

EFICACIA DE LOS SISTEMAS ELECTRÓNICOS DE SEGURIDAD

Autor:

Luis Alfonso Mayorga Pinzón

Asesor de investigación:

John Jairo Mónoga (asesor temático)

Juan Manuel Silva (asesor metodológico)



UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES Y ESTUDIOS POLITICOS

ESPECIALIZACION EN ADMINISTRACION DE LA SEGURIDAD

2016

Índice

	Pág.
Introducción	3
1 Eficacia de los sistemas electrónicos de seguridad	4
1.1 Nociones Principales Sobre Seguridad Integral.....	4
1.1.1 Objetivos Principales De Los Sistemas Electrónicos De Seguridad.....	6
1.2 Esquemas De Un Sistema Electrónico De Seguridad.....	8
1.3 Objetivos De Un Sistema Electrónico De Seguridad	9
1.4 Sistemas Electrónicos De Seguridad: Matriz De Riesgos	12
Conclusiones	14
Referencias	15

Eficacia de los sistemas electrónicos de seguridad*

Resumen

El ejercicio académico busca mostrar que los sistemas electrónicos de seguridad, independientemente de su nivel de tecnología e innovación, en ningún momento podrán ser considerados infalibles, y por el contrario deben contar con un componente humano de altísima calidad, que conozca estas fortalezas y también sus vulnerabilidades con el fin de ser complemento el uno del otro para lograr una mejor eficacia en la protección de un bien tutelado.

Palabras clave

Riesgo, factor humano, tecnología, innovación, prevención.

Introducción

La seguridad en un mundo más globalizado implica nuevos retos y desafíos para quienes desarrollan tareas de protección en sus diferentes modalidades, haciendo que su rol tome cada día más importancia en los diferentes mercados. Pero esto a su vez, está demandando que el hombre de seguridad sea cada vez más proactivo, inteligente y capacitado para manejar los diferentes contextos internos y externos donde se desarrollan estas actividades.

Por esta razón, las tendencias en el mundo de la seguridad se encaminan cada día más a trabajar los diferentes esquemas de protección, ya sea seguridad física, de personas o seguridad electrónica, entre otras; apoyándose irremediabilmente en los sistemas

* El proyecto pretende comprender y analizar la eficacia de los sistemas electrónicos de seguridad, para poderlo desarrollar me basé, sobre todo, en las asignaturas Análisis de riesgos, Seguridad física y Seguridad electrónica, así otras asignaturas vistas en la especialización también fueran muy importantes.

electrónicos de seguridad, con la aplicación a cada campo puntual de la seguridad y en muchos casos, realizando interacción entre unos y otros, con el fin de obtener mejores resultados en la eficacia de los mismos (Carrión Mena, 2006). De esta forma, se optimizan los recursos de las compañías y a su vez permite tener fuentes más fiables de información, que posteriormente permitan al hombre de seguridad, evaluar y parametrizar dicha información buscando la eficacia del esquema que se implemente en un determinado entorno.

Igualmente, estas herramientas o sistemas electrónicos de seguridad permiten optimizar el recurso humano, pero a su vez exigen una mayor preparación de quienes deben administrarlos, desarrollarlos y aplicarlos en los diferentes campos de la seguridad.

Desarrollo

Eficacia de los sistemas electrónicos de seguridad

1. Nociones principales sobre seguridad integral

La seguridad llamada integral está constituida por tres tipos de medios, los cuales deben conformar un todo.

Los medios humanos se definen como aquellos que están conformados por todo el grupo de personal de seguridad ya sea esta privada o pública. Mientras que los medios técnicos se conforman por los elementos físicos o denominados pasivos de un sistema y los medios electrónicos o denominados activos de un sistema. Y, por último, los medios de organización contemplan los planes, normas, procedimientos y estrategias, que igualmente son importantes dentro del proceso de integración.

Para poder entender y abordar si los sistemas electrónicos de seguridad son eficaces dentro de una industria o empresa, es necesario primero indicar que la percepción es un supuesto que el mismo individuo crea o ambienta en su mente basado en lo que perciben sus sentidos, haciendo entender para sí mismo que ciertos entornos pueden generarle mejores o peores sensaciones en seguridad (Carrión Mena, 2006). Es decir, todos los seres humanos que tienen la ventaja de tener todos sus sentidos en funcionamiento, pueden detectar diferentes ambientes y percepciones independientemente que estén compartiendo un mismo contexto o entorno.

