01-033

## SECURITY AS A KNOWLEDGE AREA OF PROJECT MANAGEMENT

Guerrero Chanduví, Dante A. M. [1]; Feria Garrido, Jorge [2]; Patiño Luna, Claudia [1]; Gerónimo Mendoza, Ginny Alison [3]

[1] Universidad de Piura, [2] PetroPerú, [3] Telefónica Móviles

Today, the concept of security plays a key role in the success of a project because their mismanagement may lead to the occurrence of fatal accidents, to their delay, cancellation or economic impact. This communication arises from the need to include "security" as a new knowledge area to be integrated in version 5 of the PMI PMBOK, contrasting with other certification international models, such as IPMA, PRINCE 2 and P2M. In the research, the security is defined from three perspectives: physical, information and business continuity. Project management models are analyzed, in terms of security, from the most important international certification organisms and a conceptual model is proposed. As a result, the processes of this new area of knowledge with their inputs, outputs, tools and techniques are detailed during the project life cycle. In addition, the relationship with the permanent organization is taken into account, criterion to be included in the development of project management documentation.

***Keywords:*** *Project Management; Security; process*

## LA SEGURIDAD COMO ÁREA DE CONOCIMIENTO DE LA GESTIÓN DE PROYECTOS

Hoy en día, el concepto de seguridad juega un papel clave en el éxito de un proyecto ya que su inadecuada gestión podría conllevar a la ocurrencia de accidentes fatales, a su retraso, cancelación o afectación económica. Esta comunicación surge de la necesidad de incluir a la “seguridad” como una nueva área de conocimiento a ser tomada en cuenta en la versión 5 del PMBOK del PMI, contrastando con otros modelos de certificación internacionales, tales como IPMA, PRINCE 2 y P2M. En la investigación se define a la seguridad bajo tres perspectivas: física, de la información y para la continuidad del negocio. Se analizan los modelos de gestión de proyectos, en cuanto a seguridad se refiere, de las más importantes certificadoras internacionales, y se propone un modelo conceptual. Como resultado se detallan los procesos de esta nueva área de conocimiento con sus respectivas entradas, salidas, herramientas y técnicas, durante el ciclo de vida del proyecto. Sumado a esto se tiene en cuenta la relación con la organización permanente, criterio que debe incluirse en la elaboración de la documentación de gestión del proyecto.

***Palabras clave:*** *Dirección de Proyectos; Seguridad; Procesos*

Correspondencia: Dante A. M. Guerrero Chanduví dante.guerrero@udep.pe

## 1. INTRODUCCIÓN

Actualmente, el término seguridad constituye un aspecto muy importante en las empresas de todo el mundo debido a los altos costos que acarrean los accidentes fatales tanto para la compañía como para los trabajadores. De igual manera, en el desarrollo de un proyecto, un eslabón que contribuye al éxito del mismo es una adecuada gestión de la seguridad.

El presente trabajo surge de la necesidad de incluir una nueva área de conocimiento en la versión 5 del PMBOK del PMI: la gestión de la seguridad, contrastando con otros modelos de certificación internacionales tales como: IPMA, PRINCE 2 y P2M.

Por lo general, siempre se asocia a la seguridad con la denominada seguridad física en el lugar de trabajo. No obstante, la presente investigación abarca dos perspectivas más a tomar en cuenta: la seguridad de la información y la seguridad para la continuidad del negocio, se analizan los modelos antes mencionados y se propone un modelo conceptual.

Finalmente, se detallan los procesos de esta nueva área de conocimiento con sus respectivas entradas, herramientas y técnicas, y salidas durante el ciclo de vida del proyecto. De esta manera, esta propuesta supondrá ampliar la visión del director de proyectos en lo referente a su gestión.

## 2. MARCO TEÓRICO

Durante mucho tiempo la seguridad no ha sido una materia de primer orden dentro de las organizaciones ya que centralizaban sus operaciones en la producción, asumiendo los riesgos en sus procesos como un daño inevitable. Además, existen todavía algunas de ellas que no van más allá del cumplimiento de las leyes exigibles.

Pese a esto, se ha ido tomando conciencia y ya se hace énfasis en el ámbito humano. Si bien es cierto que la gestión de la seguridad y salud en el trabajo ya está muy reconocida bajo distintos estándares, en muchas organizaciones todavía hay un campo de actuación para desarrollar una gestión de la seguridad que abarque otros ámbitos como la información y la continuidad del negocio (Merlo, 2015)

### 2.1. Seguridad física

Hoy en día, la seguridad física ocupacional es una preocupación de compañías de sectores críticos como petróleo, gas, minería y construcción, siendo este último el más peligroso, según la Agencia Europea para la Seguridad y Salud en el Trabajo (Sousa, Almeida, & Dias, 2014). Su preocupación se debe sobre todo a los terribles costos asociados, cifra que la OIT estima en 1,36 billones USD o el 4% del Producto Bruto Interno del mundo de cada año (Organización Internacional del Trabajo, 1996).

