Sistemas & Telemática
ISSN: 1692-5238
EditorSyT@icesi.edu.co
Universidad ICESI
Colombia

Acevedo, Nancy; Satizábal, Cristina
Risk management and prevention methodologies: a comparison
Sistemas & Telemática, vol. 14, núm. 36, 2016, pp. 39-58
Universidad ICESI
Cali, Colombia

Discussion paper / Artículo de reflexión - Tipo 2

Risk management and prevention methodologies: a comparison

Nancy Acevedo, Esp. / acevedoquintana@gmail.com

Cristina Satizábal, Ph.D. / cristina.satizabal@unipamplona.edu.co

Universidad de Pamplona, Colombia

ABSTRACT In this paper we analyze nine risk management and prevention methodologies, carrying out a comparison of the stages that they include and determining if they take into account the human factor in the risk analysis and treatment. We observe that only 42.85% of the studied management risk methodologies include this factor and conclude that the NIST [National Institute of Standards and Technology] Risk Management methodology is the most complete, although it would be desirable for it to focus more on the human factor like the IDB [Inter-American Development Bank] Corruption Diagnosis, Prevention and Control in Programs of Civic Security methodology.

KEYWORDS Analysis; management; methodologies; prevention; risks.

Metodologías de gestión y prevención de riesgos: una comparación

RESUMEN En este artículo se analizan nueve metodologías de gestión y prevención de riesgos a través de la comparación de sus fases y de la revisión de si consideran o no al factor humano en el análisis y tratamiento de los riesgos (se observa que menos de la mitad de ellas, esto es 42,85% considera este factor). Las investigadoras concluyen que la metodología de gestión de riesgos del Instituto Nacional de Estándares y Tecnología es la más completa, aunque sería conveniente que se enfocara más en el factor humano, como lo hace la metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del Banco Interamericano de Desarrollo.

PALABRAS CLAVE Análisis; gestión; metodologías; prevención; riesgos.

Metodologias de gestão e prevenção de riscos: uma comparação

RESUMO Este artigo analisa nove metodologias de gestão e prevenção de riscos, comparando as suas fases e avalia-se se devem ou não considerar o fator humano na análise e tratamento de riscos (observa-se que menos de metade delas, isto é 42,85% consideram esse fator). As investigadoras concluem que a metodologia de gestão de riscos do Instituto Nacional de Estándares e Tecnologia é a mais completa, embora fosse conveniente se focar mais no factor humano, como o faz a metodologia para o diagnóstico, prevenção e controle da corrupção em programas de segurança cidadã do Banco Interamericano de Desenvolvimento.

PALAVRAS-CHAVE Análise; gestão; metodologias; prevenção; riscos.

This paper is an output from the research project: Methodology for risk prevention on the management of personal information filed in the academic information system of Universidad de Pamplona / Este artículo es producto del proyecto de investigación: Metodología para la prevención de riesgos en el manejo de la información personal almacenada en el sistema de información académica de la Universidad de Pamplona. (Convocatoria de Banco de Proyectos 2014 - Vicerrectoría de Investigaciones, Universidad de Pamplona. Código: PR130-00-21 (GA190-CM-I-2014-2.1.2.2.1).

Received / Recepción: Enero 7, 2016 - Accepted / Aceptación: Marzo 1, 2016 *doi: 10.18046/syt.v14i36.2214*

I. Introduction

Effective use of information and communications technologies [ICT] is a critical factor of success in current society. Most failures are not caused by the technology itself, but rather by the manner in which it is used (Yu, 2004). Due to the misuse of personal information, many users have been victims of fraud and extortion through the Internet, yet most such incidents could be prevented if the risks were properly analyzed, and the appropriate prevention strategies for each context were implemented.

Although engineering focuses more on technology than on people (Frosdick, 1997), engineers know that "risk perception depends largely on beliefs, feelings and judgments, and has great influence on tolerance or acceptance of risk" (Strutt, 1993). However, the techniques used in engineering are more concerned with identifying technical failures than social matters such as risk perception, cultural bias, and failures in human communication.

Social scientists are strongly opposed to the vision of natural scientists and engineers regarding risk management, and warn that ignoring sociological or social questions can be problematic, since the result of a human error –or of the lack of communication– can be as disastrous as the result of a technical failure (Frosdick, 1997).

So, it is crucial to conduct a review of the methodologies of the management and prevention of existing risks, to identify common and distinctive characteristics of each, and to determine whether the human factor is considered.

In section II, prevention and risk concepts from different contexts are defined; section III describes the different management methodologies and risk prevention found in the literature; in section IV, aspects for comparing the different methodologies are identified; in section V different methodologies are compared; and section VI presents the conclusions.

II. Definitions

Risk

A timeline showing how the concept of risk has evolved in different contexts is presented in Table 1.

Prevention

At a democratic level, the concept of conflict prevention is used, having gained attention after the Cold War due to the awareness of the dangers of intra-state war and the collapse of states used (Weiss & Hubert, 2001).

Conflict prevention strategies can be divided into two categories: structural prevention, and direct or operational prevention

I. Introducción

El uso eficiente de las Tecnologías de la Información y las Comunicaciones [TIC] se ha convertido en un factor de éxito crítico para la sociedad actual. La mayoría de las fallas no se deben a la tecnología en sí, sino a la manera en que ella se usa (Yu, 2004). Debido al uso inadecuado de la información personal, muchos usuarios han sido víctimas de fraude y extorsión a través de Internet, sin embargo, la mayoría de estos incidentes se podría evitar si se analizan adecuadamente los riesgos y se implantan estrategias de prevención adecuadas a cada contexto.

Aunque la ingeniería se centra más en la tecnología que en las personas (Frosdick, 1997), los ingenieros saben que ''la percepción del riesgo depende en gran medida de las creencias, sentimientos y juicios, y tiene gran influencia sobre la tolerancia o aceptación del riesgo'' (Strutt, 1993). Sin embargo, las técnicas utilizadas en la ingeniería se preocupan más por la identificación de las fallas técnicas, que por cuestiones sociales como: la percepción del riesgo, el sesgo cultural y las fallas en la comunicación humana.

Los científicos sociales se oponen fuertemente a la visión de los científicos naturales y de los ingenieros en cuanto a la gestión de riesgos y advierten que hacer caso omiso de las cuestiones sociológicas o sociales podría resultar problemático, ya que el resultado de un error humano –o de la falta de comunicación– puede ser tan desastroso como el resultado de una falla técnica (Frosdick, 1997).

Por lo dicho, es de vital importancia hacer una revisión de las metodologías de gestión y prevención de riesgos existentes, identificar las características comunes y distintivas de cada una de ellas, y determinar si consideran el factor humano.

En la sección II se definen los conceptos de prevención y riesgo desde diferentes contextos, en la sección III se describen las diferentes metodologías de gestión y prevención de riesgos encontradas en la literatura, en la sección IV se identifican los aspectos a comparar en las diferentes metodologías, en la sección V se comparan las diferentes metodologías y en la sección VI se presentan las conclusiones.

II. Definiciones

Riesgo

En la Tabla 1 se presenta una línea de tiempo que permite apreciar cómo ha evolucionado el concepto de riesgo en los diferentes contextos.

Prevención

A nivel democrático se utiliza el concepto de prevención de conflictos, que ganó gran atención después de la Guerra Fría, debido a la concientización que hubo sobre los peligros que acarrea la guerra intra-estatal y el colapso de los Estados (Weiss & Hubert, 2001).

Date	Hito	Benchmark
Siglo XVII	Matemáticas de juegos de azar: "El riesgo es una comparación entre la probabilidad y la magnitud de las pérdidas y las ganancias potenciales". (Douglas,1990)	Mathematics associated with gambling:"Risk referred to a combination between probability and magnitude of potential gains and losses". (Douglas,1990)
Siglo XVIII	Negocios de los seguros marítimos: Riesgo todavía considerado como las ganancias y las perdidas. (Douglas,1990)	Marine insurance business: Risk, is still considered both gains and losses. (Douglas,1990)
Siglo XIX	Economía: Riesgo concepto negativo, por lo que se crearon incentivos especiales para que se tomara el riesgo que implicaba la inversión. (Douglas,1990)	Economy: The concept of risk, seen more negatively, caused entrepreneurs to call for special incentives to take the risk involved in investment. (Douglas,1990)
Siglo XX	Ingeniería y Ciencia: "El riesgo es los peligros que plantean los avances tecnológicos modernos en la industria nuclear y petroquímica". (Gerber & Von Solms, 2005)	Engineering and Science: "The risk is the hazards posed by modern technological developments such as in the petro-chemical and nuclear industries"(Gerber & Von Solms, 2005)
1991	Estándar Británico 4778: "El riesgo es la combinación de la probabilidad o de la frecuencia de ocurrencia de un peligro definido y la magnitud de las consecuencias de su ocurrencia". (British Standards Institution,1991)	British Standard 4778: "Risk is 'the combination of the probability or frequency of occurrence of a defined hazard and the magnitude of the consequences of the occurrence". (British Standards Institution, 1991)
1992	Royal Society: "El riesgo es la probabilidad de que un evento adverso particular ocurra durante un periodo de tiempo establecido o resulte de un desafío particular". (Royal Society, 1992)	Royal Society: "The risk is he probability that a particular adverse event occurs during a stated period of time, or results from a particular challenge". (Royal Society, 1992)
1993	Ingenieros saben que "Percepción del riesgo depende en gran medida de las creencias sentimientos y juicios, y tiene gran influencia sobre la tolerancia o aceptación del riesgo". (Strutt, 1993).	Engineers know that "Risk perception depends very much on beliefs, feelings and judgements [and] has major influence on the tolerability or acceptance of risk". (Strutt, 1993).
	Paradigma de las Ciencias Naturales: "Riesgo objetivo o evaluado, debido a los métodos científicos de la valoración.	Paradigm of Natural Sciences: "Target risk or evaluated, because scientific methods of valuation.
	Evaluación objetiva del riesgo sigue cálculos precisos, formulas y experimentos exactos".(Kirkwood,1994)	Objective risk assessment remains accurate calculations formulas and exact experiments". (Kirkwood, 1994)
1994	Paradigma de las Ciencias Sociales: "Riesgo subjetivo o percibido, decisión a la que se llegó sin una evaluación científica. Evaluación subjetiva del riesgo se basa en percepción, heurística o decisión a la que se llega mediante la utilización de experiencia, juicio e ingenio" (Kirkwood,1994)	Paradigm of Social Sciences: "Subjective or perceived risk, since it is a decision, which is arrived at without a scientific assessment. The subjective risk evaluation is based on perception, heuristics or rule-of-thumb guidelines. Rule-of-thumb being a decision arrived at by utilizing experience, judgment and ingenuity" (Kirkwood,1994)
1995	Ambiente Computacional: "El riesgo es el potencial del daño aun sistema, o a los activos asociados, que existe como resultado de la combinación de una amenaza de seguridad y una vulnerabilidad". (Kailay & Jarratt, 1995)	Computational Environment: "The risk is the potential for damage to a system or associated assets that exists as the result of a combination of a security threat and vulnerability. The risk exists because of the combination of threats, vulnerability and asset value". (Kailay & Jarratt, 1995)
	NIST: "El riesgo es la posibilidad de que ocurra algo adverso" (NIST,1995)	NIST: "The risk as the possibility of something adverse happening". (NIST,1995)
1996	ISO/IEC TR 13335-1 "El riesgo comprende una combinación de activos, amenazas y vulnerabilidades". (ISO/IEC TR 13335 1, 1996)	ISO / IEC TR 13335-1 "Risk comprises a combination of asset, threat and vulnerability". (ISO/IEC TR 13335 1, 1996)
1997	Frosdick: El análisis de los riesgos es la suma de identificación, estimación y evaluación del riesgo. (Frosdick, 1997)	Frosdick: The risk analysis is the sum of risk identification, estimation and evaluation. (Frosdick, 1997)
1999	La gestión de riesgos debe ir precedida de una actividad de análisis de riesgos. (Bandyopadhyay, Mykytyn & Mykytyn, 1999; Owens, 1998; BS 7799-2, 1999; Moses, 1992)	Risk management should be preceded by some risk analysis activity. (Bandyopadhyay, Mykytyn & Mykytyn, 1999; Owens, 1998; BS 7799-2, 1999; Moses, 1992)
2001	NIST: "El riesgo es el impacto negativo neto debido a una vulnerabilidad considerando su probabilidad y el impacto de ocurrencia". (NIST, 2001)	NIST : "The risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence". (NIST, 2001)
	Australian/ New Zealand Standard: "La gestión del riesgo es un proceso iterativo conformado por pasos bien definidos que llevados a cabo de manera secuencial, constituye el fundamento para la adecuada toma de decisiones, al proporcionar un mejor conocimiento de los riesgos y del impacto de los mismos". (Martínez López, 2001)	Australian/New Zealand Standard: "Risk management is an iterative process consisting of well-defined steps carried out sequentially, it is the basis for proper decision making by providing a better understanding of the risks and the impact of them". (Martínez López, 2001)