Es así que, para el caso de la seguridad integral de un determinado sistema electrónico de seguridad, uno de los componentes más importantes es el hombre de seguridad, ya que según las nuevas mutaciones de las diferentes clases de delitos, los sistemas de seguridad están llamados a jugar un papel muy significativo en lo referente a la protección de los diferentes bienes tutelados, como la protección de vidas, activos y valores, entre otros; los cuales son encomendados dentro de las responsabilidades de la seguridad (López Fornieles, 2016).

Por esta razón, se requiere que el hombre de seguridad este a la vanguardia del conocimiento técnico y tecnológico, pasa asimismo entender que la integración tecnológica va de la mano con la integración física y humana.

Hacen parte de esta percepción de la eficacia, las experiencias que determinado individuo tenga con relación a otros y su capacidad de análisis para entender eventos y situaciones, respecto del entorno sociocultural y político, que necesariamente genera en cada individuo y sociedad una respuesta diferente en cuanto a la capacidad de percibir y entender, no queriendo decir que la actitud o respuesta que este de sea equivocada o acertada, simplemente se resalta que dicha percepción de su entorno, no es producto de una

sola fuente de información, sino que hace parte de un todo. Para esto se debe entender primero que es la seguridad y qué relación tiene esta con el individuo, su entorno y lo que esta espera de ella.

La seguridad es la sensación de tranquilidad que le permite al hombre desarrollarse en su entorno, con la convicción que no tiene ninguna amenaza que pueda materializarse y hacerle daño, por tal razón iniciaremos analizando que tan importante es para el hombre su percepción de seguridad en el entorno donde se desarrolla.

1.1 Objetivos principales de los sistemas electrónicos de seguridad.

Ahora bien, en cuanto a la eficacia de los sistemas electrónicos de la seguridad, donde se puede entender y visualizar más claramente si estos tienen una aplicación y efectividad para lo que fueron diseñados. Por ello, es preciso definir los objetivos principales de los sistemas electrónicos de seguridad los siguientes:

1. Retardo.
2. Detección.
3. Alerta.
4. Reacción.

El retardo se logra mediante la implementación de unas barreras físicas o electrónicas, sensores u otros. En cuanto a la detección, tiene relación directa con los anillos de seguridad posteriores, lo cuales permiten identificar antes de, una acción determinada. La alerta estará compuesta requiere de un componente tecnológico y humano. Y la reacción es la capacidad humana que se tenga con determinado equipo capacitado y entrenado, con el fin de ofrecer una respuesta rápida y efectiva a la amenaza (Ávila Barreno, González Magallanes, & Nacipuvha González, 2009).

Los sistemas electrónicos de seguridad han estado evolucionando de acuerdo con las nuevas necesidades de una sociedad, y la mutación de los nuevos modus operandi del delincuente dentro de los diferentes sectores de la economía, para cual los clientes en este caso empresas de los diferentes sectores, requieren cada día nuevas herramientas que garanticen mayor rapidez a la solución de sus problemas y, a su vez, eficiencia en la protección de sus activos.

Los sistemas electrónicos de seguridad han adquirido unas divisiones que se denominan generaciones, con el fin de poder tener una clasificación de su manejo y capacidad operativa y de esta forma garantizará al usuario sobre su confiabilidad y que cumplirá su objetivo al obtener los nuevos desarrollos tecnológicos (Ávila Barreno, González Magallanes, & Nacipuvha González, 2009).

Existen en la actualidad gran variedad de sistemas de seguridad, los cuales pueden ir desde un simple sistema de protección para una residencia hasta la automatización y control inteligente de grandes industrias y edificios, diseñados para cubrir las necesidades que se generan a diario en el entorno de empresas y sectores industriales.

Los sistemas electrónicos de seguridad de primera generación están limitados a la implementación de un determinado dispositivo, como una alarma con un sensor en una puerta y que su objetivo básico es emitir una señal sonora, en el cual el usuario del servicio tenía que determinar de forma manual su manejo.