La OIT también indica que, a nivel mundial cada 15 segundos un trabajador muere a causa de accidentes o enfermedades relacionadas con el trabajo y 153 trabajadores tienen un accidente laboral. Cada día mueren 6.300 personas a causa de accidentes o enfermedades relacionadas con el trabajo, es decir más de 2.3 millones de muertes por año.

La Seguridad y Salud Ocupacional es el conjunto de medidas técnicas, económicas, psicológicas, etc., que tienen como meta ayudar a la empresa y a sus trabajadores a prevenir los accidentes industriales, controlando los riesgos propios de la ocupación, conservando los locales, la infraestructura industrial y sobre todo los ambientes naturales. (Chamochumbi, 2014, pág. 23).

Es por ello, que se han establecido una diversidad de leyes y reglamentos relacionados con la prevención de accidentes de trabajo y enfermedades profesionales en todo el mundo. En

el Perú, según la ley N° 29783 de Seguridad y Salud en el Trabajo y su Reglamento, todo empleador tiene la obligación de crear un SGSST con el fin de garantizar un entorno laboral seguro y saludable para sus trabajadores (Egúsquiza, Hurtado, & Atahuaman, 2013).

A nivel mundial, los estándares más conocidos son la OHSAS 18001 y la familia de normas ISO, entre las que destacan: 14001, 22000, 31000, 39001 y 50001.

En el contexto de gestión de proyectos, el rol del Director del proyecto prioriza la gestión de la línea base (tiempo, costo, alcance y calidad) en la denominada Gestión de Riesgos del PMBOK, dejando así en un segundo plano a la seguridad de la persona (Project Management Institute, 2013)

Durante todo el desarrollo, el director debe considerarse también como un "agente de seguridad" que en su ámbito de influencia, debe alinear la gestión de seguridad del proyecto a la gestión de la empresa considerando a la seguridad como una responsabilidad primaria dentro de sus funciones, al igual que las otras áreas de conocimiento. Además deberá fomentar una cultura de seguridad.

### 2.2. Seguridad de la información

El avance de la tecnología ha traído consigo un nuevo problema al mundo de la informática: la información en formato digital, es más fácil de transportar, por lo que las posibilidades de hurtarla son cada vez menos despreciables (Iscala, Meléndez, Pabon, & Peña, 2012).

En un estudio realizado a nivel mundial por Verizon que concluye en el 2012, revela que el 97% de los incidentes ocurridos podrían haber sido evitados, el 85% de los incidentes tardan en ser detectados y el 92% son detectados por terceros a la empresa (Catoira, 2012). Por otro lado, el Reporte Anual de Seguridad 2015 de Cisco (Líder mundial en TI), indica que las organizaciones deben tomar acciones inmediatas para defenderse de los ataques que cada vez son más eficientes mientras que los equipos de seguridad, deben estar constantemente mejorando su enfoque para proteger a la organización (Boletín de prensa de CISCO, 2015).

En este constante proceso de la consecución de protección de información se han definido estándares internacionales, guías de buenas prácticas empleados para asegurar la información, tales como: ISO 27001, 27002, 27005, ITIL, CoBIT, NIST SP 800-30, BS 25999 (Borbón, 2011)

Como vemos según la importancia que ha adquirido hoy en día la información en las organizaciones, es necesario ser conscientes del valor de la información y usar en cada una de las actividades diarias dicha conciencia. De manera similar ocurre en la gestión de proyectos, queda demostrado con casos particulares como los que citaremos a continuación, que proyectos de gran envergadura de empresas con sólidos Sistemas de Gestión de Seguridad, no se han salvado de grandes ataques informáticos.

Uno de los casos más sonados fue el ataque informático a un nuevo proyecto de Sony, estando casi al borde de cancelar el lanzamiento de la comedia "The Interview". (El Comercio, 2014). Coca Cola también fue víctima de un ataque a su información, estaba concretando mediante un nuevo proyecto la compra de "Huiyuan Juice Group" por 2400 millones de dólares cuando sucedió el ataque. A los tres días, el negoció se cayó (Elgin, Lawrence, & Riley, 2012).

Lo que debe preocupar al director del proyecto es la protección de la información que fluye en torno a esta nueva idea y el producto esperado, que el proyecto no sea copiado por personas que tengan acceso a él, por lo que también deberá asumir el rol de "Guardián de Seguridad de la Información". Otro aspecto importante a tomar en cuenta es que, independientemente de contar con un Sistema de Gestión de Información muy aterrizado en la organización, no se exonera su responsabilidad en el resguardo de la información del proyecto. Debe gestionarse

la seguridad de la información con la misma rigurosidad con la que se gestiona el alcance, cronograma, calidad, etc., ya que representa un activo más del proyecto.

