Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507, (Diciembre 2015)

Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001

[Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001]

Francisco Nicolás Javier Solarte Solarte[1], Edgar Rodrigo ENRIQUEZ ROSERO[2], Mirian del Carmen Benavides Ruano[3]

[1]Ingeniero de Sistemas, Especialista en Multimedia educativa, Especialista en Auditoria de Sistemas, Especialista en Administración de la Informática Educativa, Magister en Docencia. Docente Asistente de carrera, Universidad Nacional Abierta y a Distancia UNAD (Pasto, Nariño, Colombia).
francisco.solarte@unad.edu.co

[2]Ingeniero de Sistemas, Especialista en Alta Gerencia, Especialista en Redes y Servicios Telemáticos, MsC(c). en Electrónica y Telecomunicaciones. Docente Auxiliar de carrera, Universidad Nacional Abierta y a Distancia UNAD (Pasto, Nariño, Colombia).
edgar.enriquez@unad.edu.co

[3]Ingeniera de Sistemas, Especialista en Docencia Universitaria, Especialista en Informática y Telemática, Especialista en Administración de la Informática Educativa, Magister en Gestión de la Tecnología Educativa. Docente Auxiliar de carrera, Universidad Nacional Abierta y a Distancia UNAD (Pasto, Nariño, Colombia).
mirian.benavides@unad.edu.co

Resumen. El artículo tiene como objetivo desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002. Se presentan los resultados de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, clave de seguridad, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo que permitieron establecer el diagnóstico de seguridad actual. Posteriormente se aplica una lista de chequeo basada en la norma, para verificar la existencia de controles de seguridad en los procesos organizacionales. Finalmente y de acuerdo a los resultados del análisis y evaluación de los riesgos, se proponen los controles de seguridad para que sean integrados hacia el futuro dentro de un SGSI que responda a las necesidades de seguridad informática y de la información acorde a sus necesidades.

Palabras Clave: análisis y evaluación de riesgos**,** estándar ISO 27001, seguridad informática, seguridad de la Información, SGSI.

Abstract. The article aims to develop the skills of software engineers to be able to conduct diagnostic projects for implementation and implementation of information security - ISMS aligned with ISO / IEC 27001 and the control system proposed ISO / IEC 27002 standard. The article presents the results of applying the phases of audit and analysis methodology and risk assessment with the design and implementation of various instruments such as questionnaires applied to key security administrators experience interviewing staff users of information technologies and systems, penetration testing and testing that allowed the diagnosis of current security. Subsequently a checklist based on the rule applies to verify the existence of security controls in the organizational processes. Finally, according to the results of analysis and risk assessment security controls to be integrated into the future within an ISMS that meets the needs of computer security and information according to your needs it is proposed.

Keywords: Audit, ISMS, standard ISO 27001, information security, analysis and risk assessment**.**

1. Introducción

Actualmente los sistemas de información, los datos contenidos en ellas y la información son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada frente a las posibles intrusiones derivadas de las vulnerabilidades existentes en sus sistemas de seguridad. Una manera efectiva de descubrir estas vulnerabilidades y amenazas existentes es iniciando los procesos diagnósticos que permitan establecer el estado actual de la seguridad dentro de la organización, teniendo en cuenta la normatividad vigente y los procesos de análisis y evaluación de riesgos.

El análisis y evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información permiten establecer el estado actual de la organización, identificar las causas de vulnerabilidades y proponer soluciones de control que permitan su mitigación.

El diagnóstico permitirá en un futuro el diseño, implementación e implantación de un Sistema de Gestión de Seguridad de la Información - SGSI alineado al estándar ISO/IEC 27001, capaz de controlar las vulnerabilidades, amenazas y los riesgos de seguridad a que se ve expuesta la organización.

Para lograr una adecuada protección de los activos informáticos, los sistemas de información, los datos y la información, es necesaria la intervención de todo el personal de la empresa, incluyendo a los directivos que deben avalar el proyecto y brindar el apoyo a todo el personal que esté involucrado en el manejo de los activos y sistemas informáticos. Estas acciones deben estar enmarcadas en un proceso lógico, sistemático, documentado, que pueda ser difundido internamente para garantizar la gestión correcta de la seguridad informática y de la información, siguiendo el ciclo de mejora continua (planear, hacer, verificar y actuar - PHVA).