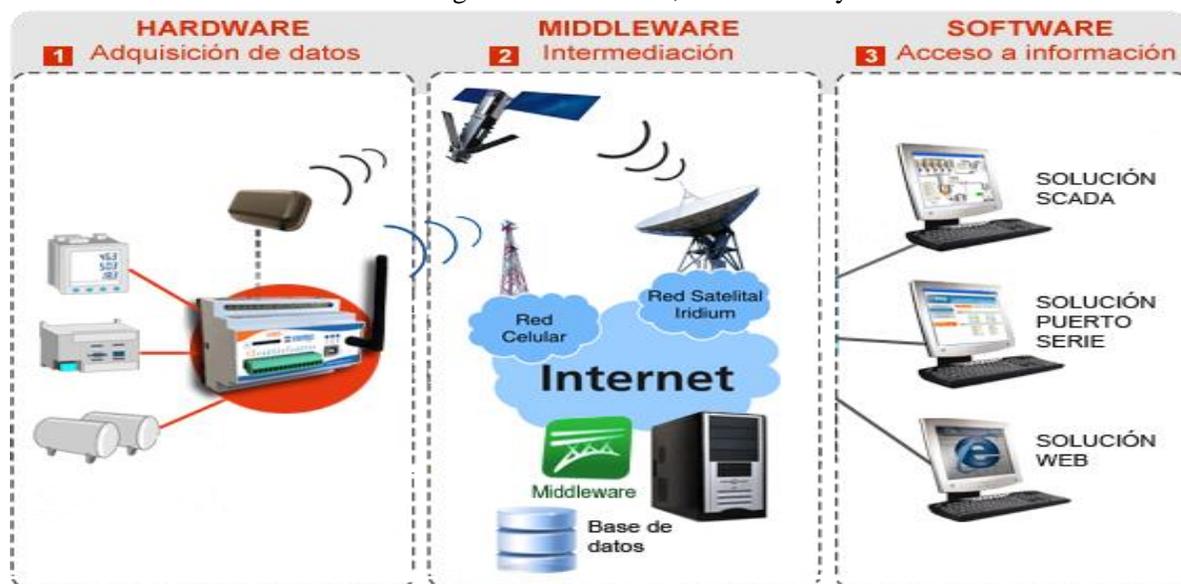
Los sistemas de segunda generación ya permitían controlar algunos eventos y en ocasiones estos mismos sistemas tenían la capacidad de tomar algunas decisiones permitiendo con esto hacerlo menos manual y evitando así en muchos casos falsas alarmas o alertas (López Fornieles, 2016).

Ya para los denominados de tercera generación podemos decir que son todos aquellos diseñados para monitorear eventos o situaciones desde lugares remotos, permitiendo que su usuario tenga mayor independencia y control del mismo sin tener que estar ubicado en un lugar determinado para ejercer su control y verificación.

Este tipo de sistemas efectivamente le permite al usuario tener una información más precisa y cuenta con bases de datos que le ayudan a establecer tendencias y estadísticas del mismo, optimizando de esta forma el sistema y permitiéndole en algunos casos tomar acciones de mejora en su empresa o instalación a la cual dese dar protección.

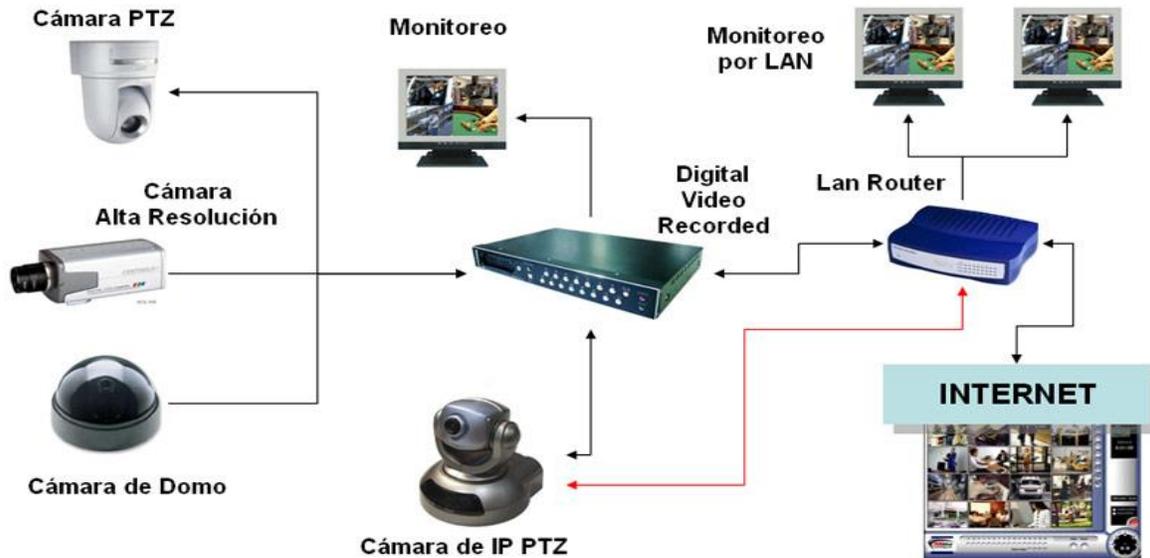
1.2 Esquemas de un sistema electrónico de seguridad.