### 2.3. Seguridad para la continuidad del negocio

La Seguridad para la Continuidad del Negocio ha empezado a cobrar relevancia en el mundo empresarial en los últimos años debido a que en cualquier momento, se pueden materializar situaciones que obliguen a las empresas a paralizar sus operaciones (Devia, 2013).

Se entiende por continuidad del negocio y de las operaciones a la capacidad de la organización para continuar brindando sus servicios y realizando sus actividades a niveles aceptables después de una interrupción. Un sistema de gestión de continuidad es parte del sistema completo de sistemas de gestión de una organización que se encarga de establecer, implementar, operar, monitorear, mantener y mejorar la continuidad del negocio y de las operaciones (International Organization for Standardization, 2012).

América Latina y el Caribe es una región donde los desastres naturales son frecuentes; además de los eventos ocasionados por el hombre: atentados terroristas, sabotajes, explosión, robo de información, entre otros. Ante tales situaciones, la implementación de un sistema de gestión de la continuidad del negocio (SGCN) se ha convertido en un verdadero respaldo (Dávila, 2013).

Según Dávila, numerosos son los casos de organizaciones que están realizando esfuerzos de continuidad del negocio y sus operaciones, principalmente las empresas reguladas – banca y en menor grado, el sector asegurador, tales como: Grupo Bancolombia, Banco de Costa Rica, Toyota Financial Services de México, Pacíficos Seguros de Perú, Telefónica Movistar de Colombia, Grupo Nutresa, entre otros.

El estándar más popular a nivel mundial referente a este tema es ISO 22301:2012, que tiene por nombre “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio”, que engloba las distintas metodologías y buenas prácticas en continuidad del negocio generadas en los últimos casi 20 años (Servat, 2012). Según Cainero, ANSI/ASIS SPC.1 es el estándar reconocido por ANSI para certificar organizaciones en continuidad del negocio.

Desde la perspectiva de la gestión de proyectos, el director del proyecto debe velar por la protección de todos los activos críticos frente a una situación de amenaza o peligro. Como tal, su rol deberá ser el de asegurarse que se ha creado, desarrollado y mantenido de forma regular un Plan de Continuidad de Negocio, dentro de su gestión.

Se concluye, por tanto, que la denominada “Gestión de la Seguridad” se fundamenta en la aplicación en los proyectos, de una serie de normas, estándares y buenas prácticas que ya han sido establecidas y son utilizadas a nivel mundial, local y empresarial para garantizar el éxito de sus procesos. Entre las buenas prácticas destacan: OHSAS 18001 y la familia de normas ISO. En el caso de Perú, cabe resaltar la ley de Seguridad y Salud en el Trabajo N°29783 y su reglamento, así como las disposiciones de diversos organismos como: Defensa Civil, INDECI, etc. Cabe resaltar que la mayoría de normas anteriormente mencionadas se sustentan en una metodología para la gestión de riesgos.

## 3. METODOLOGÍA DE LA INVESTIGACIÓN

La metodología de la investigación consta de los siguientes pasos:

### 3.1. Planteamiento de la hipótesis o proposición

Se plantea la hipótesis sobre la necesidad de incluir a la “seguridad” como una nueva área de conocimiento que debe ser tomada en cuenta en la gestión de proyectos.

### 3.2. Revisión bibliográfica sobre la seguridad en la gestión de proyectos

Se realiza una revisión de la literatura profesional sobre la seguridad en la gestión de proyectos. En primer lugar, se investiga acerca de los tres ámbitos de la seguridad: física, de la información y para la continuidad del negocio para lograr tener un enfoque global. Posteriormente, se revisa la siguiente bibliografía: los cuatro principales modelos de gestión de proyectos (PMBOK, PRINCE2, IPMA y P2M) con la finalidad de analizar la manera en que cada uno de ellos aborda el tema de la seguridad, la ISO 9001 y su enfoque basado en procesos y el Ciclo de Vida del proyecto según AEIPRO.

### 3.3. Análisis para la sustentación de la inclusión de la gestión de la seguridad como un área de conocimiento

Partiendo de la premisa que la investigación tiene como fin garantizar la gestión de la seguridad durante el ciclo de vida del proyecto, AEIPRO afirma que el ciclo de vida en los proyectos clásicos de ingeniería está compuesto de cuatro diferentes fases: estudio preliminar, anteproyecto, proyecto y realización o ejecución (Asociación Española de Dirección e Ingeniería de Proyectos, s.f.).

Por otra parte, según la ISO 9001, para que una organización funcione de manera eficaz, tiene que determinar y gestionar numerosas actividades relacionadas entre sí. Una actividad o un conjunto de actividades que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados, se puede considerar como un proceso. La aplicación de un sistema de procesos junto con la identificación e interacciones de estos procesos, así como su gestión para producir el resultado deseado, puede denominarse como "enfoque basado en procesos" (International Organization for Standarization, 2008). De la misma manera, para realizar una correcta gestión de la seguridad y tener éxito, se adopta este mismo enfoque a lo largo del ciclo de vida del proyecto.