Inicialmente se trata de comprender la norma ISO/IEC27001 en cada uno de los dominios, para determinar el alcance de su aplicabilidad. Una vez definidos los

dominios y determinados los activos existentes, se aplica la metodología para realizar análisis y evaluación de riesgos respecto a los tres criterios de información que son la confidencialidad, la integridad y la disponibilidad de la información.

La siguiente tarea consiste en la verificación de la existencia de controles de seguridad existentes en la empresa y su aplicación; ya que pueden estar incluidos dentro de los procesos de calidad organizacionales. Estos deben ser comparados con los controles definidos en la norma ISO/IEC 27002 como políticas y procedimientos; el resultado servirá de base para el diseño, la implementación e implantación futura de un SGSI como respuesta a los riesgos encontrados.

En el artículo se muestra un conjunto de instrumentos que posibilitan realizar el análisis y evaluación de riesgos, las técnicas utilizadas para conocer y comprender el estado actual de las organizaciones empresariales evaluadas y que pueden ser aplicados para realizar procesos de auditoría a la seguridad.

Finalmente se explica la metodología para aplicar el proceso de análisis y evaluación de los riesgos desde la fase inicial de conocimiento del sistema, la fase de identificación de las vulnerabilidades, amenazas y riesgos de seguridad determinando el nivel de riesgo a que se ve expuesta la organización, por probabilidad e impacto en los criterios de confidencialidad, integridad y disponibilidad de la información, para luego establecer un sistema de control acorde a los hallazgos encontrados.

2. Fundamentos Teóricos

En el marco normativo de los estándares relacionados con la seguridad informática y de la información, está incluida la familia de estándares ISO/IEC 27000 e ISM3, que son normas específicas para la gestión de seguridad de la información y pueden ser aplicables a cualquier organización, independientemente de su tamaño o actividad. Otros estándares relacionados son los de calidad ISO 9001, medio ambientales como ISO 14000, de TI como el estándar CobIT y de entrega de servicios ITIL.

2.1 Estándares ISO/IEC 27001 e ISO/IEC 27002

Las normas ISO/IEC 27001 y la ISO/IEC 27002 especifican los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI, además especifica los requerimientos para la implementación de controles de seguridad frente a las necesidades de toda la organización, frente a un proceso específico o un servicio, según el objetivo y los alcances del SGSI que se haya definido.

El estándar ISO/IEC 27001 comprende dos secciones de acuerdo a GUTIERREZ (2013).

En la primera se especifican cinco cláusulas enfocadas a características metodológicas del SGSI, que tienen estricto cumplimiento para obtener la certificación, dentro de ellas están: 4. Sistema de Gestión de Seguridad de la Información SGSI, 5. Responsabilidad de la Dirección, 6. Auditorías Internas, 7. Revisión de la Dirección y 8. Mejora continua del SGSI.

En la segunda se definen los controles para la gestión de la seguridad de la información que están determinados por el estándar ISO/IEC 27001 y asociados con cada uno de los dominios que están en el Anexo A, desde los denominados como A5 hasta A18 en la actualización del año 2013.

En su libro Nueve Claves del éxito, Calder (2006) hace una descripción del contenido de cada uno de los dominios:

x Dominio A.5. Política de Seguridad de la información x
Dominio A.6. Organización de seguridad de la Información x
Dominio A.7. Gestión de Activos de información (AI) x
Dominio A.8. Seguridad de los recursos humanos x Dominio
A.9. Seguridad Física y Medioambiental x Dominio A.10.
Gestión de operaciones y comunicaciones x Dominio A.11.
Control de acceso lógico
x Dominio A.12. Adquisición, desarrollo y mantenimiento de sistemas de información
x Dominio A.13. Gestión de incidentes de seguridad de la información x
Dominio A.14. Gestión de la continuidad de las operaciones x Dominio
A.15. Cumplimiento Regulatorio

Para cumplir con el estándar, es necesario la existencia de unos factores y condiciones que garanticen el éxito tales como: el apoyo incondicional por parte de la dirección general, la alineación de los objetivos de seguridad con los objetivos de la organización, la compatibilidad de los controles con la cultura organizacional, el conocimiento de los requerimientos de seguridad, el conocimiento de la administración de los riesgos, los canales de comunicación con los empleados para dar a conocer los aspectos de seguridad, la disposición de las políticas y procedimientos de seguridad, y los mecanismos para la medición de efectividad del programa de seguridad de la información, las políticas, los controles y planes para el tratamiento del riesgo.