Table 1. Evolution of the risk concept / Evolución del concepto de riesgo

(Wallensteen, 2002). Structural prevention incorporates measures to ensure that a crisis does not arise in the first place, and if it does, to avoid repetition. Operational or direct prevention consists of measures to address an immediate crisis (Carnegie Corp., 1957). The choice between structural or direct prevention depends on the areas of disagreement, the appropriate time to implement the preventive action, the levels at which preventive measures should be applied, and the different theories on the causes of conflict and how these should be treated (Wallensteen & Möller, 2003).

In the health field, the concept of prevention is related to the health–disease process (disease prevention). In every period of history there have been different interpretations of health and disease, which are in turn related to the political, economic and social situations of each historical moment (García-Ospina & Tobón-Correa, 2000).

Prevention was described by Henry Sigerist (1951) as one of the three functions of medicine, along with repair or treatment of injury and rehabilitation. Later, Americans classified it as a function of public health.

Prevention has been defined by the World Health Organization as "the application of technical measures including medical aspects and other disciplines that aim to prevent the onset of disease –primary prevention–, heal –secondary prevention–, and restore lost abilities –tertiary prevention" (OMS, 1986 cited by Sánchez-Peña, Sánchez-Delgado, & Agudelo-Ramírez, 2015).

Prevention in the social context is identified at a glance at first look a set of actions that can eliminate or reduce conditions of criminality present in society, when warning signs have not yet been shown, and may include measures aimed at groups at criminal risk or a criminal event that has already been committed, to prevent a subsequent recurrence (Brantingham & Faust, 1976).

In an analysis of prevention programs performed in Belgium during the 1980s, Walgrave and De Cauter (1986) critically analyzed a classification based on the distinction between the moments at which the preventive action is involved –before, during or after the unwanted event–, the focus of preventive intervention –the behaviors of subjects or modification of the social context–, and the defensive orientation –about symptoms– or offensive orientation –about the causes. Thus, social prevention is not a specific action or one of the numerous modalities of prevention, but rather a global policy, oriented to the social welfare, that cuts across all sectors of administrative policy (Graham & Bennett, 1995; Knepper, 2007; Peyre, 1986; Walgrave & De Cauter, 1986).

Las estrategias de prevención de conflictos se pueden dividir en dos categorías: prevención estructural y prevención directa u operacional (Wallensteen, 2002). La prevención estructural incorpora medidas para asegurar que la crisis no surja, en primer lugar, y si lo hace, que no se repita. La prevención operacional o directa consta de medidas para enfrentar crisis inmediatas (Carnegie Corp., 1957). La elección entre prevención estructural o directa depende de las áreas de desacuerdo, el tiempo apropiado para implantar la acción de prevención, los niveles en que las medidas preventivas deben ser aplicadas, así como de las diferentes teorías sobre las causas de los conflictos y de cómo estos deben ser tratados (Wallensteen & Möller, 2003).

En el campo de la salud, el concepto de prevención está ligado al proceso salud-enfermedad (prevención de enfermedades). En cada época de la historia se han dado diferentes interpretaciones a la salud y a la enfermedad, las cuales, a su vez, se relacionan con las situaciones políticas, económicas y sociales de cada momento histórico (García-Ospina & Tobón-Correa, 2000).

La prevención fue descrita por Henry Sigerist (1951) como una de las tres funciones de la medicina, junto con la reparación o el tratamiento del daño y la rehabilitación. Más adelante, los norteamericanos las denominaron como funciones de la salud pública.

La prevención ha sido definida por la Organización Mundial de la Salud como: "la aplicación de medidas técnicas que incluyen aspectos médicos y de otras disciplinas que tienen como finalidad impedir la aparición de la enfermedad –prevención primaria–, curarla –prevención secundaria– y devolverle las capacidades perdidas –prevención terciaria–" (OMS, 1986 citada por Sánchez-Peña, Sánchez-Delgado, y Agudelo-Ramírez, 2015).

La prevención en el contexto social se identifica a simple vista como el conjunto de acciones que permite eliminar o reducir las condiciones de criminalidad presentes en lo social, cuando todavía no se han manifestado señales de peligro, y puede comprender medidas dirigidas a grupos en riesgo delictivo o a un evento criminal que ya ha sido cometido, para prevenir posteriores recaídas (Brantingham & Faust, 1976).

En un análisis de los programas preventivos realizado en Bélgica durante los años 80, Welgrave y De Cauter (1986) analizaron críticamente una clasificación basada en la distinción entre los momentos en los que interviene la acción preventiva –antes, durante o después del evento indeseado–, el enfoque de la intervención preventiva –los comportamientos de los sujetos o la modificación del contexto social– y la orientación defensiva –sobre los síntomas– u ofensiva –sobre las causas–. Entonces, la prevención social no es una acción específica o una de las numerosas modalidades de prevención, sino una política global orientada al bienestar social que atraviesa todos los sectores de las políticas administrativas (Graham & Bennett, 1995; Knepper, 2007; Peyre, 1986; Walgrave & De Cauter, 1986).

Tonry y Farrington (1995) rechazan esta visión amplia y, con la intención de ser más claros, separan la prevención social en dos partes: una, relativa a las motivaciones individuales, la otra, al contexto social. La prevención social es simple: considerando que los comportamientos criminales son el resultado de predisposiciones y oportunidades, se intenta modificar las predisposiciones, cuanto sea posible, pasando después a modificar las oportunidades (Savona, 2004).

En el campo de la educación, la prevención de la violencia en la escuela se compone de dos vertientes: la de la salud pública y la de los derechos. En el campo de la salud pública: la prevención primaria busca fomentar un ambiente social e individual de respeto y tolerancia, de valores sociales y de conducta personal que favorezca que los conflictos se resuelvan de maneras no violentas, o sea, se dirigen a evitar que ocurra el hecho violento (Concha-EastMan, 2004); la prevención secundaria busca detener precozmente o retardar el progreso de la violencia o de sus secuelas en cualquier punto de su aparición (Vargas, Villegas, Sánchez, & Holthuis, 2003), se aplica cuando un evento violento ya ha ocurrido, y su intención es evitar nuevos episodios o disminuir su gravedad (Concha-EastMan, 2004); y la prevención terciaria se orienta a reducir las complicaciones y consecuencias de los daños de la violencia, en ella adquiere importancia la rehabilitación para mejorar la calidad de vida (Vargas et al., 2004).

Existen variables internas –endógenas– y externas –exógenas– que intervienen en la prevención de la violencia escolar. Las variables endógenas se refieren a factores que podríamos llamar instrumentales o directos, como los sistemas de normas y reglamentos, así como los proyectos político-pedagógicos (Hayden & Blaya, 2001; Ragmognino, FradJi, Soldini, & Vergés, 1997). Las variables exógenas, por su parte, están relacionadas con las habilidades vinculadas a aprender, a ser y a convivir, que cubren una amplia gama de capacidades, tales como: asumir retos en lo académico; establecer relaciones humanas estables y satisfactorias; mantener la esperanza sobre el futuro; y tomar decisiones oportunas, adecuadas, efectivas y constructivas.

La prevención en el contexto educativo debe fortalecer cuatro capacidades fundamentales: permitir al alumno establecer vínculos de calidad en diversos contextos; ser eficaz en situaciones de estudio-trabajo, movilizando la energía y el esfuerzo precisos para ello, y obteniendo el reconocimiento social necesario; integrarse en grupos de iguales constructivos, resistiendo presiones inadecuadas; y desarrollar una identidad propia y diferenciada que le ayude a encontrar su lugar en el mundo y le permita apropiarse de su futuro (Díaz-Aguado, Martínez-Arias, & Martín-Seoane, 2004).

