UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja
Máster universitario en Seguridad Informática

ISO 27001 PARA PYMES

Trabajo Fin de Máster

Presentado por: Parra Giraldo, Ángela María

Director: Del Barrio García, Alberto

Ciudad: Medellín – Colombia.
Fecha: 18-10-2014

Resumen

El uso de las tecnologías informáticas en todos los aspectos de la cotidianidad humana, ha conducido a que la seguridad informática no sea sólo una preocupación de las grandes compañías, sino también de las PYMES, las cuales inconscientemente en gran parte quedan vulnerables ante la falta de controles que les permitan protegerse de intrusiones no deseadas. Aquí se propone una metodología de implementación de la ISO 27001 para que sea aplicada en la implementación de Sistemas de Gestión de Seguridad de la Información en PYMES. Busca facilitar las tareas que en este tipo de empresas se dificultan, debido a los recursos limitados con los que cuenta en presupuesto, personal y conocimiento. Adicional a esto, se propone unas prácticas iniciales mínimas como punto de partida para organizaciones que no tienen controles de seguridad de la información, como principio para iniciar un ciclo de mejora continua, que permita que la organización alcance una maduración mayor a medida que la cultura de seguridad de la información, se afianza dentro de la compañía. Aunque se proponen soluciones básicas para PYMES, al analizar ataques a grandes compañías, se encuentran estás propuestas útiles como estrategia preventiva desde los procedimientos y controles aún para este tipo de empresas.

Palabras Clave: ISO27001, PYMES, PHVA, SGSI, Seguridad

Abstract

The use of information technology in all aspects of human life, has led to the fact that computer security is not just a concern for large companies, but also of Small and Medium Enterprises (SMEs), which are more vulnerable because of the lack of controls that allow to protect themselves from undesired intruders. In this work, I propose an ISO 27001 methodology for implementing an information safety management system in SMEs, in order to facilitate the tasks that become more difficult for this type of companies, due to their limited resources such as budget, staff, and knowledge. In addition to this, some minimum initial practices are proposed as a starting point for organizations that do not have security control information. This is done as a way to initiate a cycle of continue improvements, which allows SMEs to achieve a greater maturity while the culture of information security grows within them. Although basic solutions are proposed for SMEs, several attacks to large companies are also analyzed. I consider that the solutions derived from this study can be applied as a preventive strategy to include in the procedures and controls for SMEs.

Keywords: ISO27001, SMEs, PDCA, SGSI, Management

ÍNDICE

Índice de Ilustraciones

Índice de Tablas

1. Introducción

La seguridad informática, se ha convertido en nuestro siglo, en un pilar fundamental para garantizar la estabilidad y permanencia en el tiempo de las empresas; sin importar su tamaño, grandes o pequeñas, la tecnología es la base sobre la que se mueven la mayoría de transacciones de las compañías, convirtiéndose en un activo más de las mismas, y soportando la base para sostener y garantizar la confidencialidad, integridad y disponibilidad de la información.

Otro aspecto que hace que la seguridad informática hoy, se considere un tema de suma importancia, es que ahora no es solamente un tema de empresas, sino que tiene un alcance que va hasta la persona misma, independiente del entorno social, familiar, empresarial, cognitivo y cualquiera que se pueda considerar, hay en todo momento un enlace entre los datos personales y los datos empresariales, que convergen en un mundo integrado de información, que traslada al ciberespacio una réplica de la realidad. Esto genera infinitas posibilidades de inter-operar a nivel económico y social, pero también permite intrusiones realizar ataques, posibilitando afectar a las personas, a las empresas, a la sociedad e incluso al mundo entero.

Esta dimensión de la seguridad informática es clara en las grandes compañías, las cuáles invierten una gran porción presupuestal en la implementación de técnicas, contratación de personal capacitado, formación de personal, investigación y desarrollo de estrategias, que les permitan asegurar su estructura física y lógica y limitar al máximo las posibilidades de un ataque exitoso. Este no es el caso de las pequeñas compañías, en las que existe desconocimiento, escases de recursos, escepticismo y la confianza de creer que un ataque informático nunca llegará a ellas; esto las convierte en blancos muy vulnerables, ante los más mínimos ataques.

Debido a lo expuesto en los párrafos anteriores, se fundamenta la importancia de generar una metodología de implementación de la norma ISO 27001, que soportándose en las buenas prácticas de implementaciones exitosas, pueda servir de guía, para que las pequeñas compañías, entiendan, dimensionen, e implementen la seguridad informática, con sus limitados recursos.

Según diversos estudios internacionales (Giorgetty, 2010), el recurso humano, es el eslabón más débil de la seguridad, por esta razón hay una parte fundamental de la seguridad informática que está asociada a las personas, que son a su vez, activos de las empresas.

El desafío es lograr desarrollar una metodología que conduzca a las empresas pequeñas a implementar modelos de seguridad tan efectivos como los de las grandes compañías, pero que sean viables de acuerdo a sus recursos limitados y coherentes con el tipo de la organización.

1.1. Motivación y Enfoque

La seguridad informática, es el resultado de una gestión dinámica y evolutiva, que no se asocia exclusivamente a inversión económica, ni es un estado finito al que se pueda llegar, (Pallas, 2009) pero que si debe permitir una medición, que ayude a evaluar y monitorear, los riesgos a los que se enfrenta una organización, para tomar decisiones conscientes y razonables, frente a qué hacer para minimizar o asumir, el impacto de la materialización de los mismos.

En este trabajo se pretende, investigar si se puede adoptar una metodología de implementación de la seguridad informática en las pequeñas compañías, que sirva para implementar sistemas de gestión de seguridad de la información como la ISO 27001. Se marcan lineamientos que sirven como guía, para facilitar el entendimiento y seguimiento, por compañías que no cuenten con una maduración de seguridad, bien sea por su estructura reducida o escases de recursos económicos o humanos.

Se realizará una documentación de los principales ataques que fueron llevados a cabo en los últimos tiempos, con el fin de ilustrar los riesgos potenciales a los que se expone cualquier compañía y se evalúan métodos mediante los cuales se pueden evitar, conduciendo al impulso de la cultura de la seguridad.

En el trabajo se analizan dos PYMES una es una litografía y otra es un hotel, por lo tanto los ejemplos se presentan utilizando estas dos empresas como casos de estudio. No se aplica todo a las dos, sino que se usa en cada una lo que pueda ser más representativo que pueda demostrar la utilidad de cada propuesta.

1.2 Objetivos

- Analizar las situaciones de seguridad que presentan las Pymes y algunos ataques de las grandes compañías.
- Generar estrategias a partir de los resultados, para implementar procesos y controles que permitan implementar un Sistema de Gestión de Seguridad de la Información SGSI.
- Investigar los estudios previos a este trabajo y encontrar soluciones a la medida de las PYMES que permitan evolucionar los procesos hacia la seguridad de la información.
- Generar lineamientos que guíen a las pequeñas empresas, a minimizar riesgos a partir de la gestión de procesos y optimizando sus recursos.
- Generar una metodología de análisis de riesgos que facilite esta tarea para cualquier compañía.

- Crear plantillas para facilitar la documentación de un Sistema de Gestión de Seguridad de la información según la norma ISO 27001.

1.3 Estructura del Documento

En el Capitulo 2 se presenta el Estado del Arte del tema objeto de este trabajo, contiene un grupo de definiciones y contextualización del documento. Se aclaran conceptos importantes para el entendimiento de la investigación, se hace una presentación de la seguridad en compañías grandes y en pymes, se presentan diferentes estándares de seguridad y metodologías de evaluación de riesgos que son relevantes para la investigación, se realiza un resumen, de diferentes estudios que han tratado el mismo caso, con sus principales características, se realiza un marco normativo de las principales normativas a considerar en España y en Colombia en cuanto a seguridad de la información se refiere.

En el Capitulo 3 se plantea la hipótesis, objetivos de la investigación y se explica el método de investigación utilizado. En el Capítulo 4 se desarrolla la contribución de la investigación, se presenta una metodología de análisis de riesgos, como una plantilla en Excel que facilita esta tarea para las PYMES, se plantean una serie de controles iniciales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), se presenta la estructura de la política de seguridad de la información y una serie de políticas específicas que conducen al apoyo estratégico del cumplimiento de los controles iniciales propuestos, igualmente se referencian los anexos, donde se realizan modelos de procedimientos que permitan la implementación de las políticas, y que finalmente contienen los resultados de la investigación de los dos casos de estudio que se analizaron durante la investigación, consistentes en dos PYMES de diferente tamaño y diferentes recursos económicos, tecnológicos y de personal, haciendo un análisis de su configuración física y lógica, pasando por los diferentes ataques que han tenido y haciendo una comparación entre ambas para encontrar puntos similares de falencias, que son las que al final inspiran todo el desarrollo de la investigación. En el Capítulo 5 se exponen las conclusiones de la investigación, la respuesta a la hipótesis planteada y la contribución futura del trabajo.

2. Contexto y Estado del Arte

2.1. Definiciones

A través del documento se hablará de algunos conceptos importantes como los que se definen en este apartado(*Compendio seguridad de la información* Marzo 2013; Roa Buendía, 2013):

Activo: Cualquier cosa que tiene valor para la organización.

Amenaza: Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

Ataque: Un ataque informático es un método por el cual, un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático, ya sea un ordenador, una red privada, la privacidad de un usuario u organización, etc.

Autenticación: Es la propiedad que permite confirmar que una persona o máquina es quien dice ser y no está siendo suplantada por un impostor.

Autorización: Es la propiedad que después de que el usuario o máquina ha sido autenticado, le permite acceder a los distintos privilegios para los cuales fue autorizado.

Cifrado: Es la función que permite que la información no sea útil para cualquiera que no supere la autenticación.

Confidencialidad: Propiedad que determina que la información no esté disponible, ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Exploit: Es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

Gusano Informático: (Worm) Es un malware que tiene la propiedad de propagarse de ordenador a ordenador, sin la ayuda de una persona, se duplica a sí mismo dentro de un mismo ordenador y hacia otros.

Hacker: Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Malware: También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

No Repudio: Ante una relación entre dos partes, se evita que cualquiera de ellas pueda negar que participa de esa relación.

Phishing: o suplantación de identidad, es un término informático, que denomina un modelo de abuso informático, y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.