Corti, Betarte & De la Fuente (2005) en su artículo denominado "Hacia una implementación exitosa de un SGSI" citado por Pallas Mega (2009) establecen un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma. El siguiente cuadro especifica los principales procesos que indica la norma mapeados con las etapas del ciclo PHVA.

Tabla 1. Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27001.
Fuente: (Gustavo Pallas Mega, 2009, p 10 de 186)

Ciclo PHVA	**Procesos**
Planear (***Plan***)	Establecer el contexto. Alcance y Limites Definir Política del SGSI Definir Enfoque de Evaluación de Riesgos Identificación de riesgos Análisis y Evaluación de riesgos Evaluar alternativas para el Plan de tratamiento de riesgos Aceptación de riesgos Declaración de Aplicabilidad
Hacer	Implementar plan de tratamiento de riesgos
(***Do***)	Implementar los controles seleccionados Definir las métricas Implementar programas de formación y sensibilización Gestionar la operación del SGSI Gestionar recursos Implementar procedimientos y controles para la gestión de incidentes de seguridad
Verificar (***Check***)	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI
Actuar (***Act***)	Implementar las mejoras identificadas para el SGSI Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

En general, se puede afirmar que el tema de seguridad de la Información no es sólo un tema eminentemente técnico, sino que también involucra procesos del negocio y actividades de gobierno corporativo, que aseguren una continua gestión de los riesgos y aseguramiento de los niveles de seguridad requeridos por la organización.

La norma ISO/IEC 27002, especifica el sistema de controles aplicables a la seguridad de la información alineados a la norma ISO/IEC 27001 en cada uno de los dominios y procesos. Esta norma es la guía de implementación de los controles aplicables a la seguridad de la información en forma de políticas y procedimientos.

De acuerdo a Ureña león (2011), la norma ISO/IEC 27002 incluye los siguientes apartes: la estructura del estándar y la descripción de la estructura de la norma, la evaluación y tratamiento del riesgo, el documento de la Política de seguridad y su gestión, los aspectos organizativos de la seguridad de la información, la gestión de activos, la seguridad ligada al talento humano, la seguridad física y ambiental y seguridad de los equipos, la gestión de comunicaciones y operaciones, la gestión de servicios por terceros, la protección contra código malicioso y descargable, las copias de seguridad, la gestión de la seguridad de las redes, la manipulación de los soportes, el intercambio de información, la gestión de acceso de usuarios, el control de acceso a la red, el control de acceso al sistema operativo, el control de acceso a las aplicaciones y a la información, los controles criptográficos, la seguridad de los archivos de sistema, la gestión de incidentes de seguridad de la información y mejoras, la gestión de la continuidad del negocio, el cumplimiento de requisitos legales, y el cumplimiento de las políticas y normas de seguridad.

2.2 Seguridad informática y de la información

La seguridad informática: La seguridad informática está relacionada con las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos. Los procesos se estructuran con el uso de estándares, normas, protocolos y metodologías para mitigar y minimizar los riesgos asociados a la infraestructura tecnológica.

Seguridad de la información: La seguridad de la información está relacionada con las medidas preventivas aplicadas con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad. La información puede presentarse en diversos formatos y medios tanto físicos, como electrónicos. Por lo tanto, las organizaciones deben adoptar y adaptar metodologías para proteger los archivos y registros, mantener en funcionamiento una infraestructura tecnológica adecuada que sirva para la custodia y salvaguarda de la información.

2.3 Vulnerabilidad, amenaza y riesgo

Los conceptos de vulnerabilidad, amenaza y riesgo están relacionados entre sí haciendo parte de la concepción de la seguridad en distintos ámbitos, que también han sido aplicados en referencia a la seguridad informática y de la información. En este artículo se tomará las vulnerabilidades como las debilidades del sistema o activo informático en cuanto a seguridad, las amenazas son los posibles ataques que puede hacer una persona (interna o externa) aprovechando las vulnerabilidades o los ataques que ya se han presentado, y los riesgos como las diversas maneras en que se presenta la amenaza y la posibilidad de que ese ataque llegue a presentarse en una organización específica.

