SEGURIDAD DE LA INFORMACIÓN, LA RELACIÓN ENTRE CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y LA GESTIÓN DE RIESGOS

Fajardo Leal Jorge Alexander
alexfajar@gmail.com
Bogotá, Colombia
Universidad Piloto de Colombia

Resumen - La identificación de los activos de información hace parte de un conjunto de medidas necesarias para la identificación de riesgos, controles y medidas de contingencia tendientes a asegurar la correcta operación cualquier organización y una adecuada toma de decisiones estratégicas.

Abstract - Currently the identification of information assets and risk management are a key component to ensure adequate levels of information security in a company.

Palabras Claves – Activo de Información, Confidencialidad, Contingencia, Disponibilidad, Integridad, Riesgo.

I. INTRODUCCIÓN

En la actualidad y teniendo en cuenta las nuevas tecnologías de la información, las organizaciones se han concienciado sobre los riesgos existentes sobre robos de información y las medidas que se deben tomar para garantizar su integridad y custodia, dando respuesta así al cumplimiento de la normatividad vigente para la seguridad de la información y sus buenas prácticas o para cumplir con las expectativas de los accionistas; estos aspectos han contribuido para que poco a poco se pase del concepto de las tecnologías de la información “TI” y sistemas información como un centro de costo para la organización, por el de TI y los sistemas información forman parte de la organización y son activos importantes para el funcionamiento y evolución de la organización, y por lo tanto es necesario que se prioricen esfuerzos en su aseguramiento, integridad y disponibilidad en todas las áreas de la organización.

Para poder asegurar la TI de la organización es necesario que se forme la cultura de seguridad de la información y gestión de riesgos, para lo cual es preciso que se defina un concepto esencial para la gestión de seguridad de la información y de riesgos “activo de información”; entiéndase activo de información como aquello que tiene valor y que forman parte del diario operar de las organizaciones y por tanto es necesario identificarlo, clasificarlo, analizar su nivel de tolerancia al riesgo y las contramedidas existentes y futuras que permitan asegurar que se encuentre disponible para los interesados.

II. IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN.

En toda organización se tienen activos de información, sin embargo cuando se indaga sobre activos de información, el personal no tiene

claridad de que son o cual es manera de identificarlos; es por esta razón que desde las áreas de seguridad de la información se deben enfocar esfuerzos para capacitar a los colaboradores sobre que son los activos de información y como clasificarlos al interior de sus procesos, entonces lo primero que hay que comprender es que existen varios tipos de activos:

- Información (bases de datos, documentación de los sistemas de gestión, manuales de usuarios, instructivos, procedimientos, planes de continuidad, configuración de soporte, etc.)
- Hardware (computadores, discos de almacenamiento, etc.)
- Software: (software de nómina, software del sistema, herramientas y programas de desarrollo, paquetes ofimáticos, etc.)
- Red
- Personas
- Activos intangibles: reputación, imagen de la organización, etc.

En el listado anteriormente se define una serie de activos de información, pero cabe resaltar que el detalle de los activos varían de una organización a otra, por lo tanto es necesario antes de iniciar cualquier proceso de clasificación de activos, se realice un reconocimiento y entendimiento de los procesos propios de la organización y quienes son los líderes cada proceso. A partir de la contextualización de los procesos de la organización se debe iniciar la identificación de activos de información asociados a cada proceso, para esta actividad es recomendable entablar mesas de trabajo con los responsables o encargados de cada proceso con la finalidad de contar con el contexto delimitado del proceso en cuestión, para esto se puede emplear la técnica de ejecución de preguntas, con las cuales se pueden identificar en primera instancia aquellos componentes que se pueden ir catalogando como activos de la información del proceso; establecida esta primera lista de activos de información es necesario efectuar una nueva mesa de trabajo con el líder de proceso, la cual tiene como finalidad la socialización de los activos identificados y de esta forma establecer el listado oficial de activos del proceso, sobre los cuales se efectuará el análisis de riesgos.

Una vez que se tienen identificados y aprobados los activos de información del proceso evaluado es necesario que se continúe con el proceso de identificación de los riesgos a los que pueden estar expuestos dichos activos.