Riesgo Residual: Nivel restante de riesgo después del tratamiento del riesgo.

Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad.

Tratamiento del Riesgo: Proceso de Selección e Implementación de medidas para modificar el riesgo.

Troyano: Se denomina 'caballo de Troya' a un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

Virus: es un malware que tiene por objeto alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Vulnerabilidad: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

Botnet: Hace referencia a un conjunto o red de robots informáticos o bots (equipos zombis), que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y se usan para diversas actividades criminales.

Otras definiciones complementarias: Todas las contenidas en la norma ISO 27001 e ISO 27005.

2.1. Contextualización

Es un fenómeno, la incursión de la tecnología en el mundo, el uso del internet (Banco Mundial, 2014) puede visualizarse como un indicador en crecimiento, y en esta expansión, se genera el espacio de comunicación universal, que permite llegar a cualquier lugar. Hogares, empresas, instituciones, colegios, todos los lugares del mundo, interconectados a través de la internet. Esta globalización, ha generado impactos sociales importantes (Katz & Rice, 2006), pero también ha permitido un desarrollo en positivo de los alcances económicos, porque incorpora facilidades tanto personales como empresariales, que se sirven de la tecnología, para optimizar los procesos productivos, comunicativos, educativos y demás. Aun así, hay también impactos negativos, esta intercomunicación, trae consigo la necesidad de establecer límites, hasta dónde se quiere como persona o como empresa permitir esta intercomunicación. Un ejemplo para contextualizar lo que se expone es: "se puede vivir en un vecindario muy poblado, pero se ponen puertas y ventanas para limitar hasta donde quiero compartir lo que hay al interior de mi casa con mis vecinos", a eso se le llama privacidad, "estas puertas y ventanas tienen cerraduras, para que abran y cierren sólo cuando se desee", a eso se le llama seguridad; haciendo una comparación con el mundo virtual, del que se goza a través de internet, se tiene, un espacio de puertas y ventanas abiertas sin cerraduras, si la seguridad y la privacidad no son consideradas; es aquí cuando nace un nuevo componente importante, *la seguridad informática*, que permite limitar el

alcance de todos los elementos que participan en un mundo intercomunicado e interconectado.

La seguridad informática entra a hacer parte del juego, tiempo después de que el juego ya empezó, por lo que no todos se han enterado de la necesidad de tenerla en cuenta; en el libro de Seguridad Informática de José Fabián Roa Buendía, en su primer capítulo (Roa Buendía, 2013), explica de manera simple, por qué y de qué protegerse.

Sin pensarlo, se creó un mundo paralelo, una realidad virtual, a la que se trasladaron grandes problemáticas de la vida real. Hay nuevos escenarios para delinquir, nuevas formas de socializar, nuevas plataformas para la educación; los acontecimientos interoceánicos, encontraron cortos caminos para llegar justo a tiempo; las guerras, ahora también se llevan en la virtualidad, atacando objetivos importantes de su contrincante. En conclusión, es posible moverse entre un mundo y otro como si fueran el mismo.

Debido a la velocidad con la que ha evolucionado la tecnología, se tienen grandes brechas generacionales, entre los que recibieron la tecnología a la mitad de su vida con la llegada de los computadores, y apenas lograron asimilar su llegada, bien sea por la dificultad económica que implicaba su adquisición cuando los computadores pudieron realmente llegar a los hogares en los años 80, la ubicación geográfica en la que nacieron o cualquier otra razón, y los que nacieron en la era tecnológica, de Smartphone, Tablet, computadores portátiles. Ambas generaciones hoy comparten el mismo espacio geográfico, económico y social (Portal Wap de Personal, 2012), y se tienen problemáticas diferentes con unos y otros.

Toda la historia de la evolución tecnológica y sus impactos positivos y negativos, sirven para documentar la importancia de impactar a las personas, que son los activos vivos de las empresas, y que hasta ahora se consideran el eslabón más débil de la seguridad informática (Giorgetty, 2010).

2.2 La Seguridad de la Información y La Seguridad Informática

Según Jeimy J. Cano, PhD., CFE, la (González, 2011) *Seguridad de la información* es la disciplina que nos habla de los riesgos, amenazas, análisis de escenarios, buenas prácticas y esquema normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías, para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. Y la *Seguridad Informática*

(Cano, 2011), es la disciplina que se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías, antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

Considerando lo revisado por Tim Kayworth y Dwayne Whitten, una adecuada estrategia de seguridad de la información deberá articular tres elementos claves (Cano, 2011):

• Balance de necesidades: protección de la información y desarrollo de negocios.
• Aseguramiento del cumplimiento normativo.
• Desarrollo y afianzamiento de la cultura corporativa

Ilustración 1 Seguridad de la información vs Seguridad Informática

2.3 La seguridad en las grandes Compañías

Las empresas de tecnología son líderes en implementaciones de seguridad, destacando a IBM, Microsoft, HP, Amazon ya que estas son empresas que dentro de sus líneas de productos y servicios tienen oferta de seguridad informática para otras empresas. Otras muy destacadas como Google y Apple, son empresas que tienen una gran cobertura sobre los usuarios a nivel mundial, de éstas, Google ha implementado estándares de seguridad en sus productos. Todas éstas empresas, están calificadas dentro de las mejores empresas del mundo, incluso a nivel de ingresos y percepción en el mercado, por lo tanto estas

compañías, se convierten en importantes retos para los ciberdelincuentes, quién las encuentran como objetivos para atacar.

Por esto, y cada vez más, ellas se preocupan por la seguridad de la información y la seguridad informática, no sólo para sí mismas, sino también para los usuarios y empresas cliente, incluso en ocasiones, a pesar de ser competidoras entre sí, también se realizan alianzas para trabajar unidas por un objetivo común en favor del mundo entero como se tratará más adelante. A diferencia de otro tipo de empresas que al tratarse de seguridad informática, están enfocadas en protegerse a sí mismas, en estas empresas líderes es importante también pensar en cómo sus avances en seguridad se trasladan a sus clientes, brindándoles protección y confianza en sus productos.

A continuación una breve presentación de estas empresas:

Apple (Wikipedia, 2003-2015)**:** Empresa multinacional estadounidense, fundada por Steve Jobs, Steve Wozniak, Ronald Wayne en 1976. Entre los equipos de hardware más conocidos de la empresa se cuenta con equipos Macintosh, el iPod, el iPhone y el iPad; entre el software de Apple se encuentran los sistemas operativos Mac OSX e iOS, el explorador de contenido multimedia iTunes, la suite de productividad iWork, la suite de edición de video Final Cut Studio, edición de audio en pistas Logic Studio, intercambio de datos entre servidores Xsan, editor de imágenes RAW Aperture, Navegador web Safari, etc.

Google (Alto Nivel, 2014)**:** Empresa fundada hace 16 años por Larry Page y Sergey Brin. El motor de búsqueda Google, la página web más visitada del mundo, posee también páginas como YouTube, Blogger, posee un difundido sistema operativo Android y tiene un gran conjunto de aplicaciones con las que presta diversidad de servicios; además trabaja en importantes proyectos como los lentes de realidad aumentada Google Glass. También ha adquirido empresas especializadas en diferentes ramas de la tecnología, entre ellas Nets Labs y busca transformarse en un proveedor de internet gracias a Fiber.

Microsoft Corporation (Wikipedia, 2002-2015)**:** Multinacional Estadounidense, Fundada en 1975 por Bill Gates y Paul Allen. Los creadores del sistema operativo Windows. Compañía dedicada al sector de la informática, hardware y software, ha expandido sus actividades mediante la creación de hardware, como la nueva Tablet Surface, además de poseer otros negocios, entre ellos el Xbox.

IBM (Wikipedia, 2003 - 2013)**:** International Business Machines, es uno de los principales proveedores de hardware y software del mundo. Desde herramientas para correr campañas de marketing exitosas, hasta el prestigio de haber comercializado con éxito la primera computadora de escritorio. Ofrece servicios de infraestructura, alojamiento de internet y

consultoría en una amplia gama de áreas relacionadas con la informática, desde computadoras centrales hasta nanotecnología. Fundada en 1911.

Amazon (Wikipedia, 2006 - 2015)**:** Compañía Estadounidense de comercio electrónico y servicios de cloud computing a todos los niveles. Fundada por Jeff Bezos en 1994 y lanzada el 16 de Julio de 1995.

HP (Wikipedia, 2004 - 2015)**:** Compañía Estadounidense, una de las mayores empresas de tecnologías de la información del mundo, Fundada en 1939 por William Hewlett y David Packard. Comercializa hardware y software, además de brindar servicios de asistencia relacionados con la informática.

En una publicación del sitio web llamado Alto Nivel (Andrés Cardenal, 2014), se presenta a Google, Amazon y Apple como la triada accionaria más valiosa de las empresas tecnológicas, por su impresionante poder de marca y altos márgenes de ganancias.

Todas estas compañías poseen aplicaciones certificadas en diferentes estándares de seguridad informática, esto les ayuda a ganar la confianza de sus usuarios, al mismo tiempo que genera una cultura de la seguridad de la información en las empresas que las implementan.

El enfoque principal es generar una cultura de seguridad informática, que parte de las personas y que se replica progresivamente en todas las etapas y capas de la organización, permitiendo sinérgicamente confabular en favor de la seguridad los esfuerzos de todos los agentes que intervienen. Las actividades de capacitación permanente de los empleados, clientes y proveedores, buscando generar concienciación en la seguridad, es uno de los insumos más importantes en los procesos de la cultura de la seguridad informática.

Estas empresas multinacionales, tienen que cumplir con las regulaciones que en cada país donde tengan presencia les apliquen, y proveer a sus clientes mecanismos de cumplimiento de la legislación a través de sus ofertas de productos, que también tienen la visión de estándares internacionales que permiten la implementación de políticas y controles para la gestión de la seguridad de la información en las compañías.

2.5. Problemática de seguridad en las PYMES

Las PYMES son el componente más grande de las economías a nivel mundial, en estos apuntes sacados de la tesis doctoral de Milka E. Escalera(Escalera, 2007) habla de la importancia de las PYMES y se presentan las siguientes estadísticas:

"En diferentes investigaciones empíricas, las pequeñas y medianas empresas han sido señaladas como uno de los principales participantes del crecimiento económico así como de la creación de empleos de un país.