Vulnerabilidad informática: Son las posibilidades que se dan en el mismo ambiente, en el cual las características propician y se vuelven susceptibles a una potencial amenaza, por lo tanto, se puede considerar como la capacidad de reacción ante la

presencia de un factor que pueda posibilitar una amenaza o un ataque. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización.

De acuerdo a una de las clasificaciones, los tipos de vulnerabilidades que pueden presentarse a nivel informático son: Vulnerabilidad física, Vulnerabilidad natural, Vulnerabilidades del hardware, Vulnerabilidades del software, Vulnerabilidad de medios o dispositivos, Vulnerabilidad de las comunicaciones, Vulnerabilidad Humana.

Amenazas informáticas: Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización.

Las amenazas pueden presentarse por acciones criminales en las que intervienen seres humanos violando las normas y las leyes, o sucesos de orden físico por eventos naturales que se puede presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico, o por negligencia que son las omisiones, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad.

Las amenazas a los sistemas de información están latentes cada que se interactúa con los ellos, al utilizar dispositivos de almacenamiento externos, al ingresar a sitios web, por la inconformidad de empleados insatisfechos dentro de la misma organización. De acuerdo a lo anterior las amenazas pueden ser de varios tipos, entre ellas tenemos las amenazas por intercepción, modificación, interrupción o generación.

Riesgos informáticos: Los riesgos informáticos son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura.

2.4 Sistema de gestión de seguridad de la información – SGSI

El SGSI, tiene como propósito el establecimiento de los mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro de un conjunto de estándares previamente determinados para evaluar la seguridad. El objetivo principal es identificar cada uno de los activos y personas que apoyan los sistemas informáticos a través del proceso de gestión de riesgos asociados a los procesos y servicios que presta la organización con apoyo de TI, además de verificar la existencia de controles de seguridad que permitan integrarlos a las políticas y procedimientos para mitigar los riesgos encontrados.

Dentro de los activos informáticos se han establecido dos categorías que permiten diferenciarlos de acuerdo con su naturaleza y existencia física, la primera categoría agrupa los activos intangibles y la segunda los activos tangibles. Dentro de los activos intangibles están los bienes inmateriales tales como: relaciones inter institucionales, capacitaciones del personal, las habilidades y motivación de los empleados, las bases de datos, las herramientas tecnológicas, el conocimiento y la experiencia, y los procesos operativos. Los bienes tangibles son los de naturaleza material como: mobiliario, infraestructura tecnológica, espacios físicos, materiales y elementos de trabajo, equipos informáticos, hardware de redes, equipos de protección eléctrica, cableado estructurado, teléfonos y plantas telefónicas, entre otros.

3. Metodología

Para realizar la auditoría a la seguridad de la información, el proceso se dividió en etapas sucesivas y sistemáticas; en cada una de ellas se trata de establecer objetivos y metas claras con productos entregables, donde los productos resultado de la primera etapa servirán para adelantar la segunda y los de las segunda servirán para proseguir con la tercera etapa y así sucesivamente, ya que se plantea que la auditoría debe ser periódica o permanente dependiendo de la organización y los cambios en la tecnología de información usada en el tratamiento y procesamiento de la información.

Fase I. Determinación de vulnerabilidades, amenazas y riesgos: En esta fase se hace el estudio de las vulnerabilidades, amenazas y riesgos para los procesos y sistemas implementados actualmente en las organizaciones, que fueron objeto de la investigación.

Para recolectar la información se aplicaron las técnicas de la observación directa mediante visitas programadas y entrevistas aplicadas a los profesionales de sistemas encargados de la administración del área informática, la seguridad informática y usuarios de los sistemas. Con el conocimiento claro del área o sistema auditado, se definen y describen las vulnerabilidades o debilidades encontradas, las amenazas por parte de personal interno o externo al tratar de cometer un ilícito o un ataque, y los riesgos naturales y no naturales a que está expuesta la organización.