III. CRITERIOS PARA LA IDENTIFICACIÓN Y VALORACIÓN DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN

Para todo proceso de gestión de riesgos ya sea informáticos, de la información, operativos, entre otros; el primer paso es establecer es el modelo de gobierno y gestión de riesgos que proporcionen las directrices globales en función, una vez definido el modelo gobierno, se debe definir una metodología la cual debe contener los responsables de la

gestión de riesgos, frecuencia de la identificación de riesgo, criterios de impacto y probabilidad para la valoración del riesgo, los cuales debe estar dados en la frecuencia de ocurrencia de un evento en la organización y el impacto de la materialización del riesgo, umbrales de tolerancia y tratamiento del riesgo.

Para definir la metodología de gestión de riesgos al interior de una organización es recomendable adoptar las buenas prácticas sugeridas por el estándar de gestión ISO 31000, Octave o Magerit, y su enfoque debe estar orientado hacia la estructura y modelo de negocio, adicionalmente estos estándares proporcionan una serie de herramientas que facilitan el entendimiento y la delimitación de aspectos específicos para la construcción de la metodología de riesgos, un ejemplo a seguir se puede encontrar en el libro 2 de la metodología magerit *catálogo de elementos_es_NIPO_630 [1]* en el cual se definen una serie de activos y sus respectivas acotaciones según la tipología del activo, orientando de esta forma la clasificación de los activos que existen en las organizaciones.

En la construcción de la metodología de riesgos de la organización, es preciso definir es una escala que permita evaluar la probabilidad de ocurrencia de un riesgo a lo largo del tiempo, para la identificación de la probabilidad se puede es posible utilizar diversidad de escalas y valores, a continuación, se describe una escala para la valoración de probabilidad.

TABLA I.
MATRIZ DE PROBABILIDAD (P).

Valor de la probabilidad	Probabilidad de ocurrencia
1	Al menos una vez al año
2	Una vez por semestre
3	Una vez por Trimestre
4	Una vez al mes
5	Varias veces en el mes

Tomado de: Autoría Propia.

Siendo la menor probabilidad la ocurrencia de un evento una vez por año y la mayor probabilidad la generación del mismo suceso más de dos veces en el mes, sin embargo la frecuencia varía de una organización a otra de acuerdo a las circunstancias particulares de sus operaciones. Adicional a la identificación de la probabilidad de ocurrencia del evento de riesgo, es necesario definir el impacto generado a partir de la materialización del evento, por lo cual, se define una escala para de impacto ante la de materialización del evento de riesgos.

TABLA II.
MATRIZ DE IMPACTO (I).

Impacto	Ponderación del Impacto
No genera afectación	1
Afectación Leve	2
Afectación moderada	3
Afectación grave	4
Afectación catastrófica	5

Tomado de: Autoría Propia.

Una vez definidas las escalas de probabilidad e impacto se tiene el insumo base para gestionar riesgos de manera transversal en la

organización, sin embargo, como el objetivo del documento se encuentra orientado a los activos de información es necesario incluir en la metodología de riesgos aspectos propios de seguridad de la información en la metodología de riesgos; para lo cual es preciso hablar de sus tres pilares:

- *Confidencialidad: es la garantía de acceso a la información de los usuarios que se encuentran autorizados para tal fin. [2]*

- *Integridad: es la preservación de la información completa y exacta. [3]*

- *Disponibilidad: es la garantía de que el usuario accede a la información que necesita en ese preciso momento. [4]*

Los cuales dependiendo del enfoque que se quiera para la gestión de riesgos de la organización pueden o no incluirse en la valoración cuantitativa del riesgo inherente[1] (RI), de esta manera, si la organización solo desea trabajar la gestión de riesgos con una orientación hacia los activos de información, es recomendable incluirlos en la ecuación del riesgos inherente, pero si por el contrario quiere que la gestión de riesgos sea transversal, la recomendación es incluir casillas de verificación de afectación de cada pilar de la seguridad de la información y así de esta forma se pueden dar cumplimiento a estándares buenas prácticas como ISO 27001:13, si es que la empresa se encuentra certificado o en proceso de certificación de este estándar.

Con la definición dada en *[2]-[4]* de cada uno de los pilares de la seguridad de la información y con la finalidad de incluirlos en la ecuación para obtener el riesgo inherente al que se expone él o los activos de información, es conveniente definir una ponderación de afectación de la disponibilidad, integridad y confidencialidad de los activos de información, es necesario que al momento su definición se tenga presente nicho de negocio de empresa, la cantidad, sensibilidad y tiempo en que la empresa podría operar sin su información, para tales efectos se definen las escalas que se muestran en las tablas III, IV y V, las cuales están orientadas hacia la afectación de cada uno de los tres pilares de la seguridad de la información:

TABLA III
ESCALA DE DISPONIBILIDAD (D).