En Estados Unidos y Canadá las pequeñas empresas constituyen el 97% de todos los negocios; emplean un 57% de la fuerza laboral y producen el 45% del producto interno bruto (Ibrahim y Goodwin, 1986). Leebaert (2005) reporta que las PyMES de Estados Unidos representan un 99,7 % de todos los empleadores en Estados Unidos.

Según, (Hernández y Bruch, 1983 citados por Dart y Sarkar, 1990) en los países como: Alemania, el 98% de todas las empresas industriales son PyMES con 500 trabajadores o menos, y producen casi el 33% del volumen de negocio industria; igualmente en Italia, Suecia, Japón, Indonesia y en Malasia las PyMES contribuyen en promedio con un 90% del total de empleos.

Mientras que la Conferencia de Industrias Británicas señala que en los países industrializados, el 60 a 80 % del total de establecimientos corresponden a las PyMES cifra que se incrementa cada día (Cota, 1998). Otros autores como Wijewardena y Cooray (1995) señalan que, a nivel mundial, el 90% del total de las empresas son PyMES"

La seguridad informática en la mayoría de las pymes es algo reactivo, una vez que sucede una situación de ataque, se tiene que atender y remediar, con las consecuencias y pérdidas que haya que asumir, poniendo en riesgo incluso la estabilidad y continuidad del negocio y en la seguridad de la información, no se tienen medidas exhaustivas que permitan garantizar la protección de la información y el cumplimiento legal, al que se tenga referencia.

Cuando de seguridad informática se habla, en las PYMES hay errores comunes que se repiten y que suelen ser la causa de la mayoría de incidencias informáticas de la empresa(Juliá, n.c.):

1. Pensar que a nadie le interesan mis datos.

2. No incluir la seguridad en los contratos con empleados, clientes y proveedores.

3. Olvidar la gestión de la red informática.

4. Pensar en Reparar, no en mantener.

5. Basta con tener un antivirus y un Firewall.

Estos errores se deben en su mayoría a situaciones como:

1. Desconocimiento del alcance de los delitos informáticos.

2. Falta de recursos para invertir en soluciones costosas. Muchas veces no hay un departamento informático.

3. Desconocimiento real de lo que se necesita en la empresa para garantizar la seguridad y la ley.

4. Empresas familiares con poca o ninguna asesoría profesional.

5. Exceso de confianza con empleados y proveedores.

A diferencia de las grandes empresas, la cultura de la seguridad es poca o inexistente, ya que no es una amenaza inminente considerada por los propietarios o administradores, y la seguridad está cimentada en el sentido común de los usuarios del sistema.

Cuando el sistema se comporta extraño porque algo falla, se asume que se tiene un virus y se acude a un técnico de sistemas para desinfectar o formatear, pero no se tiene idea real de los alcances del ataque, el temor más grande es que no se pueda usar el sistema o que se pierda alguna información, pero en realidad se desconoce completamente la información relevante que debería analizarse sobre origen y finalidad del ataque, consecuencias del ataque, protección futura para evitar que se repita.

Las PYMES por pequeñas que sean, en su mayoría cuentan con:

- Acceso a Internet.

- Página Web.

- Correo Electrónico.

- Computadores administrativos.

- Programa de facturación y contabilidad.

- Información de propietarios, clientes, empleados y proveedores.

- Conmutador telefónico o línea telefónica con discados locales, nacionales e internacionales.

Las regulaciones de gobierno, en los diferentes lugares del mundo, están cada vez más interesados en estandarizar procesos que deberían ser transversales a cualquier organización sin importar su tamaño. Muchas de estas exigencias requieren plazos de cumplimiento que son prioritarios y más cortos para las empresas de gran tamaño, pero que también cobijan a empresas medianas y pequeñas, con exigencias acordes a su capacidad económica, pero también de acuerdo al impacto de la información que estas manejan.

Este tipo de regulaciones son difíciles para las PYMES, ya que no todas cuentan con el conocimiento, o capacidad de contratación para implementarlas.

En Colombia, hay algunas regulaciones gubernamentales que exigen a compañías de cualquier tamaño su implementación, con los rangos de tiempo establecidos según el número de empleados. Para el sector de alimentos, la implementación de un sistema de gestión de control de puntos críticos; para todo tipo de empresas la implementación de un sistema de gestión de salud ocupacional y seguridad industrial, para los establecimientos hoteleros la implementación de la norma técnica de turismo sostenible muy similar a la ISO 14001. Con independencia de que se acuda a un organismo certificador o no, estas regulaciones deben cumplirse, y ante una visita de cualquier ente regulador, se debe estar en capacidad de demostrar el cumplimiento de las mismas, so pena de multa o cierre del establecimiento evaluado. A nivel fiscal se deben entregar los medios magnéticos anualmente, que son documentos electrónicos en formato XML que dan información sobre facturación, ingresos y otra información de interés gubernamental sobre las empresas, que luego cruzan para hacer controles de evasiones de impuestos, etc. Desde el año 2013, se ha implementado de la ley del Habeas Data, que es similar a la ley de protección de datos personales en Europa, esto para todo tipo de empresas, por lo que vemos que poco a poco, se establece la obligatoriedad de las compañías de cualquier tamaño de preocuparse por la seguridad de la información. En España, también como se menciona en el apartado anterior, se tiene el ENS (Esquema Nacional de Seguridad), la LOPD (Ley de Protección de Datos Personales), la LSSICE (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico), la ley de Firma electrónica, Factura electrónica.

Esto tiene un proceso que va más allá de las exigencias legales, y es la de cimentar las bases para que la seguridad informática tenga un espacio en la vida de las personas y en la operación de las empresas, minimizando los riesgos que esto supone.

2.6. Ataques informáticos

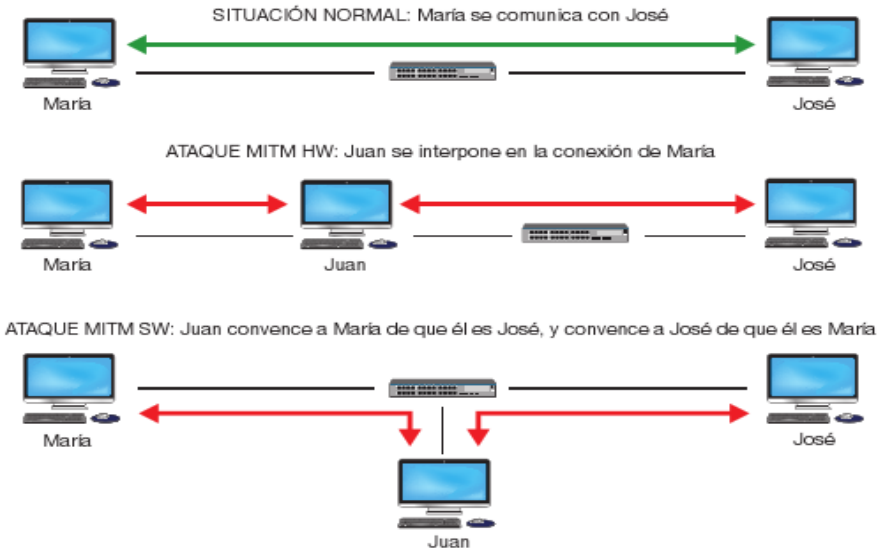
Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).

Hay diversos tipos de ataques informáticos. Se puede ampliar esta información en los libros de Seguridad Informática (Roa Buendía, 2013) y el libro de Hacking Ético de Carlos Tori (Tori, 2008).

Los ataques informáticos más frecuentes son:

Denegación de servicio, también llamado ataque DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Man in the middle, a veces abreviado MitM, es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas.



Ataques de REPLAY ó ARP, una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

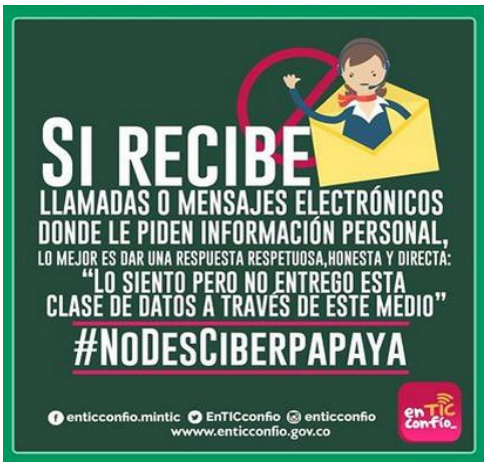
Ataque de día cero, ataque realizado contra un ordenador, a partir del cual se explotan ciertas vulnerabilidades, o agujeros de seguridad de algún programa o programas antes de que se conozcan las mismas, o que, una vez publicada la existencia de la vulnerabilidad, se realice el ataque antes de la publicación del parche que la solvente.

Ataque por fuerza bruta. No es necesariamente un procedimiento que se deba realizar por procesos informáticos, aunque este sistema ahorraría tiempos, energías y esfuerzos. El sistema de ataque por fuerza bruta, trata de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que se busca, y que permite el acceso al sistema, programa o archivo en estudio.

Ingeniería Social: Es una técnica que trata de engañar y persuadir, con la pretensión de conseguir información útil y significativa de su víctima, que puede ser desde un pequeño usuario que lee un correo y al ejecutar el archivo adjunto tiene que revelar datos personales o contraseñas, hasta una empresa o gran organización escogida con ánimo de causar el mal.

La ingeniería Social es uno de los principales temas, que compete a la hora de hablar de seguridad informática, ya que en el esfuerzo para crear una cultura de seguridad, en las organizaciones y en la sociedad, es importante dotar a las personas de la capacidad de discernir si se está siendo víctima de esta técnica. En esta capacidad de discernimiento se requiere desarrollar habilidades para cuestionarse, desconfiar y prevenir, para evitar que un ataque tenga éxito.

Esta necesidad se ha identificado, y es por esto que hoy en día se realizar diferentes campañas de sensibilización que se originan por las entidades bancarias, entidades gubernamentales, entidades educativas. A continuación una imagen del Ministerio de las TIC de Colombia, con uno de estos mensajes.