Finalmente se selecciona los dominios y objetivos de control de la norma ISO/IEC 27001, que es la norma que se tendrá en cuenta para la evaluación de la seguridad en los procesos, servicios, personal y sistemas de información de las organizaciones. Mediante los instrumentos diseñados se evalúa todos los dominios en cuanto a su cumplimiento, pero el proceso de análisis de riesgos se enfoca, teniendo en cuenta los activos informáticos disponibles en las organizaciones y a las vulnerabilidades, amenazas y riesgos que puedan presentarse.

Tabla 2. Inventario de activos.

INVENTARIOS DE ACTIVOS IMPORTANTES	
Tipo de activo	**Nombre de activo**
Activo de información	Datos de clientes, datos de proveedores, Documentos Físicos, manuales. Inventarios de hardware, contratos con terceros, otros
Software y licencias	Software SO licenciado, Software ofimático licenciado, licencias de uso de software en outsourcing, otras licencias
Hardware	Características del hardware de equipos, dispositivos de red, dispositivos móviles, equipos de protección eléctrica, otros.
Instalación red eléctrica	Red e instalaciones eléctricas para computadores, (norma RETIE), sistema de protección de aterrizaje eléctrico (polo o malla a tierra)
Servicios de terceros	Conectividad a internet, mantenimiento y soporte de hardware, mantenimiento y soporte de software, soporte y actualizaciones en software en outsourcing
Personal	Personal área informática, usuarios de los sistemas

La siguiente tabla muestra algunas de las vulnerabilidades, amenazas y riesgos de seguridad más usuales que se identificaron inicialmente, que luego deberán comprobarse mediante pruebas documentales, fotográficas y aplicando software especializado:

Tabla 3. Vulnerabilidades, amenazas y riesgos inicialmente identificados

Cod	Vulnerabilidad	Amenazas	Riesgos Potenciales
Hardware			
V3	Falta de equipos UPS's para contingencias	Cortes de energía o sobrecargas en los equipos.	Pérdida de información, daños en los equipos, pérdida de tiempo en procesos repetidos.
Software			
V4	Software no licenciado	Virus informáticos, malware, utilizar exploit.	Mal funcionamiento de sistemas, destrucción de SO, destrucción o modificación de aplicativos e inf.
V7	Software con problemas de seguridad en el desarrollo	Ataques de Inyección SQL, información inconsistente, errores de integridad de datos	Pérdida o modificación de información, robo de claves de usuario, modificación de datos, bases de datos inseguras por permisos y privilegios no definidos

V8	Actualización del SO en los equipos	Utilización de ataques exploit	Intrusión no autorizada en los equipos de usuarios para modificación, borrado o robo de información, ataques de DoS, consecución de privilegios.
Seguridad Física			
V11	No existe control de acceso físico a las oficinas y equipos informáticos	Manipulación de información sin control de acceso, ataques intencionados a equipos, desastres provocados.	Robo, destrucción, modificación o borrado de información, destrucción o desarticulación física de equipos.
Seguridad lógica			
V14	Deficiente control de acceso a los sistemas	Suplantación de identidad	Robo de datos, alteración o destrucción de los mismos, suplantación de identidad de usuarios, robo de claves de usuarios
Redes de comunicaciones			
V15	Vulnerabilidad de navegadores utilizados	Inyección de código SSI, ataques con código XSS	Alteración en el funcionamiento del código, programas y sitios, información sin autorización.
Personal			
V17	Falta de una política de seguridad clara	Ataques no intencionados, ingeniería social, phishing.	Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.

Fase II. : Análisis de riesgos y diagnóstico de la seguridad de la información: En esta fase se realizará el proceso de análisis y evaluación de riesgos de acuerdo al estándar MAGERIT que permite valorar los riesgos en cada uno de los criterios de información evaluados, identificando las posibles causas que los originan y que posteriormente permitan definir un sistema de control de seguridad de acuerdo a los hallazgos confirmados, lo que permitirá disminuir el impacto en la organización y probabilidad de ocurrencia de los mismos.

El proceso de análisis y evaluación de los riesgos se lleva a cabo teniendo en cuenta el estándar MAGERIT versión 3.0, que permite hacer la clasificación de amenazas y riesgos, los activos informáticos, muestra las escalas de valoración y los criterios de información que será evaluados.

Posteriormente se aplican las listas de chequeo que son utilizadas para verificar y determinar la existencia de controles de seguridad informática y de la información, diseñadas de acuerdo a la norma ISO/IEC 27002.