La prevención, en el contexto de las redes computacionales, significa mantener a los atacantes alejados –es decir, prevenir que los atacantes entren a la red– (Khan-Pathan, 2010), es así como se habla de la prevención de crímenes

Tonry and Farrington (1995) reject this wide vision and intend to be clearer, stating that social prevention is separated into two parts: one related to individual motivations, the other to the social context. Social prevention is simple: considering that criminal behavior is the result of predispositions and opportunities, the intention is to change the predispositions as far as possible, then to modify the opportunities (Savona, 2004).

In the field of education, the prevention of violence at school consists of two aspects: public health and rights. In the field of public health, primary prevention seeks to promote a social and individual environment of respect and tolerance, social values and personal behavior that favors a resolution of non-violent conflict, i.e., the goal is to prevent the violent event occurring (Concha-Eastman, 2004); secondary prevention aims to stop promptly or slow the progress of violence or its sequel at any point that it appears (Vargas, Villegas, Sanchez, & Holthuis, 2003). This applies when a violent event has already occurred, and their intention is avoid new episodes or reduce their severity (Concha-Eastman, 2004). Tertiary prevention aims to reduce the complications and consequences of the harm of violence, and it is here that rehabilitation becomes important to improve the quality of life (Vargas et al., 2004).

There are internal –endogenous– and external –exogenous– variables involved in preventing school violence. The endogenous variables relate to factors that might be called instrumental or direct, such as systems of rules and regulations, as well as political–pedagogical projects (Hayden & Blaya, 2001; Ragmognino, Fradji, Soldini, & Vergés, 1997). The exogenous variables, meanwhile, are related to learning skills; to be, and to coexist; covering a wide range of capabilities, such as taking on academic challenges; establishing stable and favorable human relations; maintaining hope for the future; and taking timely, appropriate, effective and constructive decisions.

Prevention in the educational context should strengthen four fundamental capabilities: enabling students to establish quality links in different contexts; being effective in work–study situations, mobilizing the energy and precise effort to do so, and obtaining the necessary social recognition; integrating groups of equal construction, resisting pressures adequately; and developing a distinct identity that helps you find your place in the world and enables you to appropriate its future (Díaz-Aguado, Martínez-Arias, & Martín-Seoane, 2004).

Prevention in the context of computer networks means keeping attackers at a distance –that is, preventing attackers from entering the network– (Khan-Pathan, 2010), and thus it speaks of cybercrime prevention, incident prevention and intrusion prevention.

Crime prevention in the context of cyberspace means reducing the risk of the occurrence of the crime and the potential gravity of the crime, and disorderly events that may occur, both on-line and off-line (Ekblom, 2003).

In the prevention of accidents, on the other hand, there are four main elements: policies, which are the basis for implementing preventive controls; awareness to reduce the number of incidents that occur by human error; mitigating vulnerabilities to eliminate some possible attack vectors; and mitigation of threats to prevent attacks on different systems and networks from being successful (Mell, Kent, & Nusbaum, 2005).

An intrusion prevention system [IPS] is a device or program used to detect signs of intrusion in networks or systems and to take action. Such action consists in generating alarms or blocking intrusions in an active way (Piper, 2011).

III. Risk management and prevention methodologies

Octave

Octave is a risk analysis methodology developed by Carnegie Mellon University in 2001. Its name is an acronym for Operationally Critical Threat, Asset and Vulnerability Evaluation. Octave studies the risks based on three principles: confidentiality, integrity and availability. This methodology is used by different government agencies such as the United States Department of Defense [DoD] (Huerta, 2012). The three phases of this methodology are defined as follows (Alberts & Dorofee, 2001):

- Phase 1: Build profiles based on active threats: important information assets, threats to assets, security requirements of the assets, the actions that the organization is taking to protect them, and weaknesses in organizational policies and practices are identified.
- Phase 2: Identify infrastructure vulnerabilities: key operating components of information technologies are examined for technological vulnerabilities that could lead to an unauthorized action.
- Phase 3: Develop strategies and security plans: the information generated in Phases 1 and 2 is analyzed to identify business risks and assess risks based on their impact on the mission of the organization. In addition, a protection strategy is developed, for organizational plans and mitigation which address the risks of highest priority.

CORAS

CORAS is a European research and technological development project. In the CORAS method an analysis of security risks is carried out in seven steps (Boge, 2001):

cibernéticos, prevención de incidentes y prevención de intrusos.

La prevención del crimen, en el contexto del ciberespacio, significa reducir el riesgo de ocurrencia del crimen y la gravedad potencial del crimen y de eventos desordenados que pueden ocurrir, tanto en línea, como fuera de línea (Ekblom, 2003).

En la prevención de incidentes, por otra parte, existen cuatro elementos principales: políticas, que son la base para implementar controles preventivos; concientización, para reducir el número de incidentes que ocurren por errores humanos; mitigación de vulnerabilidades, para eliminar algunos posibles vectores de ataque; y mitigación de amenazas, para prevenir que las amenazas de diferentes sistemas y redes atacantes sean exitosas (Mell, Kent, & Nusbaum, 2005).

Un sistema de prevención de intrusos [*Intrusion Prevention System, IPS*] es un dispositivo o programa utilizado para detectar señales de intrusión en las redes o sistemas y tomar una acción. Dicha acción consiste en generar alarmas y/o bloquear las intrusiones de manera activa (Piper, 2011).

III. Metodologías de gestión y prevención de riesgos

Octave

Octave es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en 2001, su acrónimo significa *Operationally Critical Threat, Asset and Vulnerability Evaluation*. Octave estudia los riesgos con base en tres principios: confidencialidad, integridad y disponibilidad. Esta metodología es utilizada por distintas agencias gubernamentales, tales como el Departamento de Defensa de Estados Unidos [DoD] (Huerta, 2012). Las tres fases de esta metodología se definen así (Alberts & Dorofee, 2001):

- Fase 1: construir perfiles de amenazas basados en activos: se identifican los activos de información importantes, las amenazas a los activos, los requisitos de seguridad de los activos, lo que la organización está haciendo para protegerlos y las debilidades en las políticas y prácticas organizacionales.
- Fase 2: identificar vulnerabilidades de la infraestructura: los componentes operativos clave de las tecnologías de información se examinan en busca vulnerabilidades tecnológicas que puedan conducir a una acción no autorizada.
- Fase 3: desarrollar las estrategias y los planes de seguridad: la información generada en las fases 1 y 2 se analiza para identificar riesgos para la empresa y evaluar los riesgos en función de su impacto en la misión de la organización. Además, se desarrolla una estrategia de protección para los planes de la organización y de mitigación que aborde los riesgos de más alta prioridad.

CORAS

Coras es un proyecto de investigación y desarrollo tecnológico europeo. En el método CORAS un análisis de riesgos de seguridad se lleva a cabo en siete pasos, así (Boge, 2001):

- Paso 1: reunión introductoria donde los representantes del cliente presentan sus objetivos generales de análisis y lo que desean analizar.
- Paso 2: reunión con los representantes del cliente, donde los analistas presentan su comprensión de lo que entendieron en la primera reunión y el estudio de la documentación que puso a su disposición el cliente; este segundo paso implica también un análisis básico de la seguridad de alto nivel.
- Paso 3: descripción más precisa del objeto a analizar y de todos los supuestos y otras condiciones previas hechas. Este paso termina cuando toda esta documentación ha sido aprobada por el cliente.
- Paso 4: taller con personas con experiencia en el objeto del análisis, realizado con el objetivo de identificar el mayor número de posibles incidentes no deseados como sea posible, así como las amenazas, vulnerabilidades y escenarios de amenaza.
- Paso 5: taller enfocado en la estimación de las consecuencias y de los valores de probabilidad para cada uno de los incidentes no deseados identificados.
- Paso 6: entrega al cliente del primer cuadro de riesgo general, lo que normalmente da lugar a algunos ajustes y correcciones.
- Paso 7: identificación del tratamiento y abordaje de cuestiones de costo/beneficio de los tratamientos.

Estándar australiano

La metodología de administración de riesgos según estándar australiano se desarrolla en cinco fases, las cuales, de acuerdo con el AS/NZS 4360:1999, son:

- Establecer el contexto: se definen los parámetros básicos de los procesos que ocurren dentro de la estructura organizacional de acuerdo con el contexto estratégico, organizacional y de administración de riesgos, lo que da como resultado el desarrollo de criterios de evaluación y una guía para la toma de decisiones.
- Identificar riesgos: se identifican todos los riesgos a administrar, estén o no bajo control de la organización.
- Analizar riesgos: se separan los riesgos menores de los riesgos mayores y así se proveen datos para su evaluación y tratamiento; esta fase involucra prestar atención a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias.
- Evaluar riesgos: se compara el nivel de riesgo detectado durante el proceso de análisis con los criterios de riesgo establecidos previamente, el resultado de una evaluación de riesgos es una lista de riesgos con prioridades para una acción posterior, basadas en los objetivos de

- Step 1: Introductory meeting where customer representatives present the overall objectives of their analysis and what they want to analyze.
- Step 2: Meeting with customer representatives, where analysts present their understanding of the concerns put forward at the first meeting and the study of the documentation made available by the client; This second step also involves a basic analysis of high-level security.
- Step 3: Accurate description of the object to be analyzed and of all other preconditions and assumptions made. This step ends when all this documentation has been approved by the customer.
- Step 4: Workshop with people of experience in the subject of the analysis, carried out in order to identify the largest possible number of unwanted incidents, as well as threats, vulnerabilities and threat scenarios.
- Step 5: Workshop focusing on the estimation of the consequences and probability values for each unwanted incident identified earlier.
- Step 6: Customer delivery of the first picture of overall risk, which usually results in some adjustments and corrections.
- Step 7: Identification of treatment and addressing issues of cost/benefit of treatment.

Australian standard

The risk management methodology according to the Australian Standard is divided into five phases, which, according to the AS/NZS 4360: 1999, are:

- Establish the context: The basic parameters of the processes occurring within the organizational structure are defined, according to the strategic, organizational and risk management context, which results in the development of assessment criteria and a guide for decision.
- Identify risks: All risks to be managed are identified, whether or not they are under the control of the organization.
- Analyze risks: Minor risks are separated from major risks and thus data for their evaluation and treatment are provided; this phase involves paying attention to the sources of risks, their consequences and the probabilities that those consequences may occur.
- Evaluate risks: The risk level identified during the analysis process is compared with risk criteria previously established; the result of a risk assessment is a list of

risks prioritized for further action, based on the objectives of the organization and the degree of opportunity there could be to take the risk.