Valor	Descripción	Criticidad
0	No aplica / No es relevante	No critico
1	Debe estar disponible al menos el 10% del tiempo	Menos critico
2	Debe estar disponible al menos el 50% del tiempo	Medianamente critico
3	Debe estar disponible al menos el 99% del tiempo	Critico

Tomado de: Autoría Propia.

[1] Riesgo Inherente: Riesgo al cual no se le han evaluados los controles existentes.

TABLA IV
ESCALA DE INTEGRIDAD (I).

Valor	Descripción	Nivel
0	No aplica / No es relevante	Mínima
1	No es relevante los errores que tenga o la información que falte	Baja
2	Tiene que estar correcto y completo al menos en un 50%	Media
3	Tiene que estar correcto y completo al menos en un 95%	Alta

Tomado de: Autoría Propia.

TABLA V
ESCALA DE CONFIDENCIALIDAD(C).

Valor	Descripción	Carácter
0	No aplica / No es relevante	Publico
1	Daños muy bajos, el incidente no trascendería del área afectada	Uso Interno bajo
2	Serían relevantes, el incidente implicaría a otras áreas	Uso Interno medio
3	Los daños serían catastróficos, la reputación y la imagen de la organización se verían comprometidas	Restringido

Tomado de: Autoría Propia.

Con las diferentes escalas establecidas, contamos con los recursos necesarios para poder calcular el riesgo inherente, dando como resultado la siguiente fórmula:

$$RI = (P * I) + (C + I + D) \quad (1)$$

La fórmula (1) nos permite conocer el valor cuantitativo del riesgo puro al que se encuentra expuesto cada uno de los riesgos, sin embargo, deben ser clasificados dentro de una matriz de calor con zonas de riesgo, de esta manera se elaboran los es allí cuando surgen los mapas de calor, los cuales dependiendo de la cantidad de variables que se definan para la obtención del riesgo pueden tener menor o mayor cantidad de cuadrantes, el cual proporcionara las escalas de criticidad del riesgo, adicionalmente con este se inicia el análisis del nivel de aceptación del riesgo, es recomendable que los riesgos que se acepten en la organización sean aquellos que se encuentran en niveles de riesgo bajo, existiendo en el ejemplo 5 zona de riesgo.

Muy Baja, Baja, Moderada, Alta y Muy Alta, dado que la escala de valoración del riesgo se define de 5 niveles por variable de impacto y probabilidad.

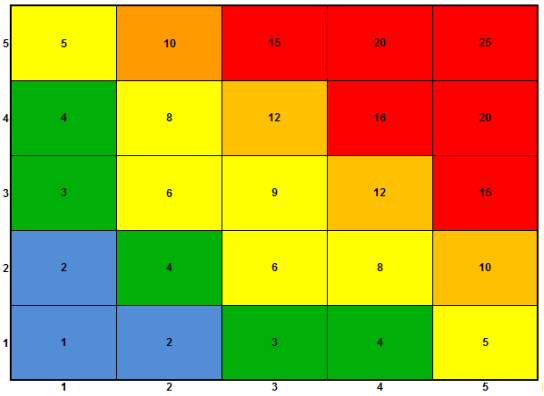

Fig. 1 Matriz De Calor
Tomado de: Autoría Propia.

Identificados todos los criterios necesarios para realizar la valoración del riesgo inherente al que se pueden enfrentar los activos de información,

es posible también relacionar otros tipos riesgos que se pueden impactar en la organización y que tiene relación indirecta con los activos, esto también permite generar una gestión de riesgos con mayor transversalidad, entre los tiempos de riesgos que se puede relacionar son:

- *Riesgo Estratégico*: Se enfoca a los temas relacionados con los planes estratégicos de toda organización, misión y el cumplimiento de los objetivos estratégicos definidos por la alta gerencia de la organización.

- *Riesgo Reputacional*: Se relacionan con la percepción y la confianza y buena imagen que tienen nuestros de los clientes, la comunidad y diferentes grupos sociales referente organización.

- *Riesgo Operativo*: Comprende todos los aspectos del funcionamiento y operatividad de los sistemas de información organizacional y la dependencia entre procesos y áreas de la organización.

- *Riesgo Financiero*: Son todos aquellos que se derivan del manejo de recursos de la organización, entre los cuales podemos encontrar, ejecución presupuestal, elaboración de los estados financieros, entre otros.