Ilustración 1 Sistema Eléctrico de Seguridad: Hardware, Middleware y Software



Fuente: Bing.com/imágenes

Ilustración 2 Sistema Eléctrico de Seguridad: Cámaras, DVR, Monitoreo por LAN, LR, Internet.



Fuente: Bing.com/imágenes

1.3 Objetivos de un sistema electrónico de seguridad.

El sistema electrónico de seguridad tiene por objetivo básico la detección de un determinado evento que genere un riesgo en un determinado entorno o industria donde este se haya instalado. S decir, la detección o alerta temprana puede ir desde la ubicación o detección de un intruso, animal, un derrame de sustancias o un incendio (López Fornieles, 2016).

Los sistemas electrónicos su funcionalidad y objetivo no solo es de detectar sino que van mucho más allá, buscan generar alertas tempranas, con el fin de evitar o mitigar riesgos de seguridad del entorno donde fueron instalados (Oficina de las Naciones Unidas para la Reducción de Riesgos de Desastres, 2004).

Por esta razón es tan importante el componente humano capacitado para entender y analizar las diferentes señales o alertas emitidos por los diferentes sistemas de seguridad.

Como el caso cuando estos están monitoreados o controlados en centrales administradas por terceros especializados, dichas señales de alarma pueden llegar en forma sonora, visual, en texto o códigos cifrados; los cuales deben ser entendidos por quien opera o recibe la señal del sistema. Igualmente se debe contar con la capacidad operativa y de análisis para determinar la acción a tomar según el caso que se presente un evento y este se materialice (López Fornieles, 2016).

Como herramienta de control, administración y mantenimiento en el tiempo, cualquier sistema de seguridad electrónica que se instale en una industria debe contar con un plano de la ubicación de sus elementos de protección, ya sean sensores, cámaras, barreras perimétricas; esto con el fin de permitir a quien los opera y recibe las señales, identificar fácil y rápidamente el elemento que le está generando la alerta, ya sea para implementar su plan de reacción en un evento o en su defecto para realizar un mantenimiento tanto correctivo o preventivo a los elementos que componen el sistema de protección (Ávila Barreno, González Magallanes, & Nacipuvha González, 2009). De esta forma, disminuir con esto los tiempos de respuesta, costos de operación y riesgos asociados al mismo.

Los sistemas electrónicos de seguridad deben contar con protocolos y procedimientos que permitan su fácil manejo y a la vez los blinden en su seguridad, también es prudente y necesario realizar desafíos al sistema con el fin de conocer las debilidades y fortalezas del mismo a fin de realizar los planes de acción tendientes a su mejora continua y efectividad al momento de ser requeridos (López Fornieles, 2016).

Cada sistema de seguridad electrónica deberá ser pensado, diseñado e implementado pensando en la necesidad de ese cliente o industria específica que se quiera proteger, es por esta razón que se hace necesario e indispensable la presencia y complemento del hombre de seguridad, capacitado en conocimientos de tecnología y experiencias en la implementación

de estos sistemas, lo anterior en virtud que los sistemas de seguridad por si solos no podrían tener una eficacia alta de no ser por quienes determinan donde cuando y como instalarlos e integrarlos con otros sistemas para obtener los resultados esperados en la protección de los bienes tutelados encomendados.

Por esta razón antes de implementar o desarrollar un determinado sistema de protección electrónico en seguridad debemos tener en cuenta los siguientes interrogantes, con el fin de tener la claridad y efectividad del mismo: ¿Qué es lo que se va a proteger? ¿Cómo lo vamos a proteger?; y asimismo la ubicación del elemento u objetivo a proteger.