Finalmente en el proceso se aplican cuestionarios que son aplicados al personal clave que realmente posea la información, para confirmar la existencia de vulnerabilidades, amenazas y riesgos; la aplicación de listas de chequeo, permite establecer la existencia de controles de seguridad, estos cuestionarios servirán como evidencia para confirmar los hallazgos y definir los controles que sean necesarios.

Escala para cuantificar los activos informáticos: **Muy Alto (MA):** valor > $ 20.000.000; **Alto (A):** $ 20.000.000 <valor> $ 10.000.000; **Medio (M):** $ 10.000.000 <valor> $ 5.000.000; **Bajo (B):** $ 5.000.000 <valor> $ 1.000.000; **Muy Bajo (MB):** $ 1.000.000 <valor> $ 500.000

Escala de valoración de los activos informáticos de acuerdo al daño que se pueda causar en ellos: **Daño catastrófico:** 10; **Daño grave:** 7 – 9; **Daño moderado:** 4 – 6; **Daño Leve:** 1 – 3; **Daño Irrelevante:** 0

Tabla 4. Dimensiones o criterios de evaluación seguridad de la información

Dimensiones						
Tipo de Activo	**Nombre de Activo**	**Confidencialidad.** Daño: que lo conociera quien no debe	**Integridad** Perjuicio: que estuviera dañado o corrupto	**Disponibilidad.** Perjuicio no tenerlo o no poder utilizarlo	**Autenticidad** Perjuicio: no saber exactamente quien hace o ha hecho cada cosa	**Trazabilidad** Daño: no saber a quién se le presta el servicio?
Activo de información	Datos de clientes y proveedores	[9][A]	[9][A]	[6][M]	[8][A]	---------- ---
Software o aplicación	software sin licencia	---------- -----	---------- ---	[10][MA]	---------- --	---------- ---
Hardware	Servidor de internet	[9][A]	[9][A]	[6][M]	[6][M]	---------- ---
Instalación eléctrica	Cumplimiento de normas	---------- ----	[7][M]	[7][M]	---------- -	---------- --
Personal	Personal usuario sistemas	[9][A]	[9][A]	[9][A]	[9][A]	[9][A]

Ahora se procede a la valoración de los riesgos en las escalas de probabilidad e impacto:

Escala de valoración de la probabilidad de ocurrencia: **Frecuencia Muy alta (MA):** 1 o más veces al día; **Frecuencia Alta (A):** 1 vez a la semana; **Frecuencia Media (M):** 1 vez cada mes; **Frecuencia Baja (B):** 1 vez cada dos meses; **Frecuencia Muy Baja (MB):** 1 vez cada seis meses

Escala de valoración de impacto: **Leve (L):** 0% a 30%; **Moderado (MO):** 31% a

65%; **Catastrófico (C):** 66% a 100%

Tabla 5. Valoración de los riesgos por probabilidad e impacto

Riesgos / Valoración		**Probabilidad**					**mpacto**		
		MA	**A**	**M**	**B**	**MB**	**L**	**M O**	**C**
Hardware (En porcentaje)									
R1	Falta de sistemas UPS				20			65	
Software (En porcentaje)									
R2	Software no licenciado					5			100
R3	Sistemas sin restricciones de acceso		70						100
R4	Falta de control de cambios del software				20		30		
Seguridad física (En porcentaje)									
R5	Pocos controles de restricción acceso		70					70	
R6	Falta de control ambiental		70					70	
R7	Falta de control de acceso físico a las oficinas			50			30		
Seguridad lógica (En porcentaje)									
R8	Deficiente control de acceso a los usuarios		70					70	
Redes y Comunicaciones (En porcentaje)									
R9	Vulnerabilidades de los navegadores		70					70	
R1	Uso de aplicaciones poco			50			30		
0	confiables para compartir archivos y asistencia remota								
Personal (En porcentaje)									
R1 1	Usuarios no se han capacitado adecuadamente		70				30		
R1 2	Personal de soporte sin experiencia			50				70	

Fase III. Definición de controles para el diseño del SGSI que incluya políticas y procedimientos para mitigar los riesgos: En esta fase se hace el estudio de las causas que originan los hallazgos. Una vez confirmados, se define los controles apropiados de acuerdo a la norma ISO/IEC 27002 se establece su tratamiento, y finalmente, se diseñan las políticas y procedimientos dentro de las cuales se incluyen los controles, y que finalmente irán en el diseño del SGSI.

