinar que una de las principales falencias en estos espacios, radica en el diseño de sistemas de seguridad física, sin contemplar las amenazas, estado de arte de la amenaza y activos a proteger, especialmente aquellos que tienen criticidad definida por la organización.

En adición, la falta de medidas administrativas de seguridad, poca o nula conciencia de seguridad por parte de toda la comunidad, con una relevancia mayor del personal estudiantil hacia el autocuidado; exponen a las universidades de manera significativa, a diferentes riesgos de seguridad que pueden impactar en mayor proporción el segmento reputacional de estas. Lógicamente, las carencias de herramientas electrónicas enfocadas en la detección, controles de seguridad físicos y humanos a profundidad, que permitan retardar al adversario, e insuficiencia, en la cantidad del personal de seguridad, impiden desincentivar a las amenazas.

Haciendo hincapié en las amenazas, entendidas como individuos y grupos de estos, que cuentan con la capacidad e intención de ocasionar eventos, se pudo evidenciar que estas

se dividen en amenazas “internas, externas y externos coludidos con internos” (ASIS, POA, 2012, p. 27), respecto a las internas encontramos a la comunidad estudiantil, comprendida por alumnos, docentes, personal de mantenimiento, servicios generales, personal administrativo, e incluso, miembros del esquema de seguridad. En contraparte, las amenazas externas, como su nombre lo indica provienen del entorno, tales como Grupos de Delincuencia Común Organizada (GDCO), habitantes de calle, vendedores informales y contratistas que requieran ingresar a los espacios interiores; a su vez, las externas coludidas con internas, hace referencia a los acuerdos entre las amenazas internas y externas, hacia la consolidación de riesgos.

Es así, que, dentro de las motivaciones de estos tres tipos de amenazas, podemos encontrar principalmente razones económicas ya sea por necesidad de la amenaza o por actividad económica ilegal de la misma, generando, en principio, intrusiones y seguidas a estas, suplantación, extorsiones, microtráfico y hurto en sus respectivas variables, ya sea calificado, interno o externo. En segundo lugar, hallamos aquellas razones de índole personal, relacionadas con el sentir de la amenaza, por ejemplo: disconformidad de la amenaza en contra de la institución o personal de la comunidad estudiantil; el sentir de la amenaza, pueden resultar en sabotajes, lesiones personales, actos sexuales consensuados o no consensuados, fuga de información, suicidios y demás riesgos asociados. En tercer lugar, apreciamos las motivaciones relacionadas por factores de creencia religiosa o política, que pueden conllevar a la ejecución del terrorismo, protestas sociales y vandalismo. Desde luego, las oportunidades catalizan la materialización del riesgo, oportunidades entendidas como vulnerabilidades en el diseño del sistema de seguridad física, por lo general, de carácter

procedimental, arquitectónico o tecnológico (García, 2008) en efecto, la intención debe ir acompañada de la oportunidad para la materialización del riesgo.

Finalmente, al haber analizado de manera holística las principales vulnerabilidades y amenazas, producto de lo indagado, la experiencia y el desarrollo de encuesta a seis jefes de seguridad de diferentes universidades en la ciudad de Bogotá, se puede concluir que estas instalaciones se encuentran expuestas a numerosos eventos no deseados, amenazas con intenciones y capacidades, que debido a la falta de cultura de seguridad, sumado a las vulnerabilidades de caracteres procedimental, arquitectónico y tecnológico, ocasionan, que la ejecución de riesgos en estos complejos sea latente.

En adición, los alto índices delictivos que atraviesa la ciudad de Bogotá y el fortalecimiento de Grupos de Delincuencia Común y Organiza, estructuran un escenario propicio a considerar para el desarrollo de estrategias. Por todo lo anterior, considero que la mejor estrategia será el diseño de sistemas de seguridad física que contemplen las capacidades y estado del arte de la amenaza, que estimen medidas efectivas de detección, retardo y respuesta, generando así, un nivel óptimo de disuasión frente a este tipo de actores.

Bibliografía

- ACFE. (S.F.). “Triángulo del fraude” disponible en: <https://acfe-spain.com/recursos-contrafraude/que-es-el-fraude/triangulo-del-fraude>
- ASIS, (2003). “General Security Risk Assessment”. Recuperado de: [https://webstore.ansi.org/preview-pages/ASIS/preview_ASIS+GSRA+GDL+\(2003\).pdf](https://webstore.ansi.org/preview-pages/ASIS/preview_ASIS+GSRA+GDL+(2003).pdf)
- ASIS, (2012). “Protección de activos en Seguridad Física”.
- Código Penal Colombiano. Ley 599 del 2000. “Art. 240, Art 111”. Disponible en: https://leyes.co/codigo_penal.htm
- Correa, H. (2012). “identificación y evaluación de amenazas a la seguridad de infraestructuras de transporte y distribución de electricidad”. Universidad de Zaragoza. Recuperado de: <https://www.bibliotecadigitaldebogota.gov.co/resources/2084171/>
- García, M, L, (2008). “The Design and Evaluation of Physical Protection Systems”. Elsevier
- Garnicas, S., Osorio, P., Jiménez, M., (2013). “La Seguridad en Instituciones de Educación Superior. estado actual y recomendaciones”. Recuperado de: <https://www.uv.mx/sugir/files/2013/02/La-seguridad-en-IES.pdf>
- González, T. (2017). “Los Riesgos En El Entorno De La Seguridad Privada”. Recuperado de la Universidad Militar Nueva Granada y disponible en: <https://repository.unimilitar.edu.co/bitstream/handle/10654/16650/GonzalezToscanoEdgar%20Alfonso2017.pdf?sequence=1>
- ISO 31000: 2018. “Administración / Gestión de Riesgos”. Disponible en: <https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486>
- Lawrence J. Fennelly. Marianna A. Perry. (2014). “The Handbook for School Safety and Security”. Elsevier
- NFPA 730, (2006). “Guía para Seguridad Física de Establecimientos”. Recuperado de: <https://es.scribd.com/document/338226177/NFPA-730-2006-Guia-Para-Seguridad-Fisica-en-Establecimientos#>
- NS POS. (11/05/2021). “¿Sufres de robo hormiga? ¡Conoce 6 estrategias para evitarlo!”. Disponible en: <https://nsposweb.com/blog/sufres-de-robo-hormiga-conoce-6-estrategias-para->

evitarlo#:~:text=%C2%BFQu%C3%A9%20es%20el%20robo%20hormiga,a%20un%20d%C3%A9ficit%20de%20ingresos.

Paul, Timm. (2015) “Seguridad Escolar, como construir y fortalecer un programa de seguridad escolar”. Elsevier

Pérez Toro, W. F., Benítez, L. C., Celis, D. C., Rojas Bermeo, D. P. (2016). “Universidad y seguridad. Hechos, situaciones, comunidades”. Universidad de Medellín, Estudios Políticos, 243–266. Recuperado de: <https://www.redalyc.org/articulo.oa?id=16443492013>

Portal Web, Mapas Bogotá. (S.F.). “Delitos de alto impacto por upz”. Disponible en: <https://mapas.bogota.gov.co/#>

Portal Web, secretaria Distrital de Seguridad Convivencia y Justicia. (S.F.). “Estadísticas delictivas”. Disponible en: <https://scj.gov.co/es>

UNAL, (S.F.) “Cartilla de Seguridad”. Recuperado de: <http://dfa.bogota.unal.edu.co/division-vigilancia-seguridad/docs/cartilla.pdf>