Se podría utilizar para esto la teoría de anillos concéntricos, para determinar niveles de protección desde los perímetros exteriores hacia adentro del objetivo a proteger así:

- El primer anillo deberá proteger las áreas exteriores con sensores de movimiento, barreras perimétricas, cercas eléctricas entre otros.
- El segundo anillo podrá contener elementos de protección para muros con sensores sísmicos, sensores magnéticos para puertas, discriminadores de audio para ventanas etc.
- Un tercer anillo protegerá directamente mediante tecnología de sensores pasivos y de movimiento, el objetivo principal detectando con esto y mediante señales tempranas el acceso a los perímetros protegidos, que podrán ser alternados con otros sistemas de seguridad electrónica, como el circuito cerrado de televisión, permitiendo un mayor control y monitoreo de los mismos, ocasionando con esto un retardo mayor en el accionar del delincuente o la amenaza, dando la oportunidad a los administradores de la seguridad, la oportunidad de tener una reacción más rápida y eficaz en la neutralización de la amenaza en contra del bien protegido (Ávila Barreno, González Magallanes, & Nacipuvha González, 2009).

1.4 Sistemas electrónicos de seguridad: matriz de riesgos.

Es de vital importancia y como complemento fundamental para mantener una adecuada eficacia en cualquier sistema de seguridad electrónica o física, el levantamiento de una matriz de riesgos que permita de forma objetiva y cuantitativa determinar los verdaderos riesgos de la empresa o industria a proteger.

Por lo tanto, ¿determinaremos inicialmente que es un riesgo?, el riesgo es la probabilidad que una amenaza se materialice y cause un determinado daño.

No obstante, de esta definición, los riesgos se pueden mitigar y manejar en cualquier ambiente o sitio donde estemos realizando nuestras actividades, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, de esta forma podemos tomar medidas tendientes a prevenir y mitigar aquellas amenazas, para que estas no se materialicen y causen un daño (Ávila Barreno, González Magallanes, & Nacipuvha González, 2009). Es por esta razón que los riesgos deben ser gestionados dentro de cualquier sistema de protección en seguridad que se dese implementar, esto nos ayuda a mantener el desarrollo sostenido de cualquier negocio y nos permite vivir de una forma más tranquila y segura. Una de las constantes en seguridad es la “prevención” esta a su vez son todas aquellas medidas que se toman tendientes a evitar que una determinada amenaza se materialice.

La segunda parte para administrar los riesgos es la mitigación de los mismos; y estas consisten en todas aquellas medidas que se implementan para reducir las vulnerabilidades detectadas frente a ciertas amenazas.

Las fases de prevención y mitigación del riesgo las podemos enunciar en tres:

1. Conocer cuáles son las amenazas y riesgos a los cuales estamos expuestos.
2. Implementación de unos planes de acción específicos para reducir estas amenazas, y de esta forma evitar que nos causen un daño.
3. Ejecutar los planes de mitigación previamente determinados (Banco Interamericano de Desarrollo. Universidad Nacional de Colombia. Instituto de Estudios Ambientales, 2002).

Ilustración 3 Ejemplo de una matriz de riesgos

Probabilidad	Consecuencias				
	Insignificante 1	Menor 2	Moderada 3	Mayor 4	Catastrófica 5
Raro 1	Bajo	Bajo	Moderado	Alto	Alto
Improbable 2	Bajo	Bajo	Moderado	Alto	Extremo
Posible 3	Bajo	Moderado	Alto	Extremo	Extremo
Probable 4	Moderado	Alto	Alto	Extremo	Extremo
Casi seguro 5	Alto	Alto	Extremo	Extremo	Extremo

Extremo: Los riesgos extremos deben ponerse en conocimiento de los Directores y ser objeto de seguimiento permanente.

Alto: Los riesgos altos requieren la atención del Presidente / Director General / Director Ejecutivo.

Moderado: Los riesgos moderados deben ser objeto de seguimiento adecuado por parte de los niveles medios de Dirección.

Bajo: Los riesgos bajos deben ser objeto de seguimiento por parte de los supervisores.

Fuente: EGV (2014).