Del análisis de los cuatro modelos de gestión de proyectos en lo que respecta a la seguridad, los resultados obtenidos se ven reflejados en la tabla 1. Dado que se elige un enfoque basado en procesos, se tienen como alternativas los modelos PMI y PRINCE 2. Sin embargo, se adopta el modelo del PMI debido a que además de que su metodología está orientada a procesos, incluye la denominada Extensión de la Construcción la cual recalca la importancia de la seguridad en los proyectos de construcción en base a una nueva área de conocimiento: Gestión de la Seguridad.

**Tabla 1: Visión de la Seguridad desde cuatro modelos de gestión de proyectos**

| CRITERIO/ MODELO DE GESTIÓN | PMI | IPMA | PRINCE2 | P2M |
|---|---|---|---|---|
| **FUNDAMENTO** | Administración de proyectos como un conjunto de nueve áreas de conocimiento que contienen una serie de procesos. Cada proceso establece unas entradas, técnicas o herramientas y salidas. | Competencias profesionales a través de la ICB o NCB, compuesta por elementos de competencias técnicas, de comportamiento y contextuales. | Dividido estructuralmente en siete Principios, siete Temáticas y siete Procesos. (Montes de Oca & Perez, 2014) | Desarrolla cuatro aspectos: entradas de proyectos, administración de proyectos, administración de programas y administración de 11 dominios. (Foon & Heap, 2012) |
| **VISIÓN DE LA SEGURIDAD** | -"Gestión de Riesgos", enfocada en la protección de la línea base.<br>-La "Extensión de la construcción de la guía del PMBOK" abarca la gestión de la seguridad como área de conocimiento, haciendo alusión únicamente a la seguridad física en proyectos de construcción. (Project Management Institute, 2007). | -La competencia contextual de Seguridad, Higiene y Medioambiente tiene como fin asegurar que la organización se comporte de forma apropiada bajo este contexto en los proyectos.<br>-Se enfoca en la seguridad de los implicados del proyecto y en el rol del Director del Proyecto como agente de seguridad. | -Temática del Riesgo: gestión de las incertidumbres relacionada con 4 parámetros: tiempo, costo, calidad y alcance. (Díaz, Gonzáles, Morales, & Rosales, 2014) | -Dominio denominado "Gestión de Riesgos". |

**Fuente: Elaboración propia**

La guía del PMBOK, estándar en la administración de proyectos desarrollado por el Project Management Institute (PMI), es una colección de 47 procesos y 10 áreas de conocimiento generalmente aceptadas como las mejores prácticas dentro de la gestión de proyectos. Para que estas buenas prácticas sean asequibles, divide el conjunto de conocimientos para la dirección de proyectos en 5 grupos de procesos: de Inicio, Planificación, Ejecución, Monitoreo y Control, Cierre.

Es así que todo proyecto (así como sus distintas fases e iteraciones) tiene que transitar por una serie de actividades de inicio, planeación, ejecución, monitoreo y control, y finalmente cierre. Estos grupos de procesos se pueden asemejar con las fases del modelo de mejora continua de Deming: "Planear, Hacer, Revisar y Actuar".

Asimismo, el PMBOK define los aspectos importantes de cada una de las Áreas de Conocimiento y cómo éstas se integran con los Grupos de Procesos. Cada Área de

Conocimiento proporciona una descripción de las entradas y salidas, herramientas y técnicas de uso más frecuente en los procesos de la dirección de proyectos para producir cada uno de los resultados. Incluye además un diagrama de flujo de datos de un proceso.

En base al enfoque de procesos adoptado, la metodología sigue el mismo curso de la Guía del PMBOK, definiendo así que los procesos a seguir deben encontrarse dentro de la matriz de correspondencia entre grupos de procesos y áreas de conocimiento de la Dirección de Proyectos, con sus elementos respectivos.

Sumado a esto, se analiza el área de conocimiento de Gestión de la Calidad del PMBOK la cual evalúa el resultado del proyecto orientado a los procesos con el objetivo de obtener un producto de calidad, incluyendo tres procesos: planificación, aseguramiento y control de la calidad. Para el caso de la Gestión de la Seguridad, es aplicable esta misma estructura de procesos ya que lo que se busca es establecer y monitorear la aplicación de buenas prácticas traducidas en requisitos de los procesos de gestión.

El último fundamento clave es la denominada “Extensión de la Construcción del PMBOK”, la cual se ocupa de las prácticas específicas de los proyectos de construcción en base a una serie de normas y directrices que se aplican a los sistemas de gestión de este tipo de sector, tales como la serie de normas ISO 9000. Incluye a la gestión de la seguridad dentro de sus áreas de conocimiento, estableciendo tres procesos: planificación, aseguramiento y control de la seguridad, los cuales se analizan y son tomados en cuenta en la definición de la propuesta.