Un artículo de revista de Junio de 2013, revela que las PYMES no se encuentran preparadas para contrarrestar o prevenir ataques informáticos. (Wallis, 2013) Este argumento lo basa en que la seguridad de las mismas apenas se asemejan a los niveles de seguridad de un hogar, teniendo en cuenta, que estas empresas mueven importantes flujos de dinero o información, es un blanco ideal para los atacantes.

Este mismo artículo, revela los retos más importantes que están enfrentando las PYMES en este aspecto:

La ingeniería social, se ejecuta a través de labores de inteligencia en sistemas de información y comunicaciones, redes sociales y correo electrónico, con el objetivo de obtener información de valor para el negocio.

•**Amenazas internas:** Cada día son más frecuentes los casos donde el robo de la información se da desde el interior de la compañía. La pérdida económica se cuantifica de acuerdo con la calidad de la información.

•**Tendencia Traiga su Propio Dispositivo (BYOD):** los puntos terminales están evolucionando, la integración de dispositivos como tabletas y Smartphone generan nuevas puertas y puentes de ataques a los sistemas informáticos, teniendo en cuenta que se está habilitando una conexión a la red corporativa desde un punto externo. Las pymes deben saber cómo administrar los nuevos dispositivos que los empleados están conectando en sus negocios.

•**La Nube:** Las pymes están simplificando sus sistemas de información. La tendencia es administrar dichos sistemas desde la nube, conectando su centro de datos a Internet.

•**APT (Amenazas Persistentes Avanzadas):** Es una tendencia muy fuerte para 2013, consiste en ataques dirigidos a sistemas informáticos de uso específico que afecta la estación de trabajo y a los sistemas informáticos. Estás amenazas son silenciosas, de bajo perfil y de características aparentemente normales.

2.6.1. Algunos ataques informáticos importantes a grandes compañías (Zahumenszky, 2014)

1) El gran *hack* de EE.UU.: 160 millones de usuarios: No tiene nombre oficial porque no afectó a una sola compañía, sino a una larga lista de ellas que incluía el índice bursátil NASDAQ, 7-Eleven, JC. Penney, JetBlue, Dow Jones o Global Payment entre otras. El ataque se prolongó durante siete años desde 2005, y robó los datos de tarjetas bancarias

de 160 millones de clientes. Cinco personas de origen ruso fueron acusadas y condenadas por el caso.

2) Adobe: 152 millones de usuarios: En octubre de 2013, Adobe reconoció haber sufrido un robo de cuentas bancarias a gran escala. La compañía comenzó dando la cifra de algo menos de tres millones de usuarios. En apenas un mes se descubrió que el ataque afectaba a 152 millones de usuarios registrados según Naked Security. Es posible que nunca se sepa la cifra exacta, porque Adobe sigue manteniendo que solo fueron 38 millones.

3) eBay: 145 millones de usuarios: Es el último gran ataque. El asalto a la base de datos de usuarios de la página de comercio online ha obligado a cambiar sus contraseñas a 145 millones de personas. Aún no se ha podido calcular el volumen de la información filtrada.

4) Heartland: 130 millones de usuarios: El hacker Albert González fue acusado de coordinar el ataque que se llevó datos de 130 millones de tarjetas de débito y crédito de la multinacional de pagos Heartland Payment Systems. Sucedió en 2008, pero no se hizo público hasta mayo de 2009.

5) TJX: 94 millones de usuarios: En enero de 2007, responsables del grupo TJX hicieron público un ataque informático que puso en peligro los datos bancarios de 94 millones de clientes entre sus cadenas de tiendas Marshals, Maxx y T.J.

6) AOL: 92 millones de usuarios: Este ataque comenzó desde dentro en 2004. Un ingeniero de la compañía que había sido despedido utilizó sus conocimientos de la empresa para infiltrarse en la red interna de AOL, y robar la lista con los correos de sus 92 millones de usuarios. Después vendió la lista online a un grupo de *spammers*.

7) Sony PlayStation Network: 77 millones de usuarios: El ataque que robó información de las cuentas de 77 millones de usuarios de los servicios PlayStation en todo el mundo supuso un duro golpe para Sony, entre otras cosas porque tardó una semana en reconocer el problema. Tuvo que compensar a los usuarios y recibió varias sanciones en países como Reino Unido.

8) Veteranos de EE.UU.: 76 millones de usuarios: Un disco duro que se envió a un servicio técnico en 2009 fue el punto por el que se robaron 76 millones de fichas personales de veteranos de guerra estadounidenses, incluyendo sus números de la seguridad social.

9) Target: 70 millones de usuarios: Aunque no tan grande en volumen como los anteriores, el ataque a la cadena de tiendas estadounidense Target fue especialmente

peligroso porque lo que los hackers se llevaron fueron números de tarjeta bancaria y claves de 40 millones de personas que utilizaron sus tarjetas en alguna tienda Target a finales de 2013. Otros 30 millones de usuarios vieron vulnerados datos personales como el teléfono o la dirección de email.

10) Evernote: 50 millones de usuarios: Este es de los pocos casos en los que la compañía reaccionó tan rápido que no hubo que lamentar daños. En marzo de 2013, Evernote envió una notificación a sus usuarios para que cambiaran sus contraseñas ante indicios de que su red había sido hackeada. No se reportó robó de información personal. La medida fue cautelar.

11) Hearbleed (Semana, 2014)**:** Es una falla en el sistema que se utiliza para cifrar información personal que circula en la red que puede incluir datos financieros y médicos. El rango de aspectos expuestos es amplio y difícil de determinar, porque el error del software le permite a los atacantes ver parte de la información que se quedó en la memoria del servidor. El mecanismo que protege los datos cuando pasan de un punto es conocido como SSL/TLS y es muy común, por lo cual Google, Yahoo, Facebook, Tumblr, Amazon Web Services y otras importantes compañías que funcionan con este sistema estuvieron en riesgo.

12) Goto Fail (Semana, 2014): A mediados de abril, Apple hizo pública una actualización de su sistema operativo OS X, porque descubrió que sus usuarios podrían ser víctimas de hackers al utilizar Internet. El problema estaba en la conexión que se establece entre el navegador de Apple -Safari- y varios sitios web, entre los que se cuentan bancos, Google y Facebook. La gran mayoría de los websites cuenta con un sistema de seguridad que protege la información que circula en la red.

13) **'Zero-day exploit' (CVE-2014-1776)** (Semana, 2014)**,** La seguridad y confiablidad de las diferentes versiones del navegador de Microsoft, Internet Explorer –que van desde la 6 hasta la 11- se pusieron en duda los últimos días de abril. Un error de programación permitió que hackers pudieran tomar control de computadoras que funcionan con el sistema operativo Windows XP. Para desespero de los usuarios, la falla, cuya existencia fue confirmada por la empresa de seguridad informática Symantec, 'congelaba' la pantalla de quienes recurrían a Explorer para navegar en Internet. El sitio de estadísticas de tecnología en internet, *NetMarket Share*, calcula que más del 50 % del mercado mundial de navegadores emplea Explorer. Pero este mecanismo quedó expuesto por la falla que afectó a los propietarios de modelos de iPhone, iPad, iPod y computadoras de Apple que funcionan con OS X.

2.7. ISO 27001 y Otros Estándares de Seguridad de la Información

2.7.1. ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

La norma ISO/IEC 27001 (*Compendio seguridad de la información* Marzo 2013) es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se busca que los aspectos trabajados dentro del SGSI se ajusten con las necesidades de la organización.

La ISO 27001 promueve un enfoque basado en procesos adoptando el modelo de Deaming, en el que se plantea un ciclo de mejora continua, a través de la repetición de las fase de "Planificar-Hacer-Verificar-Actuar" conocido como (PHVA) o (PDCA) por sus siglas en inglés "Plan-Do-Check-Act).

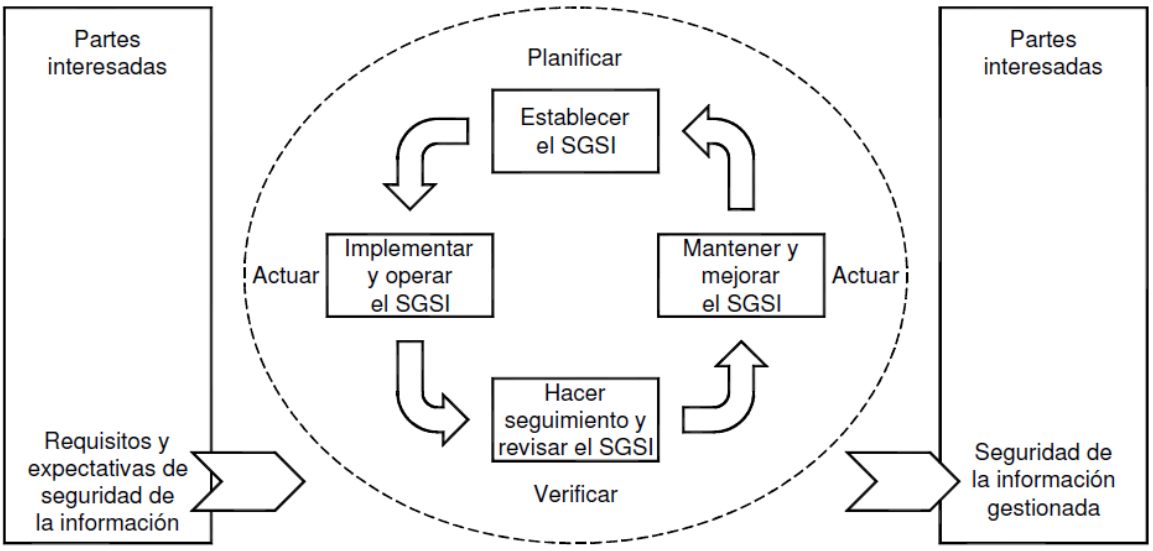


Ilustración 2 Modelo PHVA aplicado a los procesos de SGSI - ISO 27001

Tabla 1 Modelo PHVA vs proceso de la norma ISO 27001 (Tomado de compendio de seguridad de la información y Tesis de Palla)

Planificar (Plan) Establecer el SGSI	Establecer el contexto. Alcance y Límites. Definir Política del SGSI Definir enfoque de evaluación de riesgos. Identificación de Riesgos. Análisis y Evaluación de Riesgos. Evaluar alternativas para el tratamiento de riesgos. Aceptación de Riesgos. Declaración de Aplicabilidad.
Hacer (Do) Implementar y Operar el SGSI	Implementar plan de tratamiento de riesgos. 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) Hacer seguimiento y revisar el SGSI	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 (Do) Mantener y mejorar el SGSI	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 logran los objetivos previstos.