- Address risks: The range of options to address risks is identified, these options are evaluated, and risk treatment plans are prepared and implemented.

NTC-ISO/IEC 27005

This, the technical standard of risk management in information security, includes the following steps in the risk management process:

- Establish the context: This implies establishing the basic criteria necessary for risk management, defining the scope and boundaries, and establishing an appropriate organization for risk management.
- Assessing the risk: This consists in identifying the risks, describing them quantitatively or qualitatively and prioritizing them against the risk evaluation criteria and relevant objectives for the organization. It consists of the identification, estimation, and assessment of the risk.
- Risk identification: Its purpose is to determine what might happen to cause a potential loss, and to understand how, where and why this loss could occur. For this it is necessary to identify: assets, threats, existing controls, vulnerabilities, and consequences.
    - Risk estimation: An estimation methodology may be qualitative or quantitative, or a combination of these, depending on the circumstances; in practice, often qualitative estimation is used first to obtain a general indication of the level of risk and reveal the most significant risks, and subsequently, if necessary, a quantitative analysis of the significant risks is performed, since it is generally less complex and less expensive to perform a qualitative analysis than a quantitative one.
    - Risk assessment: Consists in comparing risk levels against criteria for risk assessment and their acceptance criteria.
    - Risk treatment: Consists of selecting controls to reduce, retain, avoid, or transfer risks; a plan for risk treatment should be defined.
- Acceptance of risk: This involves taking the decision to accept the risks and responsibilities for the decision and registering them in a formal way.

1. *Central Communication and Telecommunication Agency*

la organización y el grado de oportunidad que podría resultar al tomar el riesgo.

- Tratar los riesgos: se identifica el rango de opciones para tratar los riesgos, evaluar esas opciones, preparar planes para tratamiento de los riesgos e implementarlos.

NTC-ISO/IEC 27005

Esta, la norma técnica de gestión del riesgo en la seguridad de la información, incluye estos pasos en el proceso de gestión del riesgo:

- Establecer el contexto: implica establecer los criterios básicos necesarios para la gestión del riesgo, definir el alcance y los límites, y establecer una organización adecuada para la gestión del riesgo.
- Valorar el riesgo: consiste en identificar los riesgos, describirlos cuantitativa o cualitativamente y priorizarlos frente a los criterios de evaluación del riesgo y los objetivos relevantes para la organización. Se compone de la identificación, estimación y evaluación del riesgo.
    - Identificación del riesgo: su propósito es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender cómo, dónde y por qué podría ocurrir esta pérdida. Para ello se deben identificar: los activos, las amenazas, los controles existentes, las vulnerabilidades y las consecuencias.
    - Estimación del riesgo: una metodología de estimación puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias; en la práctica, con frecuencia se utiliza, en primer lugar, la estimación cualitativa para obtener una indicación general del nivel del riesgo y revelar los riesgos más importantes, y posteriormente, de ser necesario, se realiza un análisis cuantitativo de los riesgos importantes, dado que es, por lo general, menos complejo y menos costoso realizar un análisis cualitativo que uno cuantitativo.
    - Evaluación del riesgo: consiste en comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.
- Tratamiento del riesgo: consiste en seleccionar controles para reducir, retener, evitar o transferir los riesgos; se debería definir un plan para tratamiento del riesgo.
- Aceptación del riesgo: consiste en tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarlo de manera formal.

CRAMM

Según Qasem (2013), el *CCTA*[1] *Risk Analysis and Management Method* [CRAMM] ofrece un enfoque por etapas, disciplinado, que abarca aspectos técnicos y no técnicos de seguridad; se divide en tres etapas:

1. *Central Communication and Telecommunication Agency*

Identificación de activos y valoración: identifica los activos físicos, el software y los datos que conforman el sistema de información y su ubicación. Los activos físicos se valoran en términos del costo de reposición; los activos de datos y software, en términos del impacto causado si la información no estuviera disponible, fuera destruida, divulgada o modificada.

Evaluación de amenazas y vulnerabilidades: consiste en identificar la probabilidad de que los problemas potenciales se produzcan. CRAMM cubre toda la gama de amenazas, deliberadas o accidentales, que pueden afectar a los sistemas de información.

Selección de contramedidas y recomendaciones: compara la evaluación de los riesgos con el nivel de seguridad requerido, con el fin identificar si los riesgos son lo suficientemente grandes como para justificar la instalación de una contramedida particular.

Magerit

En España, el Consejo Superior de Administración Electrónica (2012) estableció la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Magerit] con el objetivo de implementar un marco común para el análisis y la gestión de riesgos en los sistemas de información, sobre la base de la norma ISO/IEC 27000. Esta metodología propone cuatro etapas:

- Etapa 1: planeación del análisis y la gestión de riesgos: establece las consideraciones necesarias para iniciar el análisis de riesgos y el proyecto de gestión, lo que permite investigar si es apropiado llevarlo a cabo.
- Etapa 2: análisis de riesgos: permite identificar y evaluar los elementos que intervienen en el riesgo para obtener una evaluación del riesgo en las diferentes áreas del dominio y estimar los umbrales de riesgo deseables.
- Etapa 3: gestión de riesgos: permite identificar las salvaguardias potenciales que reducen el riesgo detectado, simulando diferentes combinaciones de las mismas para especificar finalmente las seleccionadas.
- Etapa 4: selección de salvaguardias: permite seleccionar las contramedidas a implementarse, diseñando un enfoque para la aplicación de las salvaguardias seleccionadas. Establece los mecanismos para el seguimiento de su implementación, compila los documentos de trabajo para el análisis de riesgos y el proceso de gestión, obtiene los documentos finales del proyecto y presenta los resultados en los diferentes niveles.

Metodología del NIST para la gestión de riesgos para sistemas de TI

Esta guía del *National Institute of Standards and Technology* [NIST] proporciona las bases para el desarrollo de un programa de gestión de riesgos efectivo que contiene, tanto las definiciones, como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los

CRAMM

According to Qasem (2013), the *CCTA[1] Risk Analysis and Management Method* [CRAMM] provides a phased approach that is disciplined, covering technical and non-technical security aspects. It is divided into three stages:

- Asset identification and assessment: Identifies the physical assets, software and data that comprise the information system and its location. Physical assets are valued in terms of replacement cost; data assets and software, in terms of the impact if the information is not available, was destroyed, disclosed, or modified.
- Assessment of threats and vulnerabilities: Consists in identifying the probability of potential problems occurring. CRAMM covers the entire range of threats, deliberate or accidental, that can affect information systems.
- The selection of countermeasures and recommendations: To compare the risk assessment with the level of security required to identify if the risks are large enough to justify the installation of a special countermeasure.

Magerit

In Spain, the Consejo Superior de Administración Electrónica (2012) established the methodology Analysis and Risk Management Information Systems [Magerit] with the objective of implementing a common framework for analysis and risk management of information systems, based on the ISO/IEC standard 27000. This methodology proposes four stages:

- Stage 1: Planning analysis and risk management: Establishes the necessary considerations to initiate risk analysis and project management, allowing investigation of whether it is appropriate to carry it out.
- Stage 2: Risk analysis: Allows the organization to identify and evaluate the factors involved in the risk, to obtain a risk assessment in different areas of the domain and estimate the desired risk thresholds.
- Stage 3: Risk management: Allows the organization to identify potential safeguards that reduce the risk identified, simulating different combinations thereof, to finally specify the selected option.
- Stage 4: Selection of safeguards: allows selection of countermeasures to be implemented, designing an approach to the application of the selected safeguards. It establishes mechanisms to monitor its implementation, compiles the work documents for risk analysis, and the management process, produces the final project documents, and presents the results at different levels.

NIST Risk Management Methodology for IT systems

This guide by the National Institute of Standards and Technology [NIST] provides the basis for the development of an effective program of risk management, containing both the definitions and the practical guidelines needed to assess and mitigate the risks identified within IT systems. This guide has nine well-defined steps (NIST, 2001):

- Step 1: Characterization of the system: identifies the boundaries of the IT system together with the resources and information that constitute it.
- Step 2: Identification of threats: identifies the threats that can affect the IT system; to determine the probability of a threat, the sources of threats, potential vulnerabilities and existing controls can be considered.
- Step 3: Identification of vulnerabilities: creates a list of vulnerabilities –flaws or weaknesses– of the system, which can be exploited by potential sources of threat.
- Step 4: Analysis of controls: analyzes the implemented controls, or those which the organization plans to implement, whether they are for prevention –to prevent attempts to violate security policies and including execution control, encryption and authentication– or detection –that warn of violations or attempted violations of security policies, and include audits of tracking, intrusion detection methods and error control.
- Step 5: Determination of probability: to obtain the probability that a potential vulnerability can be exploited by an associated threat, the following factors can be considered: motivation and capability of the source of threat, the nature of the vulnerability and the existence and effectiveness of current controls.
- Step 6: Impact analysis: consists of measuring the level of risk to determine the adverse impact resulting from the successful exploitation of a vulnerability by a threat; the adverse impact on a security system can be described in terms of the loss or degradation of one or a combination of the following security objectives: integrity, availability and confidentiality.
- Step 7: Risk assessment: consists of evaluating the risk level of the IT system; risk assessment for a particular threat/vulnerability pair can be expressed in terms of: the probability that an attempted threat can exploit a particular vulnerability; the magnitude of the impact when a threat successfully exploits a vulnerability; and the adequacy of security controls, planned or existing, to reduce or eliminisistemas de TI (Tecnologías de Información). Esta guía tiene nueve pasos definidos así (NIST, 2001):