- *Riesgo De Cumplimiento*: Son aquellos riesgos producto del cumplimiento de requisitos legales, contractuales, de ética pública.

Como se observa en los criterios antes definidos, la identificación de criterios acordes a la importancia de sus activos de información es una parte fundamental del análisis de riesgos en una organización, y esto junto con la asociación a tipologías de riesgos se convierten en insumos para la toma de decisiones, sin embargo para establecer como se deben focalizar las actividades y los recursos, es necesario que además de identificar el riesgo inherente, también se deben conocer los controles o salvaguardas con que se están asegurando los activos, esto para poder determinar el nivel de riesgo en que se encuentra el activo de información y si es si es posible la aceptación del riesgo identificado.

IV. DEFINICIÓN DE LOS CONTROLES EXISTENTES

La definición correcta de los controles o salvaguardas existentes para cada uno de los riesgos importantes es parte vital del proceso de gestión de riesgos, ya que estos no permiten identificar si el riesgo identificado para algún activo informático se encuentra en niveles que no requieren la toma de acciones a corto, mediano o largo plazo.

Para la construcción de esquema de controles que permita identificar su madurez, es necesario definir las variables con las cuales se pueda definir con claridad el puntaje de evaluación, dentro de las variables a identificar su pueden tomar en consideración las siguientes: descripción del control, la cual debe

ser corta pero concisa, tipo de control *(preventivo, correctivo o ambos)*, forma de aplicación del control *(automática o manual)*, frecuencia de aplicación del control *(diario, semanal, mensual, por demanda)*, lo ideal es proporcionar valores de ponderación a cada uno de los grupos de variables antes descritos según las necesidades de la organización; al obtener el computo de cada grupo de variables y su resultado general, este debe ser computado con el puntaje obtenido del riesgo inherente y de esta forma obtener el puntaje del riesgo residual, el cual no permite establecer si el riesgo requiere la toma de acciones o no, de allí la importancia de la correcta definición de los controles, ya que sin estos no sería posible identificar que riesgos necesitamos tratar con mayor celeridad.

V. IDENTIFICACIÓN DE RIESGOS QUE REQUIEREN TRATAMIENTO

Con la identificación del riesgo residual asociado a cada riesgo se obtiene un nuevo mapa calor, el cual permite realizar la comparativa entre el riesgo inherente Vs riesgo residual, de esta forma contar con un panorama de la variación del riesgo de los activos, permitiendo la identificación de aquellos activos que se encuentran con algún grado de vulnerabilidad y/o posibilidad de explotación, es por esto que se hace necesaria la construcción de una escala de niveles de aceptación y tratamiento de riesgos, la cual debe estar alineada a las escalas definidas en el mapa de calor y de esta forma poder tener claridad que riesgos pueden ser aceptados dentro de apetito de riesgo de la organización y cuáles no, que riesgos requieren la toma de acciones inmediatas y cuales pueden contar con un tiempo mayor para su implementación, como se define a continuación:

TABLA VI
APETITO DE RIESGO.

Tipo de Riesgo	Tiempo de corrección
Riesgo Extremo	Inmediato
Riesgo Alto	Casi inmediatas
Riesgo Medio	Mediano plazo
Riesgo Bajo	Se acepta el riesgo, pero se verifican los controles
Riesgo Inusual	Se acepta el riesgo, pero se verifican los controles

Tomado de: Autoría Propia.

Establecida la escala de niveles de apetito de riesgo y en conjunto con el riesgo residual es posible identificar aquellos riesgos que requieren que ser tratados, por lo tanto, como se muestra en la *Fig. 1 matriz de calor*, aquellos riesgos que se encuentran en una zona de calor extremo y alto deben contar con planes de tratamiento que permitan mitigar las causas que generan el riesgo en un tiempo muy corto y de esta forma controlar los riesgos que afectan los activos, así mismo aquellos riesgos que se encuentre en zonas de riesgo medio pueden contar con planes de tratamiento con plazos de implementación de mediano a largo plazo, y aquellos que se encuentren en niveles bajo o inusual pueden ser aceptados por la organización, sin embargo es recomendable realizar monitoreo semestral de sus

condiciones de entorno, madurez de sus controles a fin de establecer que estos siguen en control o si por el contrario su nivel de exposición ha variado y se requiere tratamiento.