Los requerimientos de la ISO 27001 son transversales a todas las organizaciones. Pero existe una serie de requerimientos base de obligado cumplimiento para que una organización obtenga la conformidad con esta norma (Sánchez, 2009):

• **SGSI:** La organización establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado SGSI en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos. Para este propósito el proceso de esta norma, está basado en el modelo PDCA. Además, deberá controlar y mantener todos los documentos requeridos por el SGSI.

• **Responsabilidades de la administración:** La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del SGSI y asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el SGSI sea competente y esté en capacidad de ejecutar las tareas requeridas. Para ello deberá proveer las herramientas y capacitación necesaria.

• **Auditoría interna del SGSI**: La organización realizará auditorías internas al SGSI a intervalos planeados para determinar si los controles, objetivos, procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo ni cualquier otro que guarde relación con él.

• **Administración de las revisiones del SGSI**: Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el SGSI incluyendo la política de seguridad de la información y sus objetivos.

• **Mejoras del SGSI:** La organización deberá mejorar continuamente la eficiencia del SGSI a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de la administración.

ISO/IEC 27002 - Tecnología de la Información. Técnicas de Seguridad. Código de práctica para la gestión de la Seguridad de la Información - provee una guía de implementación de los controles aplicables a la seguridad de la información. Presenta once (11) cláusulas de control de la seguridad que contienen un total de treinta y nueve (39)

categorías de seguridad y por lo tanto igual número de indicaciones de Objetivos de Control, con varios Controles por cada uno de ellos. Estas cláusulas, objetivos de control y controles, son incorporados en el Anexo A de la norma ISO/IEC 27001.

Cada organización implanta sólo los controles que considera necesarios. Su principal ventaja es que la norma es neutra con respecto a la tecnología, lo que le permite su adaptación a diferentes entornos, indica qué se debe hacer de forma general pero no entrando en cómo afrontar la implantación.

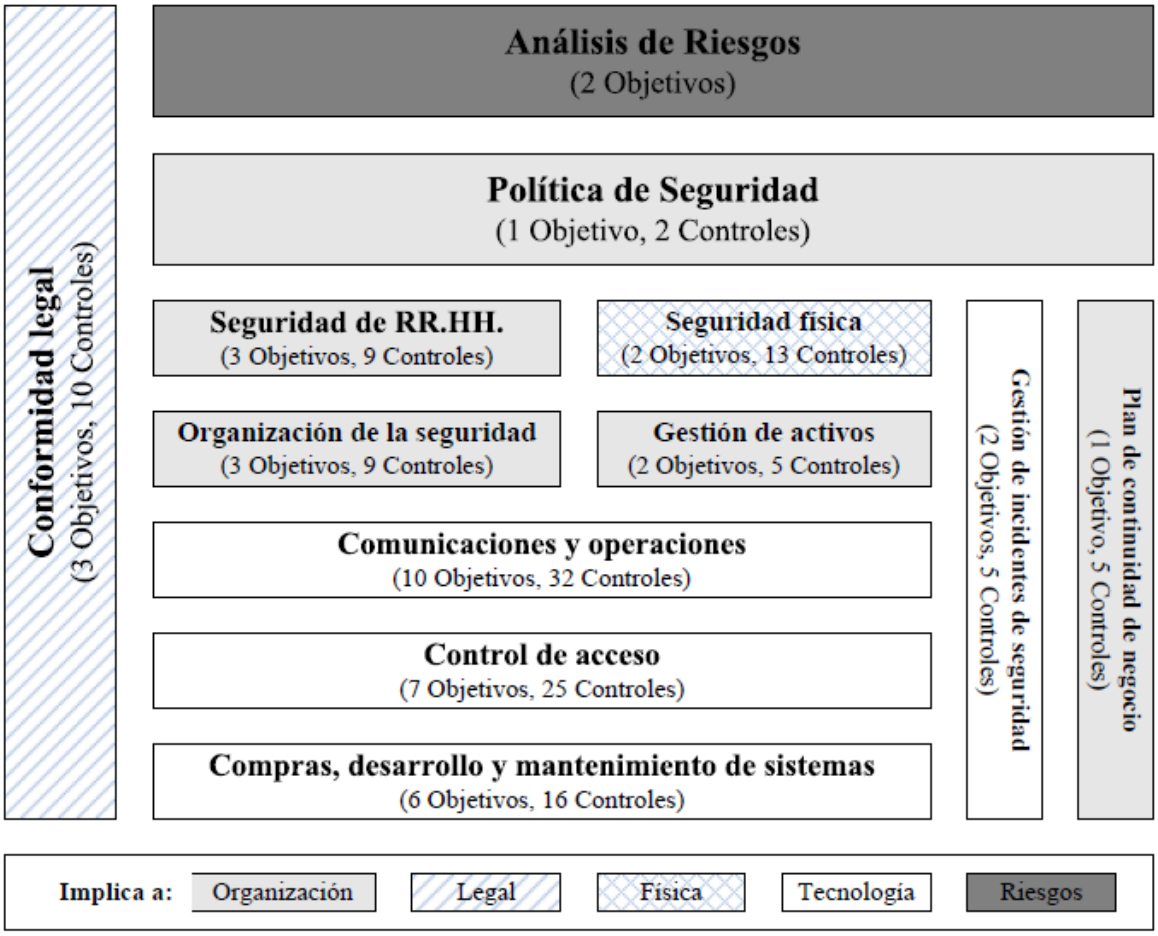


Ilustración 3 Dominios de la ISO/IEC 27002 (ISO/IEC 27002, 2007)

ISO/IEC 27003. Tecnología de la Información. Técnicas de Seguridad. Guía de Implementación de un sistema de gestión de la seguridad de la información. Se enfoca en los aspectos críticos necesarios para el diseño e implementación exitosos de un SGSI, de acuerdo con la norma ISO/IEC 27001. En la misma se describen los procesos de especificación y diseño de un SGSI, desde el inicio hasta la producción de los planes de implementación. Aquí se describe el proceso para obtener la aprobación de la dirección para implementar un SGSI, se define un proyecto para implementar un SGSI, y se brinda

orientación sobre cómo planificar el proyecto de SGSI, que da como resultado un plan de implementación final del proyecto de SGSI.

ISO/IEC 27005 (*NTC-ISO/IEC 27005: 2009*2009), Suministra directrices para la gestión del riesgo en la seguridad de la información. Brinda soporte a los conceptos generales que se especifican en la norma ISO/IEC 27001 y está diseñada para facilitar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo.

ISO/IEC 27035. Tecnología de la Información. Técnicas de Seguridad. Gestión de incidentes de seguridad de la información. Brinda orientación sobre la gestión de incidentes de seguridad de la información para empresas grandes y medianas. Las organizaciones más pequeñas pueden usar un conjunto básico de documentos, procesos y rutinas descritos en esta guía, de acuerdo con su tamaño y tipo de negocio, en relación con la situación de riesgo de seguridad de la información. También brinda orientación para organizaciones externas que prestan servicios de gestión de incidentes de seguridad de la información.

2.7.2.El Esquema Nacional de Seguridad (ENS)

Según el documento de AENOR (Gómez Fernández & Andrés Álvarez, 2012), el objeto del ENS es garantizar la seguridad de los servicios prestados mediante medios electrónicos, de manera que los ciudadanos puedan realizar cualquier trámite, con la confianza de que va a tener validez jurídica plena y que sus datos van a ser tratados de manera segura.

La ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, está siendo el motor y la guía de la administración electrónica.

El ámbito del ENS son las Administraciones públicas, los ciudadanos en sus relaciones con las Administraciones Públicas, Las relaciones entre las distintas Administraciones Públicas, y proveedores que prestan servicios para las Administraciones Públicas.

Principios del ENS

- Seguridad Integral.

- Gestión de Riesgos.

- Prevención, Reacción y Recuperación.

- Líneas de defensa.

- Reevaluación Periódica.

- Función Diferenciada.

Requisitos básicos de seguridad

- Organización e implantación del proceso de seguridad.

- Análisis y Gestión de Riesgos.

- Gestión de Personal.

- Profesionalidad.

- Autorización y control de los accesos.

- Protección de las instalaciones.

- Adquisición de Productos.

- Seguridad por Defecto.

- Integridad y actualización del Sistema.

- Protección de la información almacenada y en tránsito.

- Prevención ante otros sistemas de Información Interconectados.

- Registro de actividad.

- Incidentes de Seguridad.

- Continuidad de la actividad.

- Mejora continua del proceso de Seguridad.

Dimensiones del ENS

- Disponibilidad.

- Integridad.

- Confidencialidad.

- Trazabilidad.

- Autenticidad.

Con base al impacto que se tenga sobre cada una de las dimensiones del ENS los incidentes de seguridad se pueden clasificar en : Básico, Medio, Alto.

En este caso me parece importante mencionar que las PYMES pueden prestar servicios a las Administraciones Públicas, y en ese caso deben también ajustarse al ENS en sus relaciones con ellas.

El documento de AENOR (Gómez Fernández & Andrés Álvarez, 2012) da una explicación del ENS y su aplicación en PYMES.

2.7.3. Otros estándares de seguridad

COBIT (Objetivos de control para Tecnología de la Información) Desarrollada por ISACA y por el Instituto para el gobierno de la tecnología de información (ITGI), es una metodología y un marco de trabajo adecuado para la gestión de Tecnología de la Información (IT), orientado en el negocio y en procesos, y basado en controles. Se utiliza para planear, implementar, controlar y evaluar el gobierno de las TIC, incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Para ello considera tres dimensiones: a) los dominios, procesos y actividades de IT; b) los requerimientos de la información del negocio; y c) los recursos de IT.

COBIT, está formado por los siguientes elementos (Sánchez, 2009):

- Resumen Ejecutivo: Formado por una síntesis ejecutiva y el marco referencial. La primera proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT y la segunda le proporciona un entendimiento más detallado de los conceptos clave y principios de COBIT, e identifica dominios y procesos de COBIT).