- Paso 1: caracterización del sistema: identifica los límites del sistema TI, junto con los recursos y la información que lo constituyen.
- Paso 2: identificación de amenazas: identifica las amenazas que pueden afectar el sistema TI; para determinar la probabilidad de una amenaza, se pueden considerar las fuentes de amenaza, las vulnerabilidades potenciales y los controles existentes.
- Paso 3: identificación de vulnerabilidades: crea una lista de las vulnerabilidades –fallas o debilidades– del sistema, que pueden ser explotadas por las fuentes potenciales de amenaza.
- Paso 4: análisis de controles: analiza los controles implementados o que planea implementar la organización, sean preventivos –que evitan los intentos de violar las políticas de seguridad e incluyen el control de ejecución, el cifrado y la autenticación– o de detección –que alertan sobre violaciones o intentos de violaciones de las políticas de seguridad e incluyen auditorías de rastreo, métodos de detección de intrusión y control de errores–.
- Paso 5: determinación de la probabilidad: para obtener la probabilidad de que una vulnerabilidad potencial pueda ser explotada por una amenaza asociada, se pueden considerar los siguientes factores: motivación y capacidad de la fuente de amenaza, naturaleza de la vulnerabilidad, y existencia y efectividad de los controles actuales
- Paso 6: análisis del impacto: consiste en medir el nivel de riesgo para determinar el impacto adverso que resulta de la explotación exitosa de una vulnerabilidad por una amenaza; el impacto adverso de un sistema de seguridad puede describirse en términos de la pérdida o degradación de uno o de una combinación de los siguientes objetivos de seguridad: integridad, disponibilidad y confidencialidad.
- Paso 7: determinación de riesgos: consiste en evaluar el nivel de riesgo del sistema TI; la determinación del riesgo para una pareja particular amenaza/vulnerabilidad puede ser expresada en función de: la probabilidad de que un intento de amenaza dado explote una determinada vulnerabilidad; la magnitud del impacto cuando una amenaza explota exitosamente una vulnerabilidad; y la idoneidad de los controles de seguridad planeados o existentes para reducir o eliminar los riesgos. Se debe obtener: la medida del riesgo, la escala del riesgo y la matriz de nivel del riesgo.
- Paso 8: recomendaciones de control: determina los controles que pueden mitigar o eliminar los riesgos identificados. Los siguientes factores deberían considerarse al recomendar controles: efectividad de las opcio-

nes recomendadas (es decir, compatibilidad del sistema), legislación y regulación, política organizacional, impacto operacional, y seguridad y confiabilidad.

- Paso 9: documentación de resultados: Los resultados deben ser documentados en un reporte oficial o instrucciones; un reporte de evaluación de riesgos es un reporte de gestión que ayuda a la alta gerencia a tomar decisiones respecto de las políticas, los procedimientos, el presupuesto y los cambios en el sistema operacional y de gestión.

Metodología del BID para el diagnóstico, la prevención y el control de la corrupción en programas de seguridad ciudadana

Esta metodología parte de la correlación entre la seguridad ciudadana y la corrupción, y se basa en el análisis de la cadena de valor; se identifican los procesos que aportan más a la generación de valor en una organización o programa, para lo cual se dividen en dos tipos: actividades primarias o críticas –que contribuyen directamente a la creación de valor–, y actividades administrativas o de soporte –que sustentan el desarrollo de las actividades primarias–.

Los macro-procesos críticos de la cadena de valor de la seguridad ciudadana son (García-Mejía, 2010):

- Desarrollar políticas de seguridad: articular la respuesta pública a las demandas y necesidades sociales de seguridad ciudadana.
- Prevenir la violencia: contrarrestar los factores multidimensionales que aumentan los riesgos de criminalidad y victimización.
- Controlar y sancionar: asegurar el respeto de la ley y el orden público, proteger a las personas y bienes ante la amenaza de delitos, de ser el caso, aplicando las consecuencias jurídicas derivadas del incumplimiento de la ley.
- Rehabilitar y reinsertar en la sociedad: tratar y rehabilitar a la población reclusa o a menores de edad que han infringido la ley (prevención terciaria) para su reinserción social, así como a las víctimas de delitos.
- Supervisar y evaluar las políticas: monitorear, supervisar y evaluar el cumplimiento de la misión, los objetivos y las metas establecidas en los planes y actividades de manera ordenada y eficiente.

Cada uno de estos macro-procesos implica llevar a cabo los siguientes pasos (García-Mejía, 2010):

- Identificación y análisis de los riesgos: identificar los riesgos de cada uno de los principales procesos, así como su nivel, entendido éste como la probabilidad de ocurrencia y el impacto que generaría en caso de materializarse; el impacto del riesgo varía en cada proyecto, por lo que debe ser analizado, caso por caso.
- Respuesta a los riesgos: identificar un abanico de alternativas de respuesta a los riesgos identificados; se puede

nate risks. The risk measure, the scale of risk and level of risk matrix must be obtained.

- Step 8: Control recommendations: determines the controls that can mitigate or eliminate the identified risks. For the recommendation of controls the following controls should be considered: effectiveness of the recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability.
- Step 9: Documentation of results: results should be documented in an official report or instructions; a risk assessment report is a management report that helps senior management to make decisions on policies, procedures, budget and changes in the operational and management system.

IDB Corruption Diagnosis, Prevention and Control in Programs of Civic Security Methodology

This methodology is based on the correlation between citizens' security and corruption, and on the analysis of the value chain; the processes that contribute most to the generation of value in an organization or program are identified, and divided into two types: critical or primary activities –that contribute directly to the creation of value–, and administrative activities or support –supporting the development of primary activities.

The critical macro-processes of the value chain of public safety are (García-Mejía, 2010):

- Develop security policies: Orchestrating the public response to the demands and social needs of public safety.
- Violence prevention: Counteract the multi-dimensional factors that increase the risk of crime and victimization.
- Control and sanction: Ensure compliance with the law and public order, protect people and assets against the threat of crime, applying, if appropriate, the juridical consequences due to breach of law.
- Rehabilitate and reintegrate into society: Treat and rehabilitate the prison population or minors who have infringed the law (tertiary prevention) for their social reintegration, as well as victims of crime.
- Monitor and evaluate policies: Monitor, supervise, and evaluate the achievement of the mission, objectives and goals set in plans and activities in an orderly and efficient manner.

Each of these macro-processes involves performing the following steps (García-Mejía, 2010):

- Identification and analysis of risks: To identify the risks of each of the main processes as well as its level, understand this as the probability of occurrence and the impact that would be generated if it is materialized; the impact of risk on each project varies, and should therefore be analyzed case by case.
- Risk response: Identifying a range of possible responses to the identified risks; one or a combination of actions able to give an effective response to the identified risks can be selected; to accomplish this response to the risks, consideration is given to the dimensions of analysis and a review of the available alternatives.

Two dimensions of analysis were taken into account: The risk responses that can be transversal and specific, and strategic categories of risk response suggested by the Project Management Institute [PMI] (2008), mainly to avoid and mitigate.

In some cases, the risk responses are generated by reforms to other processes of the value chain, and not directly to the process at risk, since the source of risk is another process.

Concerning the review of the available alternatives, the fight against corruption can be not only or primarily an effort to identify and punish the corrupt, which in any case is necessary and essential, but to identify patterns of corruption, that is, the most vulnerable areas, and its main manifestations, in order to modernize institutional management to reduce the individual discretion of public servants, make their actions transparent and hold them accountable for their acts (Campos & Pradhan, 2007).

NIST Malware Incident Prevention Methodology

In this methodology, the NIST considers that the four main elements of prevention are (Mell et al., 2005):

- Policies: Policies aimed at preventing malware are the basis for implementing preventive controls. If an organization does not clearly establish malware prevention considerations into their policies, it is improbable that they will be able to perform malware prevention activities consistently and effectively along the organization. Policies related to malware prevention should be as wide as possible to provide flexibility in their implementation and reduce the need for frequent updates, as well as being sufficiently specific in order that their purpose and scope are clear.
- Awareness: Establish and maintain general programs of raising awareness about malware for all users, as well as specific training programs about raising awareness for IT staff directly involved in incident prevention activities, this being critical to reduce the number of incidents that occur

seleccionar una o una combinación de acciones capaz de dar una respuesta efectiva a los riesgos identificados; para llevar a cabo esta respuesta a los riegos se consideran: las dimensiones de análisis y la revisión de las alternativas disponibles.

Se tuvo en cuenta dos dimensiones de análisis: las respuestas a los riesgos, que pueden ser transversales y específicas, y las categorías estratégicas de respuesta a los riesgos sugeridas por el Project Management Institute [PMI] (2008), principalmente evitar y mitigar.

En algunos casos las respuestas a los riesgos pasan por introducir reformas a otros procesos de la cadena de valor, no directamente al proceso en riesgo, pues el origen del riesgo está en otro proceso.

En cuanto a la revisión de las alternativas disponibles, la lucha contra la corrupción no puede ser solo ni principalmente un esfuerzo para identificar y castigar a los corruptos, lo que en cualquier caso es necesario e imprescindible, sino por identificar los patrones de la corrupción, esto es, sus áreas más vulnerables y sus principales manifestaciones, con el propósito de modernizar la gestión institucional para reducir la discrecionalidad de los servidores públicos, transparentar su actuación y hacerlos responsables de sus actos (Campos & Pradhan, 2007).

Metodología de prevención de incidentes de malware del NIST

En esta metodología, el NIST considera que los cuatro elementos principales de la prevención son (Mell et al., 2005):

- Políticas: las políticas dirigidas a la prevención del malware son la base para implementar controles preventivos. Si una organización no establece claramente las consideraciones de prevención del malware en sus políticas, es improbable que lleve a cabo actividades de prevención del malware consistentes y efectivas a lo largo de la organización. Las políticas relacionadas con la prevención del malware deben ser tan generales como sea posible para proveer flexibilidad en su implementación y reducir la necesidad de frecuentes actualizaciones de las mismas, pero también deben ser lo suficientemente específicas para que su propósito y alcance sean claros.
- Concientización: establecer y mantener programas generales de concientización sobre el malware para todos los usuarios, así como programas de entrenamiento específico en concientización para el personal de TI directamente involucrado en las actividades de prevención de incidentes, es crítico para reducir el número de incidentes que ocurre por errores humanos. Todos los usuarios de una organización deberían ser conscientes de: las maneras en que entra el malware a los sistemas, los infecta y se expande; los riesgos que supone el malware; la inhabilidad de los controles técnicos para prevenir todos los incidentes y la importancia de que los usuarios prevengan estos incidentes.