### 3.4. Definición de la propuesta en base a los lineamientos del PMBOK

La definición de la propuesta se realiza siguiendo el mismo curso de la Guía del PMBOK.

Se contrastan los procesos del área de conocimiento de la Gestión de Calidad del PMBOK con los de la Gestión de Seguridad de la Extensión de la Construcción, definiéndose tres procesos: Planificación, Aseguramiento y Control.

Asimismo, se verifican las entradas, herramientas y técnicas y salidas, para cada uno de los procesos de las áreas de conocimiento anteriormente mencionadas y se seleccionan aquellas que van acorde con los tres ámbitos de la seguridad. Luego se analizan qué otros factores impactan a la seguridad y se plantean nuevas entradas, herramientas y técnicas y salidas que complementen la propuesta.

## 4. RESULTADOS DE LA PROPUESTA

Como resultado de la investigación se definen los tres procesos que debería conformar la Gestión de la Seguridad: Planificación de la Seguridad, Aseguramiento de la Seguridad y Control de la Seguridad. Ver ilustración 1: Procesos de la Gestión de la Seguridad.

**Ilustración 1: Procesos de la Gestión de la Seguridad**

| Área de conocimiento | GRUPOS DE PROCESOS DE DIRECCIÓN DE PROYECTOS | | | | |
|---|---|---|---|---|---|
| | Grupo de Procesos de Iniciación | Grupo de Procesos de Planificación | Grupo de Procesos de Ejecución | Grupo de Procesos de Seguimiento y Control | Grupo de Procesos de Cierre |
| Gestión de la Seguridad | | Planificación de la Seguridad | Aseguramiento de la Seguridad | Control de la Seguridad | |

**Fuente: Elaboración propia**

### 4.1. Planificación de la Seguridad

Es un proceso por el cual se identifican los requisitos y normas de seguridad necesarios para el proyecto. Proporciona una guía y dirección sobre cómo se gestionará y verificará que se lleve a cabo la seguridad. Ver ilustración 2: Planificación de la Seguridad. La planificación de la seguridad debería realizarse en paralelo con los demás procesos de planificación.

**Ilustración 2: Planificación de la Seguridad**


**Fuente: Elaboración propia**

Los apetitos y las tolerancias a los riesgos constituyen entradas estratégicas para definir el Plan de Gestión de la Seguridad. Los apetitos de riesgo son aquellos riesgos que se están dispuestos a aceptar en la búsqueda de la misión/visión de la empresa; en cambio, las tolerancias al riesgo se definen como los niveles aceptables de variación en los resultados de la empresa relativos a la consecución de sus objetivos (Committee of Sponsoring Organizations of the Treadway Commission, 2009).

Las técnicas de planificación de seguridad que se describen en esta sección son las que se emplean con más frecuencia en los proyectos. Existen muchas otras que pueden ser útiles dependiendo del tipo de proyecto y el área de aplicación.

Una de ellas es análisis de brechas del proyecto con el fin de comparar lo que la Empresa ya tiene implementado en cuanto a seguridad con lo que se requiere en el Proyecto. Otra técnica importante es el Benchmarking a fin de comparar las prácticas actuales o previstas de un proyecto en lo referente a la seguridad, con aquellas correspondientes a otros proyectos similares para identificar las mejores prácticas, generar ideas de mejora, y proporcionar una base para medir el desempeño.

Como salida fundamental del proceso se tiene el Plan de Gestión de Seguridad que forma parte del Plan General del Proyecto, el cual define esencialmente la metodología a ser adoptada por la organización ejecutante para llevar a cabo la gestión de la seguridad y la manera de cumplir con los requisitos del proyecto. Ésta será una de las principales entradas para el aseguramiento de la seguridad.

También es importante definir ciertas métricas para cuando se realice el aseguramiento y control de seguridad del proyecto. Dichas métricas deben ser capaces de medir la evolución

de la seguridad del proyecto a lo largo del tiempo. Por ejemplo: número de empleados capacitados en temas de seguridad, número de verificaciones sin accidentes, cantidad de accesos a red (autorizados y no autorizados), efectividad de los sistemas de seguridad ante amenazas, número de accidentes en la empresa, entre otros.

### 4.2. Aseguramiento de la Seguridad

Involucra la aplicación de las actividades planificadas y sistemáticas de seguridad para asegurar que el proyecto emplee todos los procesos necesarios para cumplir con los requisitos, la determinación de si dichos procesos son efectivos en el aseguramiento de los requisitos de seguridad del proyecto y el producto, propios del sistema de gestión del proyecto y la evaluación de los resultados de la gestión de seguridad de forma regular con el objetivo de proporcionar confianza en que el proyecto satisfará las normas de seguridad relacionadas. Ver ilustración 3: Aseguramiento de la Seguridad.