Conclusiones

Los sistemas de seguridad en el campo electrónico, concurre a la medición objetiva y cuantitativa de un determinado riesgo, de tal forma que se convierte en el punto de partida para lograr la implementación de la integralidad de los sistemas electrónicos de seguridad, mediante la protección física para un determinado cliente, ya sea empresarial o industrial. Para lo cual se permite al hombre de seguridad la determinación de los diferentes riesgos inminentes, con el fin de identificar los procesos de tratamiento adecuado, de acuerdo con la categorización en la matriz de riesgos.

La mayor parte de las irregularidades de los sistemas electrónicos de seguridad se originan de la poca eficacia, ya que el hombre de seguridad profesional no cuenta con el conocimiento suficiente sobre los múltiples beneficios, repercutiendo en el desconocimiento técnico del elemento tecnológico de seguridad, como es el caso de una cámara de televisión que tiene alcance en metros, su radio de acción con el lente instalado, ya sea que posea infrarrojos, capacidad de almacenamiento de la información, pixelación, entre otros.

La ignorancia de este tipo de conceptos técnicos sobre la tecnología, conlleva a que el sistema que se implemente, en muchos casos, no aplique para lo que fue inicialmente estaba concebido según el sistema de seguridad, definiéndose por tal motivo, como ineficaces.

De conformidad con todo lo anterior, se puede concluir que los sistemas electrónicos de seguridad por sí solos son menos eficaces, pero cuando el profesional de la seguridad conocedor y estudioso de los mismos, logra integrar los preceptos técnicos y tecnológicos a favor del empresario o industria, de forma objetiva, solo así se obedece a la planificación previa como esquema de protección alcanzando resultados de alta eficacia.

Por esta razón, los componentes de un adecuado sistema de protección deberá siempre contar con un excelente profesional de la seguridad, un grupo humano conocedor de los sistemas electrónicos de seguridad tanto en sus bondades como sus vulnerabilidades, la integración de los mismos según el objetivo a proteger en una determinada empresa o industria, como también de un componente de altísimo valor como es la implementación de la matriz de riesgos sus planes de mitigación y monitoreo y seguimiento a los mismo en el tiempo, para poder garantizar la continuidad de un determinado negocio o industria.

Referencias.

- Ávila Barreno, N. K., González Magallanes, D. L., & Nacipuvha González, L. M. (2009). Proyecto de Implementación de un sistema de seguridad para la empresa DEVIES CORP en la ciudad de Milagro para prevenir pérdidas de inventarios por casos fortuitos. *Escuela Superior Politécnica del Litoral. Facultad de Economía y Negocios.*
- Carrión Mena, F. &.-V. (2006). La inseguridad en la ciudad: hacia una comprensión de la producción social del miedo. *Eure (Santiago)*, 32(97), 7-16.
- López Fornieles, D. (2016). Sistemas de seguridad. *Universidad Politécnica de Cataluña.*
- Herrera, Omar. Sistemas de detección de intrusos. Artículos de seguridad Informática y seguridad de redes 2003.
- Alarcón, Vicente, Curso de Redes de computadora. Universidad de las Américas Puebla, México, 2009.
- Seguridad y Tecnología Coogee Theme, Seguridad y Amenazas en Redes. Noviembre 2008. Buenos Aires Argentina.
- Sistemas de Seguridad. Julio Muñoz Guerrero, S.A Ediciones Paraninfo 2000.
- Bello, Claudia E. ARCERT. Manual de seguridad en redes, Argentina. Año 2000

Internet.

Banco Interamericano de Desarrollo. Universidad Nacional de Colombia. Instituto de Estudios Ambientales. (16 de diciembre de 2002). *Amenaza, Vulnerabilidad, Riesgo, Desastre, Mitigación, Prevención*. Obtenido de

<http://idea.unalmz.edu.co/documentos/Anne-Catherine%20fase%20I.pdf>

EGV. (2014). *EGV se reúne para Revisar y Complementar la Matriz de Riesgos utilizada en Faenas*. Obtenido de <http://www.egv.cl/noticias.html>

Oficina de las Naciones Unidas para la Reducción de Riesgos de Desastres. (2004). *Vivir con el Riesgo: informe mundial sobre iniciativas para la reducción de desastres*.

Obtenido de <http://www.eird.org/fulltext/LwR2004-esp/pdf/ch1%20Section%201.pdf>