- Mitigación de vulnerabilidades: invertir esfuerzos en la mitigación de vulnerabilidades puede eliminar algunos posibles vectores de ataque. Debido a los desafíos que presenta la mitigación de vulnerabilidades, incluyendo el continuo descubrimiento de nuevas vulnerabilidades, las organizaciones deben tener documentadas las políticas, los procesos y los procedimientos para la mitigación de vulnerabilidades, y deberían también considerar la creación de un programa de gestión de vulnerabilidades que ayude en las tareas de mitigación. También se deben evaluar constantemente las vulnerabilidades, para que las tareas de mitigación sean priorizadas apropiadamente.
- Mitigación de amenazas: implementar una combinación de técnicas y herramientas de mitigación de amenazas, como software antivirus y cortafuegos, puede prevenir las amenazas que atacan exitosamente los diferentes sistemas y redes. Las organizaciones deben realizar la mitigación de amenazas para detectar y parar el malware antes de que afecte a sus objetivos.

Las organizaciones deben crear una guía de recomendaciones para cada categoría a fin de crear una defensa en capas efectiva contra el malware. Sin embargo, las organizaciones deben ser conscientes de que, sin importar el esfuerzo que pongan en la prevención de incidentes de malware, los incidentes aún ocurrirán –por ejemplo, por tipos de amenaza desconocidos, errores humanos, etc.– (Mell et al., 2005).

IV. Aspectos a comparar

Ya que se van a comparar diferentes metodologías, se va a establecer un paralelo entre las fases o pasos que estas incluyen. Se han identificado cuatro fases básicas, que se repiten en casi todas ellas:

- Establecer el contexto: identificar los activos importantes para la organización, los requisitos de seguridad de esos activos, lo que la organización está haciendo para protegerlos, y los objetivos que se persiguen con el análisis de riesgos.
- Identificar los riesgos: determinar qué vulnerabilidades poseen los diferentes activos e identificar las amenazas que pueden explotarlas.
- Analizar los riesgos: calcular la probabilidad de que una amenaza explote una determinada vulnerabilidad y establecer el nivel de riesgo de cada activo, priorizándolos para tomar acciones posteriores.
- Tratar los riesgos: implantar contramedidas que permitan evitar, mitigar, aceptar o transferir los riesgos.

La comparación va a consistir en determinar si las diferentes metodologías incluyen estas fases y establecer si se enfocan en una fase determinada o si especifican claramente lo que se hace en cada una de ellas. También se va a determinar si estas metodologías consideran el factor humano dentro de sus diferentes pasos, ya que el ser humano es el eslabón más débil de la cadena de la seguridad.

due to human error. All users in an organization should be conscious of: the ways in which malware enters, infects and expands in systems; the risks involved in malware; the inability of technical controls to prevent all incidents, and the importance of users avoiding such incidents.

- Vulnerabilities mitigation: Investing efforts in the mitigation of vulnerabilities can eliminate some possible attack vectors. Due to the challenges posed by mitigating vulnerabilities, including the continual discovery of new vulnerabilities, organizations must have documented policies, processes and procedures for mitigating vulnerabilities, and they should also consider creating a vulnerability management program to assist in the mitigation tasks. Also, vulnerabilities must be constantly evaluated, in order that mitigation tasks are prioritized appropriately.
- Threat mitigation: Implementing a combination of techniques and threat mitigation tools, such as antivirus software and firewalls, can successfully prevent threats that attack the different systems and networks. Organizations should perform threat mitigation to detect and stop malware before it affects their objectives.

Organizations must create a guide with recommendations for each category in order to create an effective layered defense against malware. However, organizations should be aware that, regardless of the effort put into preventing malware incidents, incidents will still take place – for example, by unknown types of threats, human error, etc. (Mell et al., 2005).

IV. Aspects to compare

Since different methodologies will be compared, a comparison between the phases or steps that include these should be established. Four basic steps that are repeated in almost all of them have been identified:

- Set the context: Identify important assets for the organization, the security requirements of these assets, what the organization is doing to protect them, and the objectives pursued with risk analysis.
- Identify risks: Determine which vulnerabilities the different assets have and identify threats that can exploit them.
- Analyze risks: Calculate the probability that a threat will exploit a particular vulnerability and establish the level of risk of each asset, and prioritize them for taking action in response.
- Deal with risks: Implement countermeasures to avoid, mitigate, accept or transfer risks.

Metodología...	De gestión de riesgos							De Prevención de Riesgos	
Item	OCTAVE (Phases)	CORAS (Steps)	Australian St (Phases)	NTC – ISO/ IEC 27005 (Steps)	CRAMM (Stages)	MAGERIT (Stages)	NITS (Steps)	BID (Steps)	NIST (core elements)
Establishment of the context/ *Establecer el contexto*	1	1, 2, 3	1	1	1	1	1	N/A	N/A
Identify risks/ *Identifica los riesgos*	1 y 2	4	2	2	2	2	2, 3, 4	1	N/A
Analyze risks/ Analizar los riesgos	3	5 y 6	3 y 4				5, 6, 7		N/A
Manage risks/ *Tratar los riesgos*		7	5	3 y 4	3	3 y 4	8 y 9	2	4

Table 2. Comparison of methodologies / Comparación de metodologías

The comparison will be to determine whether the different methodologies include these phases and establish if they focus on a particular stage or if they specify clearly what is done in each one; also to determine whether these methodologies consider the human factor in the different steps, since the human being is the weakest link in the security chain.

V. Comparison of Methodologies

Table 2 compares the different methodologies described, indicating whether they include the phases identified in section IV of this article.

As shown in **Table 2**, the Octave methodology, while including the four phases that are defined for this analysis, does not present a strict division of them. Octave focuses mainly on the first phase, where the knowledge and safety practices of senior management, operational and staff are identified, and so builds the different profiles of threats; therefore, at this stage it takes into account the human factor. Risk identification is carried out in the first and second phases of Octave, because in the first phase it establishes the threats profiles and in the second identifies vulnerabilities. However, to determine in the first instance the threats and then the vulnerabilities, the correspondence between these is not clear, given that the identification of which threats can exploit a particular vulnerability must be done; at this stage of risks identification, the human factor is not explicitly considered, but rather the assets of the organization. The third phase of Octave includes both the analysis and treatment of risks and takes into account the human factor, because in its processes it includes risk analysis of behavior and promotes the protection strategy in the organization. However, specific protection and prevention strategies are not established.

The CORAS methodology is based on the realization of a series of meetings and workshops for different purposes, according to the step that is being performed. As shown in Table 2, this

V. Comparación de metodologías

En la **Tabla 2** se muestra el cuadro comparativo de las diferentes metodologías descritas, indicando si incluyen las fases identificadas en la sección IV de este artículo.

Como se puede apreciar en la **Tabla 2**, la metodología Octave, aunque incluye las cuatro fases que se han definido para este análisis, no presenta una división estricta de ellas. Octave se centra principalmente en su primera fase, donde se identifica primero el conocimiento y prácticas de seguridad de la alta gerencia, del área operacional y del personal, para construir posteriormente los diferentes perfiles de amenazas; por tanto, en esta fase se tiene en cuenta el factor humano. La identificación de riesgos, se lleva a cabo en la primera y segunda fase de Octave, porque en la primera fase establece los perfiles de amenazas y en la segunda identifica las vulnerabilidades, sin embargo, al determinar primero las amenazas y luego las vulnerabilidades, no queda claro la correspondencia entre estas, pues se debe identificar qué amenazas pueden explotar una determinada vulnerabilidad; en esta fase de identificación de los riesgos no se considera explícitamente el factor humano sino los activos de la organización. La tercera fase de Octave incluye, tanto el análisis, como el tratamiento de los riesgos, y tiene en cuenta el factor humano, porque en sus procesos hace un análisis de riesgos de conducta y fomenta la estrategia de protección en la organización, sin embargo, no se establecen estrategias específicas de protección y prevención.

En cuanto a la metodología CORAS, esta se basa en la realización de una serie de reuniones y talleres con diferentes fines, de acuerdo con el paso que se esté realizando. Como se aprecia en la Tabla 2, esta metodología incluye las cuatro fases consideradas en este análisis. La fase de establecimiento del contexto, se lleva a cabo en los tres primeros pasos de CORAS, en este caso, los analistas se basan en la información proporcionada por los representantes del cliente, por lo que no son ellos los que reúnen directamente la información que requieren de la empresa, lo que puede llevar a no contar con toda la información necesaria para realizar un análisis de riesgos completo; sin embargo, se hacen en

esta primera fase tres reuniones para asegurar la completa y adecuada comprensión de la información presentada por el cliente. La fase de identificación de riesgos, se lleva a cabo en el cuarto paso, donde se identifican las vulnerabilidades y los diferentes escenarios de amenaza a través de un taller con expertos en el objeto de análisis. La fase de análisis de riesgos, se lleva a cabo en los pasos 5 y 6, donde se obtienen los valores de probabilidad y un cuadro de riesgos general. La fase de tratamiento de riesgos, se lleva a cabo en el séptimo paso, donde se determina qué tratamiento se va a dar a los riegos y se hace un análisis costo/beneficio. Ya que los analistas no tienen un contacto directo con el personal de la empresa cliente, esto puede llevar a descuidar el factor humano y a tener una visión errada de los procesos y de las prácticas de seguridad que se llevan a cabo en ella, obteniendo resultados que pueden no adaptarse al contexto real de la empresa. No se establecen estrategias específicas de protección y prevención.

Según la **Tabla 2**, la metodología de administración de riesgos del estándar australiano incluye las cuatro fases consideradas en este análisis. Esta metodología se centra en las fases de identificación y análisis de riesgos, donde se incluyen todos los riesgos (estén o no bajo el control de la organización) y se analizan las fuentes y consecuencias de los mismos para calcular luego su probabilidad y establecer su nivel, de acuerdo con un análisis, tanto cualitativo, como cuantitativo. Sin embargo, el establecimiento del contexto se hace teniendo en cuenta el contexto estratégico, organizacional y de administración de riesgos, por lo que no se centra en el factor humano, sino en los objetivos que quiere alcanzar la organización; tampoco se definen estrategias específicas de protección y prevención en la fase de tratamiento de los riesgos, aunque si se establece un proceso cíclico de tratamiento de los mismos, lo que permite verificar si las contramedidas implementadas tienen el efecto esperado o si deben reemplazarse por otras.