- **El Marco Referencial:** Describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control.

- **Objetivos de control:** Contienen la definición de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de TI.

- **Directrices de Auditoría:** Contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel, para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI, con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o una recomendaciones de mejoramiento.

- **Conjunto de Herramientas de Implementación:** Lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. el conjunto de herramientas de implementación, incluye la **síntesis ejecutiva.**

COBIT Define cuatro dominios o fases, que representan los pasos necesarios para la construcción del SGSI, siguiendo el ciclo PDCA, estos dominios tienen procesos (34), que a su vez describen actividades concretas y especifican una serie de objetivos de control.

Los dominios son: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (ES), y Monitoreo y Evaluación (ME).

En particular, en el dominio PO, se centra la atención en la alineación de IT con los objetivos y estrategia del negocio, y en la gestión de riesgos. Así como en ES, se especifica un proceso de “Aseguramiento de Continuidad del Servicio / Operaciones”.

A los efectos de satisfacer los objetivos de negocio se definen siete criterios en términos de requerimientos de la información, ellos son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento (marco legal y reglamentario, normas, contratos, etc.), y confiabilidad.

En cuanto a los recursos, y para el fin propuesto, se consideran los siguientes: aplicaciones, infraestructura, información y recursos humanos.

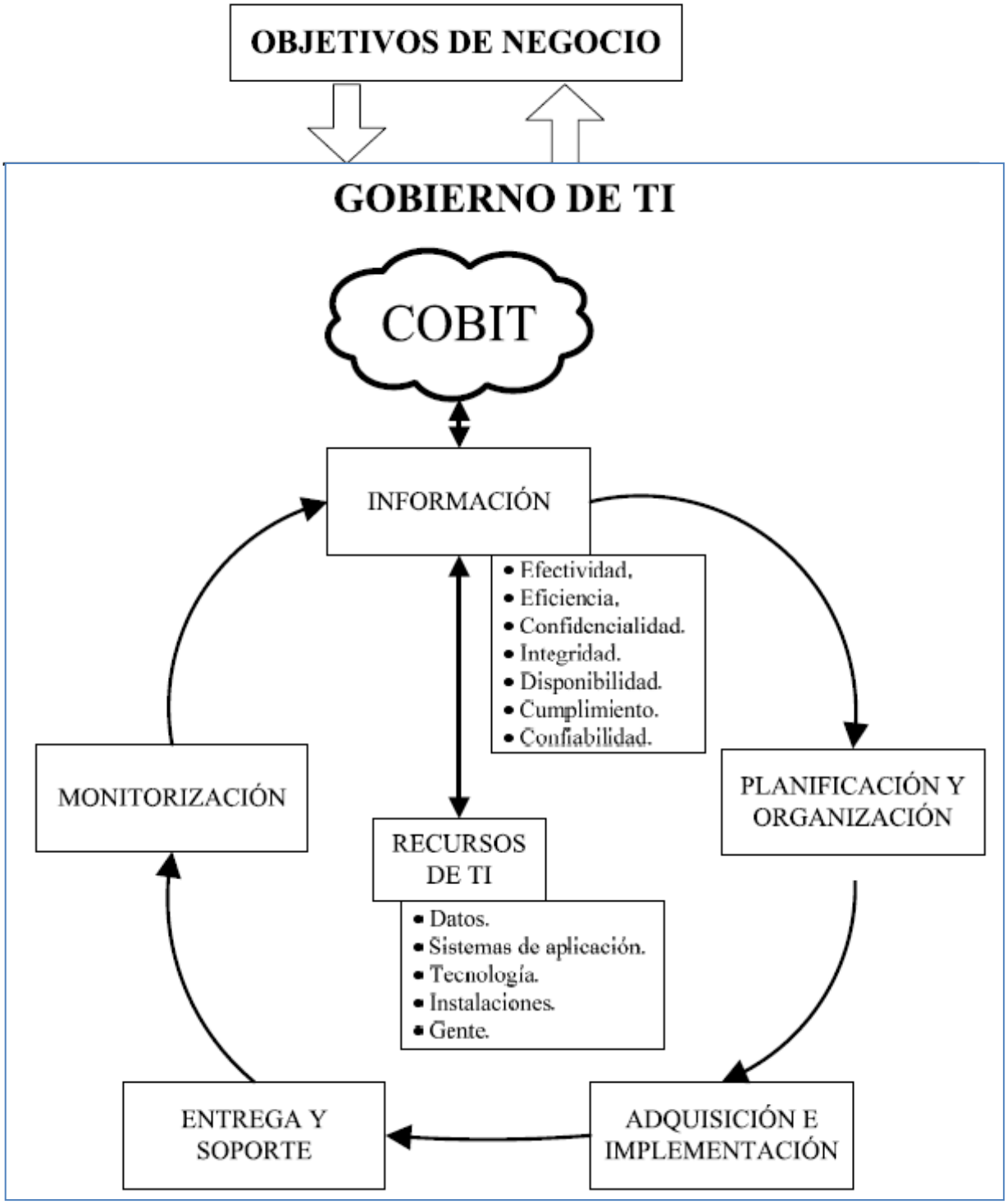


Ilustración 4 Flujo de los Dominios de COBIT (COBIT v4.0, 2006)

ITIL (Biblioteca de Infraestructura de Tecnologías de Información), es un marco de trabajo integral, consistente y coherente de buenas prácticas destinadas a facilitar la entrega de servicios de TI y los proceso relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI. ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. (*Alineando COBIT 4.1, ITIL V3, e ISO/IEC 27002 en beneficio del negocio.*2008)

El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima.

Desarrollada a finales de 1980, no fue adoptada por las organizaciones hasta mediados de los 90 y se ha convertido en uno de los estándares mundiales de facto más utilizados en la gestión de servicios informáticos. (Sánchez, 2009)

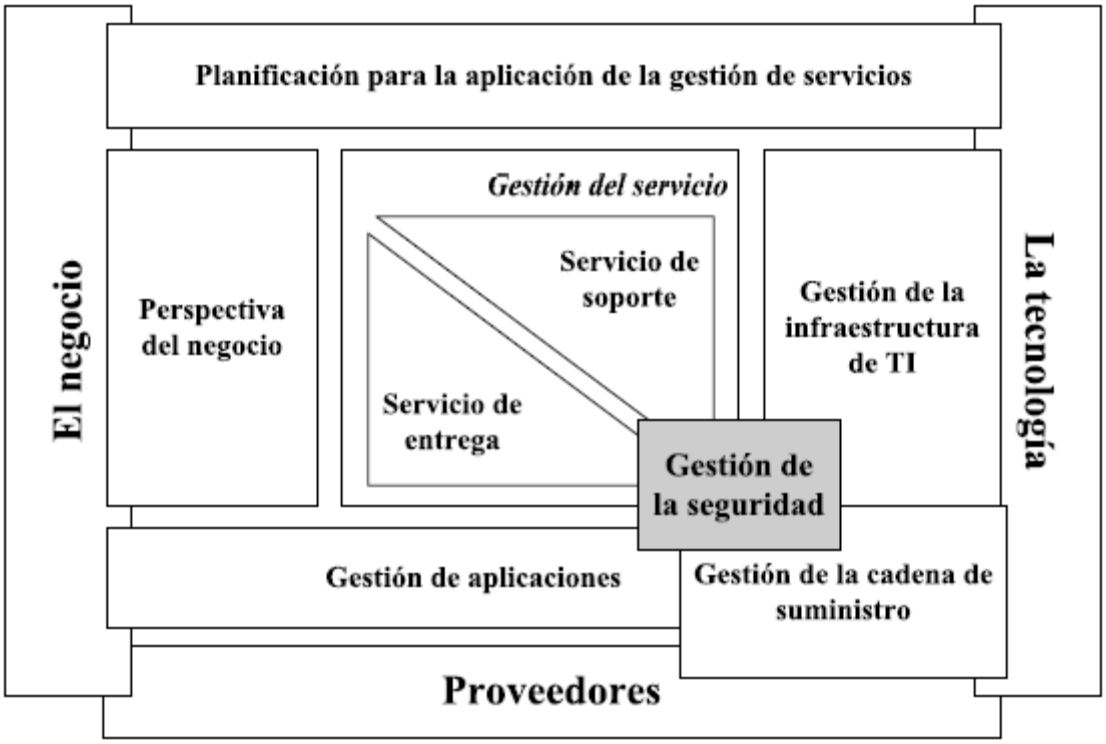


Ilustración 5 Marco de trabajo de ITIL

CMMI Es un enfoque para la mejora de procesos, que proporciona a una organización, los elementos esenciales para llevar a cabo sus procesos de manera efectiva. CMMI no es un proceso de desarrollo de software, sino más bien una guía que describe las características que hacen efectivo a un proceso. CMMI, se emplea para comparar (y mejorar) el proceso de desarrollo de software de una organización describiendo una progresión continua en cinco niveles.