Confirmados los hallazgos, se establecen los controles de seguridad como políticas y procedimientos de acuerdo a la norma ISO/IEC 27002, se definen los más apropiados para mitigar los riesgos y se adaptan para la organización. Luego se determina el tratamiento de los riesgos para aceptarlos, transferirlos a terceros o aplicar los controles y posteriormente éstos se integran a las políticas y a los procedimientos institucionales si existen.

Al culminar, se elabora el informe final que servirá de insumo para el diseño e implementación del SGSI teniendo en cuenta el ciclo de mejora contínua PHVA que permita las actividades para planear, hacer, verificar y actuar, que intervengan y permeen todos los procesos y servicios dentro de la organización.

4. Resultados

Dentro de los resultados generales más importantes de la aplicación de la metodología de análisis y evaluación de riesgos, y los instrumentos diseñados están:

Algunos de los problemas de seguridad en las organizaciones evaluadas están relacionados principalmente con: el desconocimiento sobre aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática y de la información que comprometen seriamente la imagen Institucional.

Las posibles causas origen de los problemas están: mínima cultura en el tema de seguridad de información, la organización no formal del área informática, la no existencia de responsables de la seguridad, no existencia o falta de cumplimiento de políticas y procedimientos de seguridad dentro de la organización, falencias en el manejo de los inventarios de activos informáticos, en general la competencia limitada del personal para proteger los activos informáticos y de información frente a las amenazas y riesgos a que se ven enfrentadas.

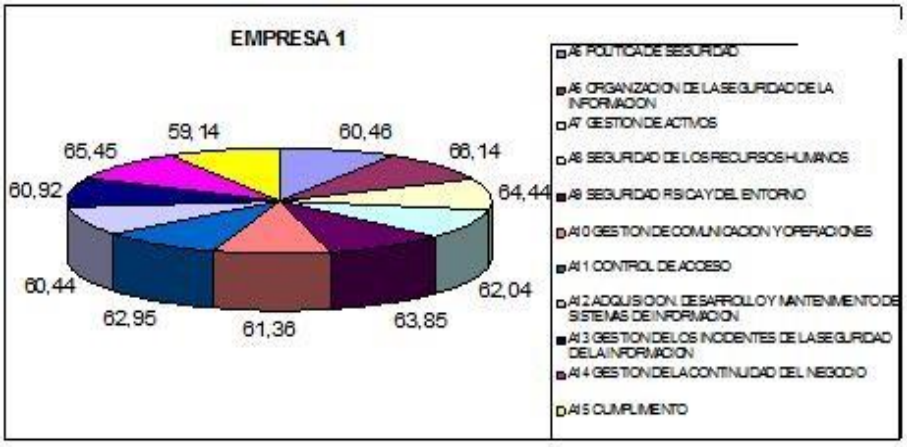

Fig. 1. Resultado diagnóstico controles ISO/IEC 27001. Fuente: Solarte Francisco, 2013

La figura muestra los resultados del diagnóstico/análisis de brecha para los dominios de la norma ISO/IEC 27001 en porcentaje (%) de cumplimiento al aplicar la lista de chequeo diseñada. Los porcentajes en cada uno de los dominios son asociados a la escala de madurez e interpretados de acuerdo al porcentaje de cumplimiento. Para los cálculos totales, se determinaron por el promedio de los valores para obtener el nivel de madurez en cada dominio.

Como resultado del análisis se encontró que frente a los requerimientos de la norma ISO/IEC 27001 e ISO/IEC 27002, las organizaciones analizadas obtuvieron una calificación promedio de 2, lo que quiere decir que se encuentra en un nivel de madurez ***Repetible*****,** cuya interpretación es que se han adelantado actividades para la implementación de controles y buenas prácticas, que en su mayoría siguen un patrón regular, pero que no se han formalizado y por ende su ejecución depende de cada persona.