La metodología de gestión de riesgos NTC-ISO /IEC 27005 incluye las cuatro fases consideradas en este análisis, pero no menciona específicamente el factor humano, pues sus pasos se describen de manera muy general. Esta metodología tiene un interés particular en la valoración del riesgo donde se realiza la identificación, estimación y evaluación del mismo.; ya que la eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, si la información que arroja este paso no es suficiente, se llevan a cabo tantas iteraciones como sean necesarias de valoración del riesgo con un contexto revisado, para poder realizar un tratamiento adecuado. Además, no se definen estrategias específicas de protección y prevención en el paso de tratamiento del riesgo.

El método de análisis CRAMM, aunque incluye las cuatro fases consideradas en este análisis, es bastante general y no se centra en ninguna de estas fases; tampoco habla específicamente del factor humano ni define estrategias específicas de protección y prevención. La etapa de identifi-

methodology includes the four phases considered in this analysis. The phase of establishing the context takes place in the first three steps of CORAS. In this case, analysts depend on information provided by representatives of the customer, so they do not directly gather the information required from the company, which may mean that not all the information necessary to perform a full risk analysis is available. However, three meetings are held in this first phase to ensure full and proper understanding of the information presented by the client. The risk identification phase is carried out in the fourth step, where different vulnerabilities and threat scenarios are identified, through a workshop with experts on the object of analysis. The risk analysis phase is carried out in steps 5 and 6, where the probability values and a picture of the overall risk are obtained. The phase of risk treatment is carried out in the seventh step, where it is determined how the risks will be handled, and a cost/benefit analysis is performed. Since the analysts have no direct contact with the staff of the client company, this can lead to neglect of the human factor and a mistaken view of the processes and safety practices that are carried out, yielding results that are possibly not related with the actual context of the company. No specific protection and prevention strategies are set.

According to **Table 2**, the risk management methodology of the Australian Standard includes the four phases considered in this analysis. This methodology focuses on the phases of identification and risk analysis, where all risks are included (whether or not under the control of the organization) and the sources and consequences of these are analyzed, after which the probability is calculated, and their levels are established, according to an analysis in both qualitative and quantitative terms. However, the establishment of the context is performed according to the strategic, organizational and risk management context, so it does not focus on the human factor, but rather on the objectives that the organization wants to achieve. The treatment phase of the risks does not define specific strategies for protection and prevention, even if a cyclical process of treatment of the same is established, and thus does not allow a verification that the implemented countermeasures have the desired effect or whether they should be replaced by others.

The risk management methodology NTC-ISO / IEC 27005 includes the four phases considered in this analysis, but does not specifically mention the human factor, because the steps are described in very general terms. This methodology is particularly interested in the risk assessment, with identification, estimation and evaluation of the risk; since the efficacy of the risk treatment depends on the results of the risk assessment, if the information obtained in this step is not sufficient, iterations are carried out as

necessary of the risk assessment with a revised context, to ensure appropriate treatment. In addition, no specific protection and prevention strategies are defined in the risk treatment step.

The CRAMM analysis method, though including the four phases considered in this analysis, is rather general and does not focus on any of these phases, and does not speak specifically of the human factor or define specific strategies for protection and prevention. The asset identification and evaluation stage of CRAMM focuses only on physical assets and information, although at the stage of assessing threats and vulnerabilities it affirms that all deliberate and accidental threats are considered, which could imply the human factor.

The Magerit methodology is also very general in the description of its stages, though it includes the four phases considered in this analysis. In the planning stage of analysis and risk management it does consider human resources, but in carrying out risk analysis it does not speak of the human factor in the organization. In addition, in the analysis stage of risk it does not specify what types of threat are considered, or the process of identifying desirable risk thresholds. Magerit focuses mainly on the stage of risk management which simulates different combinations of safeguards in order to select those that best fit the context of the organization, and then, at the stage of selecting safeguards, monitors the implementation of these safeguards, documenting and disclosing them at different levels of the organization. Thus, at least at this stage, it takes into account the human factor. Magerit does not define specific strategies for protection and prevention.

The NIST methodology of risk management is perhaps the most complete methodology of all those studied, because it includes the four phases considered in this analysis and provides definitions such as the practical guidance needed to assess and mitigate the risks identified in IT systems, and consequently describes in a very precise way what to do in each of its nine steps. This methodology also considers the human factor, taking into account the motivation of the different sources of threats, which helps determine the likelihood of risk. It also considers preventive and corrective controls.

Methodologies for risk prevention provide an overview focused on risk analysis and especially on the treatment of these same risks. The IDB methodology for the diagnosis, prevention and control of corruption in citizen security programs, although not oriented to IT systems, is very interesting for this study because it focuses on the human factor, considering the chain value of the different processes that are carried out in an organization, as well as the individual, institutional and social responsibilities at the time of implementing preventive controls. In this methodology the identification and analysis of risk is performed mainly in

cación de activos y valoración de CRAMM se centra solo en los activos físicos y de información, aunque en la etapa de evaluación de amenazas y vulnerabilidades si dice que se consideran todas las amenazas deliberadas o accidentales, lo que podría tener implícito el factor humano.

La metodología Magerit es también bastante general en la descripción de sus etapas, aunque incluye las cuatro fases consideradas en este análisis. En la etapa de planeación del análisis y gestión de riesgos considera los recursos humanos pero para llevar a cabo el análisis de riesgos, no habla en sí del factor humano de la organización. Además, en la etapa de análisis de riesgos no se especifica qué tipos de amenaza se consideran ni cómo se determinan los umbrales de riesgo deseables. Magerit se centra principalmente en la etapa de gestión de riesgos donde simula diferentes combinaciones de salvaguardias para seleccionar las que más se acomoden al contexto de la organización, y luego, en la etapa de selección de salvaguardias, hace un seguimiento a la implementación de estas salvaguardias, las documenta y las da a conocer en los diferentes niveles de la organización, así que, por lo menos en esta etapa, tiene en cuenta el factor humano. Magerit no define estrategias específicas de protección y prevención.

La metodología de gestión de riesgos del NIST es quizás la metodología más completa de todas las estudiadas, ya que incluye las cuatro fases consideradas en este análisis y proporciona, tanto las definiciones, como las orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de TI, por lo que describe de una manera muy precisa lo que se debe hacer en cada uno de sus nueve pasos. Esta metodología también considera el factor humano, pues tiene en cuenta la motivación de las diferentes fuentes de amenazas, lo que ayuda a determinar la probabilidad del riesgo; además, considera los controles preventivos y correctivos.

Las metodologías de prevención de riesgos ofrecen un panorama centrado en el análisis de riesgos y sobretodo en el tratamiento de los mismos. La metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del BID, aunque no es una metodología orientada a los sistemas de TI, es muy interesante para este estudio, pues se centra en el factor humano, considerando la cadena de valor de los diferentes procesos que se llevan a cabo en una organización y las responsabilidades individuales, institucionales y sociales, a la hora de implementar los controles preventivos. En esta metodología la identificación y el análisis de los riesgos se hacen de manera más cualitativa que cuantitativa, mientras en la respuesta a los riesgos se consideran varias dimensiones de análisis y se revisan las alternativas disponibles.

La metodología de prevención de incidentes de malware del NIST, por su parte, incluye solamente la fase del tratamiento de los riesgos, estableciendo los cuatro elementos principales de la prevención: las políticas, la concientización, la mitigación de vulnerabilidades y la mitigación de

amenazas. En la concientización es donde incluye el factor humano, y describe los aspectos a tener en cuenta para implementar los cuatro elementos de prevención.

IV. Conclusiones

De las siete metodologías de gestión de riesgos estudiadas, solo tres consideran el factor humano (Octave, Magerit y la metodología de gestión de riesgos del NIST) y cuatro no lo consideran de manera explícita (CORAS, la metodología del estándar australiano, la NTC-ISO/IEC 27005 y CRAMM). Por su parte, las metodologías de prevención de riesgos estudiadas si consideran el factor humano, principalmente la de diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana del BID. Como se determinó en la introducción de este artículo, el que estas metodologías consideren el factor humano es muy importante, pues son los seres humanos el eslabón más débil en la cadena de la seguridad.

De las metodologías de gestión de riesgos, la más completa es la metodología de gestión de riesgos del NIST, ya que incluye las cuatro fases consideradas en este análisis y proporciona las definiciones y orientaciones prácticas necesarias para evaluar y mitigar los riesgos identificados en los sistemas de TI. Sin embargo, sería bueno complementar el análisis de riesgos que realiza, teniendo en cuenta las responsabilidades individuales, institucionales y sociales, como lo hace la metodología citada del BID, lo que podría llevar a implementar estrategias de prevención más completas y efectivas.

Por otra parte, la Metodología de Prevención de Incidentes de Malware del NIST, especifica los cuatro elementos principales de la prevención, brindando una buena guía sobre los aspectos a considerar a la hora de implementar estrategias de prevención.

Aunque las metodologías de prevención de riesgos estudiadas no incluyen las cuatro fases consideradas en este análisis, si sería bueno que lo hicieran, puesto que del establecimiento adecuado del contexto y del análisis completo de los riesgos existentes van a derivarse las diferentes estrategias de prevención a implantar.

Finalmente, se puede concluir que una metodología de prevención de riesgos completa debería combinar los aspectos destacables de las diferentes metodologías estudiadas. S&T

a qualitative rather than quantitative way, while in the response to the risks, several dimensions of analysis are considered, and the available alternatives are reviewed.

The NIST methodology of malware incident prevention, meanwhile, includes only the phase of risk treatment, establishing the four main elements of prevention: policies, awareness, mitigation of vulnerabilities and threat. It is in the awareness that the human factor is included, describing aspects to consider for implementing the four elements of prevention.

VI. Conclusions

Of the seven risk management methodologies studied, only three consider the human factor (Octave, Magerit, and the NIST's risk management methodology) and four do not consider it explicitly (CORAS, Australian Standard methodology, NTC ISO/IEC 27005 and CRAMM). Meanwhile, of the methodologies of risk prevention studied, the human factor is considered mainly in the diagnosis, prevention and control of corruption in the public safety programs of the IDB. As determined in the introduction to this article, the fact that these methodologies consider the human factor is very important because humans are the weakest link in the security chain.

Of the methodologies of risk management, the most complete is the NIST methodology because it includes the four phases considered in this analysis and provides the definitions and practical guidance needed to assess and mitigate the risks identified in IT systems. However, it would be good to complement the risk analysis performed by taking into account the individual, institutional and social responsibilities, as does the aforementioned IDB methodology, which could lead to prevention strategies that are more complete and effective.