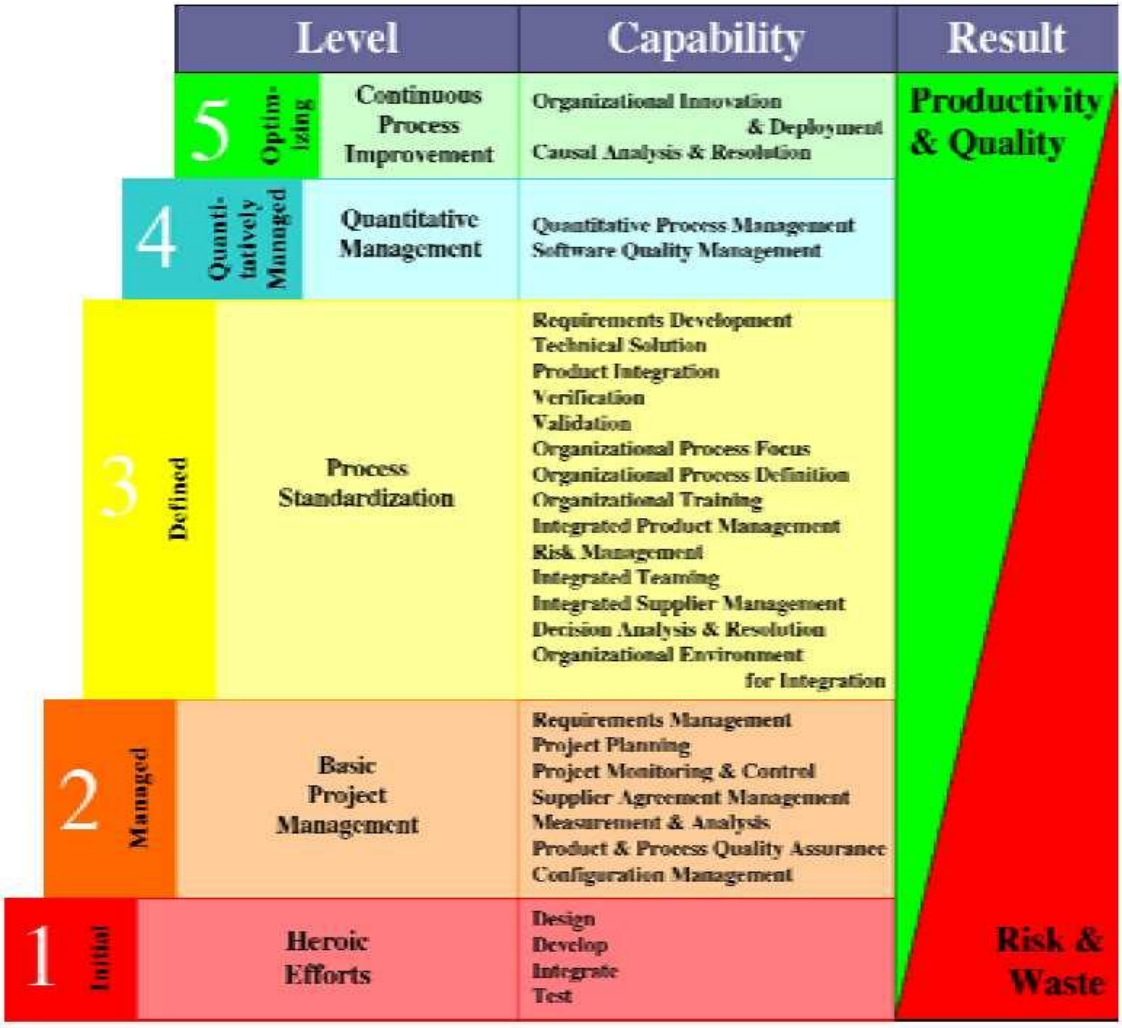


Ilustración 6 Niveles de CMMi

Existe un conjunto importante de metodologías y herramientas cuyo objetivo es gestionar la Seguridad de la información, en particular, orientadas al Análisis y Gestión de Riesgos.

- ISM3 (ISM3, 2007).

Es un modelo de gestión de la seguridad y madurez orientado a implementar un SGSI y definir diferentes niveles de seguridad, donde cada uno de ellos puede ser el objetivo final de una organización.

Algunas de sus principales características son:

• **Métricas de Seguridad de la Información:** ISM3 contiene un pequeño conjunto de métricas de gestión de procesos.

• **Niveles de Madurez:** ISM3 se adapta tanto a organizaciones maduras como a emergentes mediante sus cinco niveles de madurez, los cuales se adaptan a los objetivos de seguridad de la organización y a los recursos que están disponibles.

• **Basado el Procesos**: ISM3 está basado en procesos, lo que lo hace especialmente atractivo para organizaciones que tienen experiencia con ISO 9001 o que utilizan ITIL como modelo de gestión de TIC.

• **Adopción de las Mejores Prácticas**: Una implementación de ISM3 tiene ventajas como las referencias a estándares bien conocidos en cada proceso, así como la distribución explícita de responsabilidades entre los líderes, gestores y el personal técnico usando el concepto de gestión estratégica, táctica y operativa.

• **Certificación**: Los sistemas de gestión basados en ISM3 pueden certificarse bajo ISO 9001 o ISO/IEC 27001, lo que implica que se puede usar ISM3 para implementar un SGSI basado en ISO/IEC 27001.

ISM3 considera que hay tres niveles de gestión de seguridad:

• **Estratégico**, que trata de los objetivos globales y la provisión de recursos y está formado por los siguientes procesos: i) SSP-1 Informar a los accionistas; ii) SSP-2 Coordinar; iii) SSP-3 Alcanzar visión estratégica; iv) SSP-4 Definir las reglas para la separación de responsabilidades: transparencia, particionado, supervisión, rotación y separación de responsabilidades (TPSRSR); v) SSP-5 Comprobar el cumplimiento con las reglas TPSRSR; y vi) SSP-6 Asignar recursos para seguridad de la información.

• **Táctico**, que trata de los objetivos específicos y la gestión de recursos y está formado por los siguientes procesos: i) TSP-1 Informar a la gestión estratégica; ii) TSP-2 Gestionar los recursos asignados; iii) TSP-3 Definir las metas de seguridad; iv) TSP-4 Definir los indicadores para los procesos de seguridad; v)TSP-5 Definir grupos de propiedades; vi) TSP-6 Definir ambientes y ciclos de vida; vii) TSP-7 Investigar antecedentes y referencias; viii) TSP-8 Seleccionar el personal de seguridad; ix) TSP-9 Capacitar al personal de seguridad; x) TSP-10 Definir procesos disciplinarios; xi) TSP-11 Alcanzar conciencia en seguridad; y xii) TSP-12 Seleccionar procesos específicos.

• **Operativo**, que trata del logro de los objetivos definidos y está formado por los siguientes procesos: i) OSP-1 Informar a la gestión táctica; ii) OSP-2 Seleccionar las herramientas para implementar las medidas de seguridad; iii)OSP-3 Gestionar el inventario; iv) OSP-4

Controlar el cambio del ambiente de los sistemas de información; v) OSP-5 Re-fraccionar el ambiente; vi) OSP-6 Limpiar el ambiente; vii) OSP-7 Fortalecer el ambiente; vii) OSP-8 Controlar el ciclo de vida del desarrollo de software; ix) OSP-9 Controlar los cambios en las medidas de seguridad; x) OSP-10 Gestionar el respaldo y redundancia; xi) OSP-11 Controlar el acceso a servicios, canales, repositorios e interfaces; xii) OSP-12 Llevar el registro de usuarios; xiii) OSP-13 Gestionar el cifrado; xiv) OSP-14 Gestionar la protección del ambiente físico; xv) OSP-15 Gestionar la continuidad de operaciones; xvi) OSP-16 Gestionar el filtrado y segmentación; xvii) OSP-17 Gestionar la protección contra Malware; xviii) OSP-18 Gestionar el aseguramiento; xix) OSP-19 Emular ataques, errores y accidentes; xx) OSP-20 Emular incidentes; xxi) OSP-21 Comprobar la calidad de la información; xxii) OSP-22 Monitorizar alertas; xxiii) OSP-23 Detectar y analizar los eventos; xxiv) OSP-24 Manejar los incidentes y pseudo-incidentes; y xxv) OSP-25 Realizar el análisis forense.

En una organización pequeña o mediana es posible que los tres niveles puedan estar fusionados en dos, con una gestión sénior con responsabilidades tanto estratégicas como tácticas. La gestión junior puede tener tanto un rol táctico como uno operativo. En la aplicación de ISM3 no es importante el grado de gestión, sino la forma de pensar acerca de cada proceso.

ISM3 define un conjunto de niveles de madurez de seguridad:

• **Nivel ISM3 0:** Si bien este nivel puede producir ganancias a corto plazo, es improbable que produzca una reducción significativa del riesgo de las amenazas a medio o largo plazo sin inversiones impredecibles.

• **Nivel ISM3 1**: Este nivel debería resultar en una reducción significativa del riesgo de amenazas técnicas con una inversión mínima en procesos ISM esenciales. Se recomienda este nivel para organizaciones con metas de seguridad bajas en ambientes de riesgo bajo.

• **Nivel ISM3 2**: Este nivel debería resultar en una mayor reducción del riesgo por amenazas técnicas con una inversión moderada en procesos ISM. Se recomienda este nivel para organizaciones con metas de seguridad normales en ambientes de riesgo normal.

• **Nivel ISM3 3:** Este nivel debería resultar en una reducción alta del riesgo por amenazas técnicas, con una inversión en procesos ISM. Se recomienda este nivel para organizaciones con metas de seguridad altas en ambientes de riesgo normal o alto.

• **Nivel ISM3 4**: Este nivel debería resultar en la mayor reducción de amenazas, tanto técnicas como internas, con una inversión en procesos ISM. Se recomienda este nivel para organizaciones afectadas por requerimientos específicos (como suministradoras de energía y agua, instituciones financieras y organizaciones que comparten o almacenan información sensible) con metas de seguridad muy altas en ambientes de riesgo normal o alto.

Los niveles de madurez van asociados a los procesos de los niveles de seguridad de tal forma que, dependiendo del nivel de madurez, la empresa estará obligada a cumplir con una serie de procesos. Un nivel 0 implicará no cumplir con ningún proceso. En la Ilustración 6. se puede ver cómo se asocian los procesos y los niveles de madurez de ISM3, marcando las X los procesos que deben cumplirse en cada nivel de madurez.

Proceso	ISM3 0	ISM3 1	ISM3 2	ISM3 3	ISM3 4
GP–1		X	X	X	X
SSP–1,2,3,6		X	X	X	X
SSP–4,5					X
TSP–1,2,3,12		X	X	X	X
TSP–5,6,10,11			X	X	X
TSP–4,9				X	X
TSP–7,8					X
OSP–1,5,10,16,17		X	X	X	X
OSP–2,4,6,7,9,11,12,14,19,22			X	X	X
OSP–3,8,13,15,20,24				X	X
OSP–18,21,23,25					X

Ilustración 7 Asociación de los procesos ISM3 a sus niveles de madurez.

La implantación de un SGSI utilizando ISM3 estará formada por las siguientes tareas: i) determinar los requerimientos regulatorios; ii) determinar los objetivos de seguridad de la información; iii) determinar el presupuesto de seguridad de la información; iv) determinar los ambientes y ciclos de vida; v) determinar las metas de seguridad de la información; vi) elegir un método de selección de procesos (nivel de madurez ISM3, evaluación de riesgo, evaluación de vulnerabilidades, evaluación de impacto en los negocios, evaluación de amenazas, evaluación ROSI); vii) seleccionar los procesos apropiados; viii) revisar las metas de seguridad de la información; ix)determinar los indicadores de seguridad de la información; x) diseñar y documentar el SGSI basado en ISM3 (acuerdos, políticas, procedimientos, plantillas); xi) implementar el SGSI; xii) operar el SGSI; xiii) auditar o certificar el SGSI periódicamente; xiv) mantener y mejorar el SGSI.