Constituye un proceso de ejecución, que se encarga de auditar los datos generados durante los procesos de Planificación y Control de Seguridad, es decir los requisitos de Seguridad y los resultados obtenidos a partir de las medidas de control de seguridad, con la finalidad de garantizar la utilización de los estándares de seguridad y las definiciones operativas adecuadas.

**Ilustración 3: Aseguramiento de la Seguridad**

| Entradas | Herramientas | Salidas |
|---|---|---|
| •Plan de gestión de la seguridad<br>•Métricas de Seguridad<br>•Plan de Mejoras del Proceso<br>•Información del rendimiento del trabajo.<br>•Solicitudes de Cambio Aprobadas<br>•Medidas de Control de Seguridad<br>•Solicitudes de Cambio<br>•Activos de los Procesos Organizacionales<br>•Requisitos del contrato | •Herramientas y técnicas de la planificación de la seguridad.<br>•Auditorías de Seguridad<br>•Análisis de Riesgos y Peligros de Seguridad<br>•Análisis de Procesos<br>•Herramientas y técnicas de Control de Seguridad<br>•Evaluaciones a la Gestión de Seguridad<br>•Herramientas y técnicas de los procesos de gestión de riesgos | •Solicitud de cambio<br>•Activos de los procesos de la Organización (Actualizaciones)<br>•Actualizaciones al Plan para la Dirección del Proyecto<br>•Realizar mediciones del aseguramiento de la seguridad<br>•Plan de Gestión de Seguridad (Actualizaciones)<br>•Plan de Mejoras de procesos (Actualizaciones)<br>•Plan de Monitoreo y Control de la Seguridad |

**Fuente: Elaboración propia**

Implementa un conjunto de acciones y procesos planificados y sistemáticos de seguridad, los cuales forman parte del Plan de gestión de la Seguridad. Asimismo, hace uso de métricas de seguridad, para verificar los atributos y variaciones permitidas, del plan de mejoras de los procesos para identificar las actividades que incrementen el valor del producto y de las mediciones de control de seguridad para reevaluar y analizar el desempeño del sistema de gestión de la seguridad del proyecto.

Las herramientas y técnicas a emplear en este proceso son las mismas utilizadas para planificar y controlar la seguridad, entre las principales se encuentran: auditorías de seguridad, análisis de riesgos y peligros de seguridad, análisis de procesos, entre otros. Como resultado se obtienen solicitudes de cambio y actualizaciones a diversos documentos del proyecto.

### 4.3. Control de la Seguridad

El proceso de Control de la Seguridad tiene como fin evaluar el desempeño y recomendar los cambios necesarios, a través del monitoreo y registro de los resultados de la ejecución de las actividades de seguridad. Identifica los desempeños insatisfactorios y las maneras de eliminar sus causas. Esto incluye los fallos por parte de la seguridad durante los procesos anteriormente descritos. Ver ilustración 4: Control de la Seguridad.

**Ilustración 4: Control de la Seguridad**

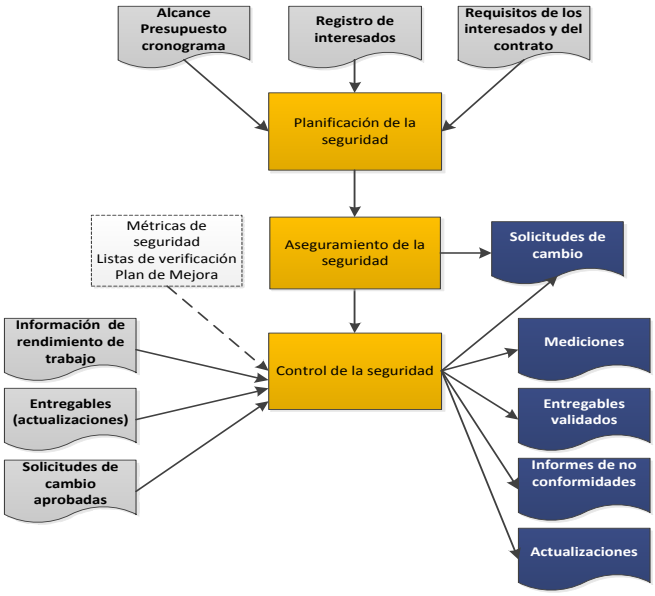

**Fuente: Elaboración propia**

Las herramientas y técnicas más relevantes de este proceso son: el análisis de riesgos y peligros, con el fin de identificar los peligros potenciales de seguridad del proyecto; la investigación de accidentes físicos y delitos informáticos a fin de lograr mejoras en el desempeño en la seguridad partiendo de la identificación de las causas respectivas, métodos de análisis estadísticos de procesos e información tales: como inspecciones, análisis de causa y efecto, gráficos de control, análisis de Pareto, etc; cuyo objetivo es determinar si se cumplen o no con los requisitos de seguridad definidos en el proyecto.