VI. DEFINICIÓN DE ACCIONES DE TRATAMIENTO PARA LOS RIESGOS

Identificados y clasificados los activos de información, junto con sus respectivas valoraciones de riesgo se inicia la definición de las acciones a implementar para la mitigación del riesgo, aunque en apariencia es un proceso sencillo, esta labor debe realizarse con detenimiento a fin de establecer planes que logren efectivamente su propósito de mitigación o control del riesgo, es por esto que para cada riesgo se debe analizar la causa raíz que lo origina y de esta forma establecer un plan que mitigue aquellas causas del riesgo y no las consecuencias que se pueden presentar. De la misma forma y con el fin de optimizar costos y esfuerzo del capital humano que pondrá en marcha los planes, es necesario que se analicen todos los planes de tratamiento propuestos, el objetivo de esta actividad es identificar los planes de tratamiento con acciones en común y de esta forma un plan de tratamiento macro que permitan generar avances globales de planes de mitigación de riesgo que afectan a los activos, esto a su vez permite a futuro establecer controles transversales para los riesgo con lo cual se optimiza el uso de recursos, tecnológicos, económicos y de esfuerzos humanos en la ejecución de los controles.

Por otro lado, un aspecto poco explorado en la identificación de planes de tratamiento para los riesgos que se encuentran fuera del apetito de riesgo, son aquellas actividades correctivas que se deben ejecutar en caso de materialización del riesgo, es importante que se identifiquen las acciones de corrección inmediatas con el plan de tratamiento, ya que la implementación de una plan general de tratamiento puede llegar a tomar varios meses y es importante conocer las acciones o caminos que se deben seguir al momento de presentarse un evento disruptivo mientras que se implementa el plan completo de tratamiento. Al contar con las acciones correctivas el impacto de la materialización del riesgo sobre los activos pueden contribuir a la disminución del impacto, debido a que se ejecutan acciones prontas para contener el riesgo.

Ahora bien, si el foco es la identificación de los riesgos que se encuentran fuera del apetito de riesgo para su definición de planes de tratamiento y nuevos controles, es preciso que no se dejen a un lado aquellos riesgos que se encuentran en el margen del apetito de riesgo, ya que es un error pensar que al ser riesgos en niveles bajos no pueden generar mayor afectación o se encuentran controlados en su totalidad, es por esto que estos riesgos deben contar con un seguimiento general.

VII. SEGUIMIENTO AL TRATAMIENTO DE LOS RIESGOS

Una vez se tiene definidos y aprobados los planes de tratamiento

para cada uno de los riesgos que afectan los activos de información y que se encuentran fuera del apetito de riesgo de la organización, es necesario que se realicen ciclos de seguimiento a la evolución de la implementación de dichos planes; esto con el objetivo de llevar los riesgos a niveles aceptables, una estrategias posible para el seguimiento al tratamiento de riesgos, es efectuar este proceso de manera mensual sobre los riesgos niveles de riesgo residual extremo, de esta forma poder contar con un grado de disminución de los riesgos en este nivel en el menor tiempo posible, así mismo no se deben dejar atrás aquellos riegos en niveles altos y medios, ya que aquellos riesgos en zonas extremas que van siendo tratados pueden convertirse en riesgos altos o medios, por esta razón se precisa definir intervalos de seguimiento bimestral y semestral respectivamente y de esta forma dar continuidad al proceso constante de mitigación y control de los riesgos existentes en la organización.

Es importante que los seguimientos realizados sean informados periódicamente a los dueños del riesgo, esto con la finalidad de contar con el apoyo y gestión en caso de no poder evidenciar oportuna mitigación de los riesgos por aquellas personas encomendadas a dar tratamiento a los riesgos.

VIII. CONCLUSIONES

Establecer una adecuada gestión de riesgo en cualquier organización se convierte en una herramienta esencial para garantizar su mejora continua y proyección de crecimiento, ya que esta permite establecer un apropiado nivel de seguridad de sus activos, propendiendo por la identificación temprana de aquellos puntos de falla que pueden afectar la consecución de sus objetivos de negocio, es por esto que para la adecuada adopción de la gestión del riesgo se hace preciso que la definición de un marco de trabajo basado en las buenas practicas avaladas internacionalmente, sin embargo el trabajo de la gestión de riesgo no solo deben basarse en la construcción de una metodología inicial de gestión de riesgos, debe ser todo un proceso evolutivo que involucre a todos los estamentos de la organización, comenzando con procesos de sensibilización y unificación del lenguaje del riesgo, el cual permitirá en primera instancia la identificación inicial de riesgos reactivos o producto de incidentes materializado, pero que con la evolución de su modelo permitían la identificación de riesgos de forma proactiva, pasando de esta forma a la identificación de debilidades y posibles desviaciones en sus procesos, hasta la identificación de sus fortalezas y el aprovechamiento del riesgo positivo.