On the other hand, the NIST methodology of malware incident prevention specifies the four main elements of prevention, providing a good guide on aspects to consider at the time of implementing prevention strategies.

Although the methodologies of risk prevention studied did not include the four phases considered in this analysis, it would be good to include these, because the appropriate establishment of context and comprehensive analysis of the risks will make it possible to derive different prevention strategies to be implemented.

Finally, we can conclude that a complete risk prevention methodology should combine the highlights of the different methodologies studied. S&T

References / Referencias

Alberts, C., & Dorofee, A. (2001). *An introduction to the octave method.* Pittsburg, PA: Carnegie Mellon University.

AS/NZS 4360:1999 -Estándar Australiano, Administración de Riesgos. (1999). Retrieved form: http://www.bcu.gub.uy/Acerca-de-BCU/Concursos/Est%C3%A1ndar%20Australiano_Adm_Riesgos.pdf

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437- 444.

Boge, K. (2001). *A platform for risk analysis of security critical systems* (CORAS. IST-2000-25031). Oslo, Norway: Norsk_ Regnesentral.

Brantingham, P. J. & Faust, F. L. (1976). A conceptual model of crime prevention. *Crime and Delinquency, 22*(3), 284-296.

British Standards Institution [BSI]. (1991). *Quality vocabulary* (No. BS4778 [Part 3 Section 3.2 = IEC 1990 50(191)]). London, UK: BSI.

British Standards Institution [BSI]. (1999). BS7799-2. *Information security management -part 2: specification for information security management systems*. London, UK: BSI.

Campos, E. & Pradhan, S. (2007). *The many faces of the corruption: tracking vulnerabilities at the sector level*. Washington DC: World Bank.

Carnegie Corporation. (1957). *Carnegie Commission on Preventing Deadly Conflict. Final report with executive summary*. New York, NY: Carnegie Corporation.

Concha-EastMan, A. (2004). Violencia urbana en América Latina y el Caribe: dimensiones, explicaciones, acciones. In S. Rotker (Ed.), *Ciudadanías del miedo* (pp. 39-53.). Caracas, Venezuela: Rutgers.

Consejo Superior de Administración Electrónica (2012). MAGERIT versión 3. Metodología de análisis y gestión de riesgos de los sistemas de información.. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Díaz-Aguado, M. J., Martínez-Arias, R., & Martín-Seoane, G. (2004). Prevención de la violencia y lucha contra la exclusión desde la adolescencia. In *Volumen uno: La violencia entre Iguales en la escuela y en el ocio. estudios comparativos e instrumentos de valuación.* Madrid, España: Instituto de la Juventud.

Douglas, M. (1990). Risk as a forensic resource. Daedalus, 119(4). Retrieved from: http://www.jstor.org/stable/20025335

Ekblom, P. (2003). *The conjunction of criminal opportunity: a framework for crime reduction.* London, UK: Home Office Crime and Policing Group.

Frosdick, S. (1997). The techniques of risk analysis are insufficient in themselves. *Disaster Prevention and Management, 6*(3), 165-177.

García-Mejía, M. (2010). *Metodología para el diagnóstico, prevención y control de la corrupción en programas de seguridad ciudadana* (No. Documento de Debate #IDB-DP-117). Washington, DC: Banco Interamericano de Desarrollo (BID).

García-Ospina, C. & Tobón-Correa, O. (2000). Promoción de la salud, prevención de la enfermedad, atención primaria en salud y plan de atención básica. ¿Qué los acerca? ¿Qué los separa? *Hacia Promoción de la Salud, 5,* 7-21.

Gerber, M., & Von Solms, R. (2005). Management of risk in the information age. *Computer & Security, 24*, 16-30.

Graham, J., & Bennett, T. (1995). *Crime prevention strategies in Europe and North America* (Vol. 28). Helsinki-New York: European Institute for Crime Prevention and Control.

Hayden, C., & Blaya, C. (2001). Violence et comportements agressifs dans les écoles anglaises. In E. Debarbieux & C. Blaya (Eds.), *La violence en millieu scolaire-3- dix approaches en Europe* (pp. 43-70.). Paris, France: ESF.

Huerta, A. (2012, April 2). Introducción al análisis de riesgos - metodologías (II) [blog security artwork]. Retrieved from: http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/

ISO/IEC_TR_13335-1. (1996). *Information technology - guidelines for the management of it security - part 1: concepts and models for it security* (1st ed.). Geneva, Switzerland: ISO/IEC.

Kailay, M. P., & Jarratt, P. (1995). RAMeX: a prototype expert system for computer security analysis and management. *Computers and Security, 14,* 449-463.

Khan-Pathan, A.S. (2010). *The state of the art in intrusion prevention and detection*. Kuala Lumpur, Malaysia: CRC.

Kirkwood, A. S. (1994). Why do we worry when scientists say there is no risk? *Disaster Prevention and Management, 3*(2), 15- 22.

Knepper, P. (2007). *Criminology and social policy*. London, UK: Sage.

Martínez, F., & Ruiz, J. (2001). *Manual de gestión de riesgos sanitarios*: Madrid, Spain: Diaz De Santos.

Mell, P., Kent, K., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling*. Gaithersburg, MD: NIST.

Moses, R. H. (1992). Risk analysis and management. In K. M. Jackson & J. Hruska (Eds.), *Computer security reference book*. Oxford, UK: Butterworth-Heinemann.

National Institute of Standards and Technology [NIST]. (1995). *An introduction to computer security*. Washington DC: US Department of Commerce.

National Institute of Standards and Technology [NIST]. (2001). *Risk management guide for information technology systems*. Washington DC: US Department of Commerce.

NTC-ISO/IEC 27005: Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la Información. Bogotá, Colombia: ICONTEC.

Owens, S. (1998). *Information security management: an introduction*. London, UK: British Standards Institution.

Peyre, V. (1986). Introduction: elements d'un debat sur la prévention de la delinquance. *Annales de Vaucresson, 1*(24), 9-13.

Piper, S. (2011). *Intrusion detection systems for dummies*. Hoboken, NJ: Wiley.

Project Management Institute [PMI]. (2008). *A guide to the project management body of knowledge (PMBOK Guide)* (4ta ed.). Newtown Square, PA: PMI.

Qasem, M. (2013). Information technology risk assessment methodologies: current status and future directions. *International Journal of Scientific & Engineering Research, 4*(12), 966-972.

Ragmognino, N., FradJi, D., Soldini, F., & Vergés, P. (1997). L'École comme dispositive simbolique et les violences: le example de trois ecoles em Marseille. In B. Charlot & J. C. Émin (Eds.), *Violences à l'école - État des Savoirs.* Paris, France: Masson & Armand Colin.

Royal Society. (1992). *Risk: analysis, perception and management*. London, UK: The Royal Society.

Sánchez-Peña, M., Sánchez-Delgado, K., Agudelo-Ramírez, A. (2015). Estrategias lúdicas para aumentar el conocimiento de un grupo de adolescentes escolarizados sobre la gingivitis. Duazary, 12(2), 100-111.

Savona, E. U. (2004). Ipotesi per uno scenario della prevenzione. In R. Selmini (Ed.), *(a cura di) la sicurezza urbana,* (pp. 273-284). Bologna, Italy: Il Mulino.

Sigerist, H. (1951). A history of medicine: primitive and archaic medicine. New York, NY: Oxford University Press.

Strutt, J. (1993). *Risk assessment and management: the engineering approach.* Cranfield, UK: Cranfield University.

Tonry, M. & Farrington, D. (1995). Strategic approach to crime prevention. Crime and Justice, 19, 1-20. Retrieved from: http://www.jstor.org/stable/1147594

Vargas, I., Villegas, O., Sánchez, A., & Holthuis, K. (2003). Promoción, prevención y educación para la salud. San José, Costa Rica: EDNASSS. Available at: http://www.cendeisss.sa.cr/posgrados/modulos/Modulo2/Modulo_2.pdf

Walgrave, L., & De Cauter, F. (1986). Une tentative de clarification de la notion de prévention. *Annales de Vaucresson, 1*(24), 31-51.

Wallensteen, P. & Möller, F. (2003). Conflict prevention: methodology for knowing the unknown [Uppsala Peace Research Papers No. 7, Department of Peace and Conflict Research]. Sweden: Uppsala University. Retrieved from: http://www.pcr.uu.se/digitalAssets/61/61533_1prevention___knowing_the_unknown.pdf

Wallensteen, P. (2002). Understanding conflict resolution. London, UK: Sage.

Weiss, T. & Hubert, D. (2001). *The responsibility to protect* . Ottawa, ON: International Development Research Center. Available at: http://www.idrc.ca/EN/Resources/Publications/openebooks/963-1/index.html

Yu, E. (2004). Information systems (in the Internet age). In *Practical Handbook of Internet Computing:* Boca Raton, FL: CRC.

CURRICULUM VITAE

Nancy Acevedo Commercial and Systems Manager; Specialist in Project Management; and candidate to Magister in Informatics Project Management from Universidad de Pamplona (Colombia). Professor, OPS in the administrative area at the Basic Sciences Faculty, and member of LOGOS research group hotbed at the Universidad de Pamplona. / Administradora Comercial y de Sistemas, Especialista en Gerencia de Proyectos y candidata a Magister en Gestión de Proyectos Informáticos de la Universidad de Pamplona (Colombia). Se desempeña como docente hora cátedra, OPS en el área administrativa de la Facultad de Ciencias Básicas y miembro del semillero del grupo de investigación LOGOS de la Universidad de Pamplona.

Cristina Satizabal Electronics and Telecommunications Engineering from Universidad del Cauca (Colombia) and Ph.D in Telematics Engineering from Universidad Politécnica de Cataluña (España). Professor at the Telecommunications Engineering Program (Universidad de Pamplona) and member of the LOGOS research group. / Ingeniera en Electrónica y Telecomunicaciones de la Universidad del Cauca (Colombia) y Doctora en Ingeniería Telemática de la Universidad Politécnica de Cataluña (España). Se desempeña como docente de tiempo completo ocasional del Programa de Ingeniería en Telecomunicaciones de la Universidad de Pamplona, donde además forma parte del grupo de investigación LOGOS.