El resultado muestra que es imperativo el apoyo y compromiso real de la gerencia o administración para el proceso de diseño, implementación e implantación de un SGSI de acuerdo a los resultados de la auditoria; además se debe formalizar los procesos y procedimientos que así lo requieran y documentarlos, en la mayoría de casos se verificó la no existencia de procesos por lo cual se debe definir los procesos y procedimientos faltantes; también se debe implementar un sistema de control de seguridad informático estableciendo mecanismos que permitan la medición permanente orientadas hacia la mejora de la seguridad de la información y al diseño, implementación e implantación de un SGSI en cada una de las organizaciones de acuerdo a sus necesidades.

4. Conclusiones

Del proceso diagnóstico llevado a cabo, se puede concluir que no existe una cultura de seguridad de la información dentro de las organizaciones, tampoco existe sistemas de control de seguridad informática y de información, y mucho menos, procesos y procedimientos documentados para protección de la información.

De los resultados obtenidos se puede concluir que no existe un compromiso real de las directivas, que los empleados no son conscientes de los objetivos que se pretende con el sistema de control de seguridad de la información y que el personal del área informática no está capacitado para asumir esta responsabilidad. Por tanto, es fundamental que las organizaciones cuenten con un marco normativo de seguridad, que permita aplicar la auditoría basada en la norma ISO/IEC 27002.

Del proceso de auditoría a la seguridad de la información se concluye que este proceso debe ser continuo y que debe ser realizado por los entes de control interno de cada organización, y periódico por empresas auditoras externas que permitan hacer la evaluación y seguimiento del sistema de control de seguridad informático para el diseño, implementación e implantación de un SGSI adecuado a sus necesidades.

5. Referencias bibliográficas

Alexander, Alberto.: Diseño de un Sistema de Gestión de Seguridad de la Información – óptica ISO 27001:2005. Alfaomega. Bogotá - Colombia (2007)

Alegsa.: Definición de vulnerabilidad, http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Bisongo, M.: Metodología para el aseguramiento de entornos informatizados, http://materias.fi.uba.ar/7500/bisogno-tesisdegradoingenieriainformatica.pdf.

Calder, Alan.: Nueve Claves para el Éxito: Una visión general de la implementación de la norma NTC – ISO/IEC 27001. Instituto Colombiano de Normas Técnicas y Certificación ICONTEC, Bogotá – Colombia (2006)

Cevallos, Soledad: Modelo de madurez según CobIT. http://es.scribd.com/doc/110374485/Modelo-de-Madurez-Segun-Cobit

Gómez, J.: La seguridad y la confidencialidad de la información es obligación de todos, http://www.merca20.com/la-seguridad-y-confidencialidad-de-la-informaciones-obligacion-de-todos/

Gutiérrez, John Hegel: Guía GAP 1.0, http://es.scribd.com/doc/180290502/SGSI27001-2012-Guia-Gap-1-0

ICONTEC: Compendio, sistema de gestión de seguridad de la información (SGSI). Instituto
Colombiano de Normas Técnicas y Certificación ICONTEC, Bogotá – Colombia (2009)
ISO 27000: El directorio de la norma ISO 27000, http://www.27000.org/other.htm

ISO: Gestión de la seguridad de la información - 27001 ISO / IEC, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Ministerio de Comunicaciones: Modelo de seguridad de la información, http://programa.gobiernoenlinea.gov.co/apc-aafiles/5854534aee4eee4102f0bd5ca294791f/ModeloSeguridad_SANSI_SGSI.pdf

Pallas Mega, Gustavo.: Metodología de Implantación de un SGSI en un grupo empresarial jerárquico: Tesis de Maestría (Ingeniería en Computación): Universidad de la República, p 186. Montevideo - Uruguay (2009)

Puig, Toni: Implementación de un sistema de gestión de seguridad, http://www.mailxmail.com/curso-implantacion-sistema-gestion-seguridad/delimitar-entornoalcance-sgsi

Sánhez, Luis Enrique, Villafranca, Daniel, Fernández Medina, Eduardo, Piattini, Mario: MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES, http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2sesion3%283%29.pdf

Sótelo, Marcos: Implantando un SGSI alineado a ISO/IEC 27001, http://ecomputacion.net/av200/course/view.php?id=2

Ureña León, Edsel Enrique: Sistema de Gestión de la seguridad de la Información – SGSI, http://edselenrique.wikispaces.com/file/view/SGSI.pdf