Para aquellos elementos que no cumplan con los requisitos de seguridad planificados, comúnmente se debe preparar un informe de no conformidad, delineando las deficiencias, la acción correctiva inmediata para adaptar el trabajo no conforme, y la acción preventiva para evitar la recurrencia de la condición que causó la no conformidad.

Finalmente la ilustración 5: Procesos de la Gestión de la Seguridad, muestra un resumen de los tres procesos definidos para el área de conocimiento de la Seguridad en la guía del PMBOK, en donde se muestran las entradas y salidas que impliquen documentación.

**Ilustración 5: Procesos de la Gestión de la Seguridad**




**Fuente: Elaboración propia**

## 5. CONCLUSIONES

Hoy en día, en el contexto de los proyectos, el Director del Proyecto apunta sólo a la protección de la línea base dentro de su gestión durante todo el proyecto, mas no a los tres activos más importantes del mismo: la persona humana, la información y la continuidad del negocio, surgiendo así claramente una necesidad.

Si bien el PMBOK habla de una gestión de recursos humanos, ésta no está enfocada a la protección física de la persona. Además, la Extensión de la Construcción del PMBOK está abocada a proyectos de construcción, mientras que nuestra propuesta implica la aplicación de la gestión de la seguridad al marco más general de la gestión de proyectos de cualquier índole.

El presente artículo pretende alertar de la importancia de la gestión de la seguridad dentro de la gestión de proyectos bajo el enfoque del Project Management Institute (PMI), proponiendo la adopción de una nueva área de conocimiento de “Gestión de Seguridad” para la guía del PMBOK, que contemple la protección de cualquier tipo de activo del proyecto y principalmente de los tres tipos de activos anteriormente mencionados.

Los equipos de proyecto deben utilizar las 10 áreas de Conocimiento de la manera más adecuada en su proyecto específico. Con el planteamiento de agregar esta nueva área de conocimiento se busca concientizar a todos los Directores de Proyecto para que, además de las áreas de conocimiento definidas en este marco, tomen en cuenta la gestión de la seguridad con una relevancia mayor a la que se le ha venido dando.

Los resultados revelan que es necesario llevar a cabo tres procesos para conseguir una correcta gestión de la seguridad: Planificación, Aseguramiento y Control de la Seguridad. Estos procesos incluyen todas las actividades que el sponsor, propietario y la organización deben ejecutar a fin de evitar desastres tanto para el proyecto como para la empresa.

El proceso de planificación define cómo enfocar, planificar y ejecutar los requisitos de gestión de la seguridad del proyecto, el aseguramiento a fin de aplicar lo planificado y el control como último proceso a fin de identificar maneras de eliminar las causas de desempeño de seguridad

insatisfactoria. No se han definido procesos de iniciación y cierre dado que se utilizan estos procesos para obtener la autorización formalizada de inicio o cierre del proyecto o fase.

Por otro lado, cabe resaltar la diferencia entre Gestión de Riesgos y Gestión de la Seguridad. Mientras que la aplicación de la Gestión de Riesgos se ha venido enfocando en la protección de las líneas base del proyecto, la Gestión de la Seguridad apunta a proteger los activos del proyecto, mediante la aplicación de una serie de buenas prácticas o estándares globalmente o localmente aceptados, que se sustentan en una Gestión de Riesgos previa. Es por esta razón por la que no se ha considerado necesario realizar un análisis de riesgos para identificar posibles respuestas a eventos que puedan afectar a los activos del proyecto. Este trabajo ya ha sido realizado bajo muchos enfoques, con la participación de muchos expertos, generando un conocimiento basado en “Buenas prácticas” estandarizadas, que es justamente las que deben aplicarse también en los proyectos.

Al analizar las brechas de seguridad entre lo implementado en la organización permanente y el proyecto en desarrollo, podríamos tener que la organización está más madura que lo que requiere el proyecto, o viceversa. En cualquier escenario, la responsabilidad de la gestión de la seguridad siempre recaerá en el Director del Proyecto, y será su función determinar cómo cubrir la brecha que requiere el proyecto (de haber una brecha por cubrir).

## 6. BIBLIOGRAFIA

Asociación Española de Dirección e Ingeniería de Proyectos. (s.f.). Concepto de Proyecto. Recuperado el 6 de Abril de 2015, de AEIPRO: http://aeipro.com/index.php/es/mainmenu-aeipro/project-manag/885-concepto-de-proyecto

Boletín de prensa de CISCO. (20 de Enero de 2015). Reporte de Seguridad de Cisco revela incremento en la brecha entre la percepción y la realidad en Seguridad Informática. San José, California, Estados Unidos. Obtenido de http://americas.thecisconetwork.com/site/content/lang/es/id/2716

Borbón, J. S. (Agosto de 2011). Buenas prácticas, estándares y normas. Punto Seguridad, Defensa Digital(11), 28. Obtenido de http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Seguridad_Num_11_0.pdf

Catoira, F. (31 de Mayo de 2012). Estudio sobre el estado de la seguridad de información corporativa. Buenos Aires, Buenos Aires, Argentina. Obtenido de http://www.welivesecurity.com/la-es/2012/05/31/estudio-estado-seguridad-informacion-corporativa/

Chamochumbi, C. M. (2014). Seguridad e Higiene Industrial. Lima: Fondo Editorial de la Universidad Inca Garcilaso de la Vega.