Para que una organización llegue a nivel de aprovechamiento de riesgo positivo, es necesario que se adopten lineamientos claros la gestión del riesgo, pero a su vez estos no deben permanecer estáticos en el tiempo, deben ir evolucionando a la par con la evolución de la organización, mejorando sus procesos de identificación de activos, evolución en la forma que se perciben y definen los controles y su madurez, interrelaciones entre riesgos y como

la materialización de un riesgo puede disparar otros riesgos asociados.

Entonces si en la organización se realiza un adecuado proceso de identificación y clasificación los activos de información y cuáles son los riesgos asociados a cada activo, sus vulnerabilidades, su nivel de exposición y los planes de acción para mitigar dichas falencias, es posible contar con una poderosa herramienta para el fortalecimiento de los procesos de la organización y el aseguramiento de la información que en esta se maneja, generando valor a la organización y alternativas para la toma oportuna de decisiones que pueden llegar a afectar los intereses propios de la organización o los servicios que esta prestas a sus clientes, así mismo, la correcta identificación de riesgos se puede ver traducida en la disminución de fallas o no disponibilidad de los servicios prestados a clientes, generando de esta manera mayor satisfacción del cliente final.

Referencias

[1] Gobierno de España, “MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos” Ver. 3, Ministerio de Hacienda y Administraciones Públicas, Madrid, 2012.

[2] ISOTools, (2015, Enero), “ISO 27001: Pilares fundamentales de un SGSI”, [OnLine], Disponible en: http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

[3] ISOTools, (2015, Enero), “ISO 27001: Pilares fundamentales de un SGSI”, [OnLine], Disponible en: http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

[4] ISOTools, (2015, Enero), “ISO 27001: Pilares fundamentales de un SGSI”, [OnLine], Disponible en: http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

[5] ISOTools, (2015, Mayo), “¿Cómo clasificar los activos de seguridad en un SGSI?”, [OnLine], Disponible en: http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

[6] ISOTools, (2015, Mayo), “Las Claves del Éxito para la Gestión de Riesgos”. [OnLine], Disponible en :https://www.isotools.org/pdfs-pro/whitepaper-claves-exito-gestion-riesgos.pdf?utm_medium=email&_hsenc=p2ANqtz-9YbMBrokoqeTgwZXi9-uFQLlXSvnJ1ksCd9t9fIVfT_MtxkvNzMexJ1FblQXDNvbRfrPXdoydgCTUuQdVW2JcU2Cak9Q&_hsmi=15296836&utm_content=15296836&utm_source=hs_automation&hsCtaTracking=2071b1f5-fe74-498e-81e1-cdf6e4acc6cc%7C99784546-6700-430c-884a-02384fc80b20

[7] Alcaldia Mayor de Bogotá, “Inventario De Activos De Información”, [OnLine], Disponible en: http://secretariageneralalcaldiamayor.gov.co/sites/default/files/lineamiento_11_inventario_de_activos_de_informacion.pdf

[8] Universidad Nacional de Lujan,“Material adicional del Seminario Taller Riesgo vs. Seguridad de la Información”, [OnLine], Disponible en: http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

[9] Ministerio de Educación, Cultura y Deporte de Espana, “Introducción a la seguridad informática”, [On Line], Disponible en: ,http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1

[10] Markus Erb, “Gestión de Riesgo en la Seguridad Informática”, [On Line], Disponoble en: :https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

[11] Ministerio de Salud, Argentina., “Conceptos básicos de la gestión de riesgos”, [OnLine], Disponible en: http://www.msal.gob.ar/salud-y-desastres/index.php/informacion-para-comunicadores/conceptos-basicos-de-la-gestion-de-riesgos

[12] Icontec, “NTC-ISO27001:2013”, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2013

[13] Icontec, “NTC-ISO 31000:2009”, Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2011

[14] INN, “NCh-ISO 31010”, Primera Edición, Instituto Nacional de Normalización, 2013

[15] iso27000.es, “Sistema de Gestión de la Seguridad de la Información”, [OnLine], Disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

[16] Leonardo Cameno, (2015, Mayo), “Gestión de Riesgos”, [OnLine], Disponible en: http://seguridadinformacioncolombia.blogspot.com.co/2010/05/gestion-de-riesgos.html