Committee of Sponsoring Organizations of the Treadway Commission. (2009). Gestión de Riesgos Corporativos Marco Integrado. Jersey: The Committee of Sponsoring Organization.

Dávila, Y. (Agosto de 2013). La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones. 4. Caracas, Caracas, Venezuela: Secretaría Permanente del SELA. Obtenido de http://www.sela.org/attach/258/EDOCS/SRed/2013/07/T023600005211-0-_Continuidad_de_negocios_y_operaciones_frente_a_situaciones_de_desastre_en_ALC_.pdf

Devia, J. A. (2013). La Continuidad del Negocio: ¿ deseable o requerido? RCT(63), 21-24. Obtenido de http://cintel.org.co/publicaciones/revista-rct/revista-rct-63/

Díaz, M. d., Gonzáles, C., Morales, F., & Rosales, V. F. (2014). Processes's Treatment of Risk Management in Project Management Approaches. 18th International Congress on Project Management and Engineering (pág. 12). Alcañiz: Asociación Española de Dirección e Ingeniería de Proyectos.

Egúsquiza, B., Hurtado, G., & Atahuaman, C. (2013). Seguridad y Salud en el Trabajo Guía Práctica. Lima: Instituto Pacífico - Pacífico Editores.

El Comercio. (18 de Diciembre de 2014). Sony cancela estreno de The Interview por amenazas terroristas. Lima, Lima, Perú. Obtenido de http://elcomercio.pe/mundo/actualidad/sony-cancela-estreno-the-interview-amenazas-terroristas-noticia-1779214

Elgin, B., Lawrence, D., & Riley, M. A. (4 de Noviembre de 2012). Coke gets hacked and doesn't tell anyone. Estados Unidos. Obtenido de http://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell

Foon, L., & Heap, C. (30 de Noviembre de 2012). A review towards the japanese project. Trends and Development in Management Studies, 1, 25-41. Obtenido de http://jyotiacademicpress.net/a_review_towards_the_new.pdf

International Organization for Standardization. (2012). ISO 22301: Seguridad de la Sociedad - Sistemas de Gestión de la Continuidad del Negocio. Ginebra, Suiza. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

International Organization for Standarization. (2008). Enfoque basado en procesos. En I. O. Standarization, ISO 9001 : Sistemas de Gestión de Calidad (pág. 1). Ginebra: Secretaría Central de ISO.

Iscala, N. A., Meléndez, S. M., Pabon, M. Y., & Peña, C. A. (10 de Abril de 2012). Diseño de un protocolo de Seguridad de la Información del Área Financiera de Secretaria de Educación Departamental de Norte de Santander. Ocaña, Santander, Colombia. Obtenido de http://repositorio.ufpso.edu.co:8080/dspaceufpso/bitstream/123456789/329/1/25096.pdf

Merlo, J. L. (3 de Marzo de 2015). Blog La Salle IGS. La gestión de la seguridad en las organizaciones. Madrid, Madrid, España. Obtenido de http://blogslasalleigs.com/2015/03/03/la-gestion-de-la-seguridad-en-las-organizaciones/

Montes de Oca, J., & Perez, M. D. (9 de Junio de 2014). Comparación de Metodologías de Gerencia de Proyectos PRINCE2 y PMBOK5. Bogotá, Bogotá, Colombia.

Organización Internacional del Trabajo. (1996). Seguridad y Salud en el Trabajo. Recuperado el 12 de Enero de 2015, de Organización Internacional del Trabajo: http://ilo.org/global/topics/safety-and-health-at-work/lang--es/index.htm

Project Management Institute. (2007). Construction Extension to the PMBOK Guide (3 ed.). Pennsylvania: PMI Publications.

Project Management Institute. (2013). A guide to the Project Management Body of Knowledge (PMBOK Guide) (Quinta ed.). Pennsylvania: PMI Publications.

Servat, A. A. (Octubre-Diciembre de 2012). Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012. Gestión, 25-31. Obtenido de http://www.gestion.com.do/index.php/octubre-2012/300-nuevo-estandar-internacional-en-continuidad-del-negocio-iso-223012012

Sousa, V., Almeida, N. M., & Dias, L. A. (2014). Risk-based management of occupational safety and health in the construction industry - Part 1: Background knowledge. Safety Science, 76.