Sin embargo esta implementación para las PYMES es difícil, ya que se abarca a nivel muy general para que sea útil para todos los tipos de compañías, generando posiblemente altos costos de implementación.

2.8. Metodologías de Evaluación de Riesgos:

2.8.1. MAGERIT (CNI, 2012)

"Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" desarrollado por el Ministerio de las Administraciones Públicas de España.

La metodología MAGERIT fue elaborada por Consejo Superior de Administración Electrónica, para el análisis y gestión de riesgos. MAGERIT permite realizar una aproximación metódica para conocer el riesgo al que están sometidos los elementos de trabajo. MAGERIT es una metodología de carácter público, perteneciente al Ministerio de Hacienda y Administraciones Públicas; su utilización no requiere autorización previa del mismo.

MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

A la hora de llevar a cabo un proyecto de análisis y gestión de riesgos de acuerdo con MAGERIT se debe proceder con las siguientes 3 fases:

Planificación del proyecto
Análisis de riesgos
Gestión de riesgos

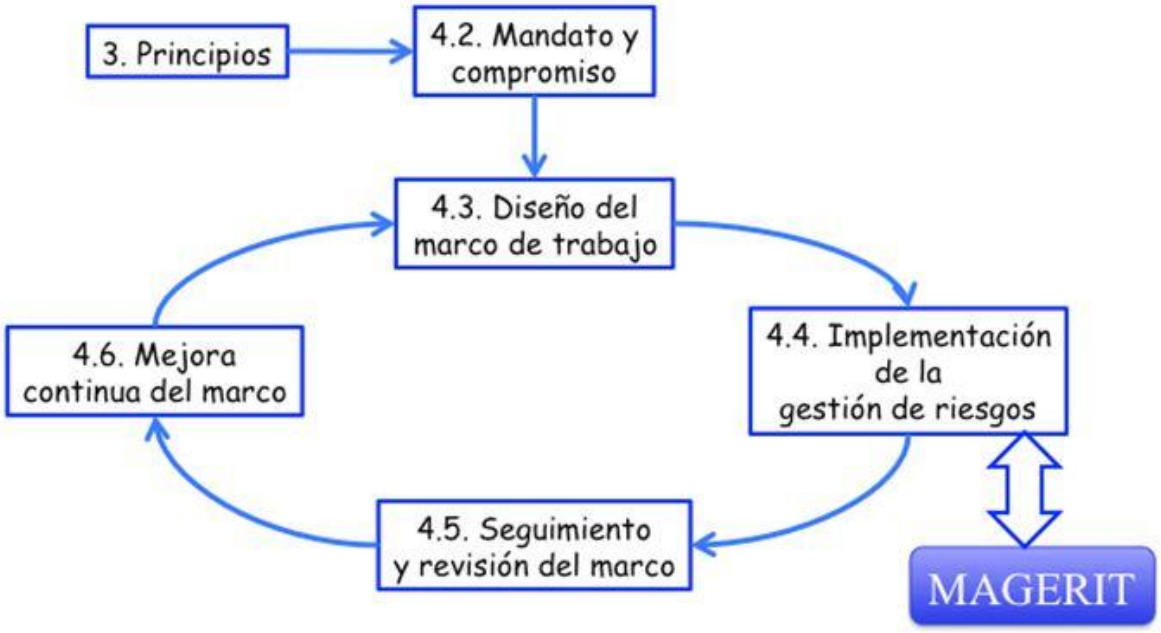


Ilustración 8. ISO 31000 - Marco de trabajo para la gestión de riesgos

MAGERIT versión 3 se ha estructurado en tres libros:

Libro I: Método

Libro II: Catálogo de Elementos

Libro III: Guía de Técnicas

Libro I : Método

Se estructura de la siguiente forma:

- El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.
- El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.
- El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

- El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.
- El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

Libro II: Catálogo de Elementos

Marca unas pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

Libro III: Guía de Técnicas

Aporta luz adicional y orientación sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

2.8.2 Otras Metodologías

- EAR / PILAR esta herramienta da soporte al análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT. Está diseñada para apoyar el proceso de gestión de riesgo a lo largo de períodos prolongados. Dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son: ISO /IEC 27002:2005, SP800-53:2006, Criterios de Seguridad, Normalización y Conservación del Consejo Superior de Informática y para el impulso de la administración electrónica.

- CRAMM: "CCTA Risk Assessment and Management Methodology" Desarrollado por Insight Consulting. Proporciona una manera fácil de implementarla, dispone de una herramienta que apoya la metodología. Soporta completamente las tres etapas del método Cramm por medio de una aproximación ordenada y etapa a etapa. La herramienta está disponible en tres versiones: CRAMM experto, CRAMM exprés y BS 7799 revisión.

- MEHARI: "Methode Harmonisée d'Analyse de Risque" es una metodología de análisis y gestión de riesgos desarrollada por CLUSIF ("Club de la Sécurité de l'Information Français").

- **NIST(6) SP 800-30**: es una Guía de Gestión de Riesgos para los Sistemas y Tecnologías de la Información.

- NIST SP 800-39 "Managing Risk from Information Systems - An Organizational Perspective" (7).

-OCTAVE: "Operationally Critical Threat, Asset, and Vulnerability Evaluation"

Es un conjunto de métodos, herramientas y técnicas del CERT para la planificación estratégica y evaluación de la seguridad de la información. Los tres argumentos básicos del método son: los principios, los atributos y los resultados, lo que permite que cualquier metodología que aplique estos principios, se considere compatible con el método OCTAVE.
El Software Engineering Institute, ha publicado tres metodologías basadas en OCTAVE, que son:

- OCTAVE que es la metodología original destinada a grandes organizaciones.
- OCTAVE-S Basada en la anterior pero destinada a pequeñas organizaciones.
- OCTAVE ALLEGRO para realizar un análisis de riesgos basado en los activos de información.

- **IT GRUNDSCHUTZ:** “ IT Baseline”, desarrollado por la Oficina Federal de Seguridad de la Información de Alemania.

- ISM3-RA: Es el método de valoración riesgos propuesto por el modelo de madurez la seguridad de la información ISM3.

2.9. Investigaciones previas

En el proceso de investigación, se han encontrado muchas referencias de intentos por resolver el problema de la implementación de Sistemas de Información de Seguridad de la información, entre ellas, una tesis doctoral de Luis Enrique Sánchez de la Universidad de Castilla - La Mancha, el cuál desarrolla una Metodología para la Gestión de la Seguridad y su Madurez en las PYMES a la que llamó MGSM-PYME.

2.9.1 Metodología MGSM-PYME

La metodología MGSM-PYME se acerca mucho a la que se pretende proponer en este trabajo, sin embargo al final, genera un desarrollo que implica la adquisición de un software por parte de la empresa, que es una de las principales cosas que las PYMES no hacen.
La metodología MGSM-PYME desarrolla un conjunto de matrices, que permiten relacionar los diferentes componentes del SGSI (controles, activos, amenazas, vulnerabilidades, criterios de riesgo, procedimientos, registros, plantillas, instrucciones técnicas, reglamentes y métricas) con el modelo que lo utilizará, para generar automáticamente gran parte de la información necesaria, reduciendo de forma muy notable los tiempos necesarios para el desarrollo e implantación del SGSI.

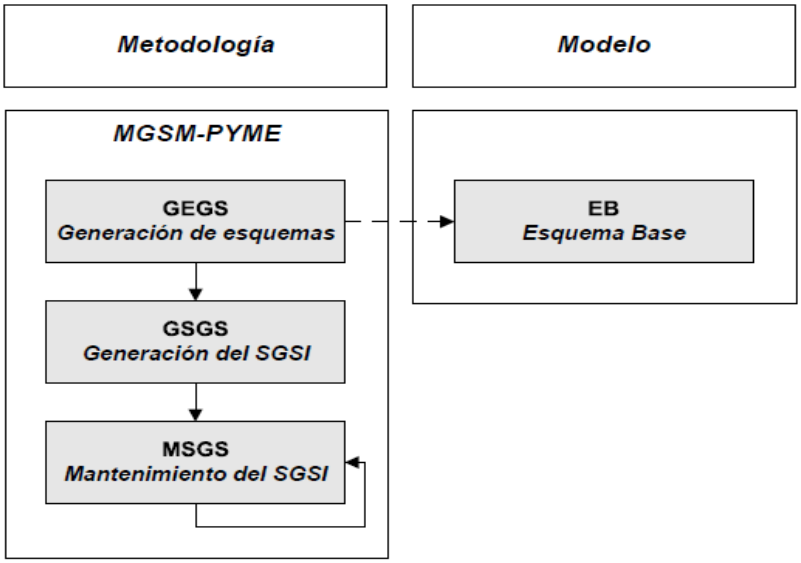


Ilustración 9 Esquema inicial de la metodología MGSM-PYME y su modelo.

Está metodología consta de tres subprocesos principales:

• **GEGS** – **Generación de Esquemas de Gestión de Seguridad**: El principal objetivo de este subproceso está orientado a la construcción de "esquemas", que son estructuras necesarias para la construcción de SGSIs, creadas para un conjunto de posibles compañías de la misma categoría. Estos esquemas son reutilizables y permiten reducir el tiempo de creación del SGSI, así como sus costes de mantenimiento hasta hacerlos adecuados para la dimensión de una PYME. El uso de esquemas es de especial interés y relevancia en el caso de las PYMES ya que por sus especiales características, éstas suelen tener sistemas de información sencillos y muy parecidos entre sí.

• **GSGS – Generación de Sistemas de Gestión de Seguridad**: El objetivo principal de este subproceso es la creación de un SGSI adecuado para una compañía, utilizando para ello un esquema existente.

• **MSGS – Mantenimiento del Sistema de Gestión de Seguridad**: El objetivo principal de este subproceso es el mantener y gestionar la seguridad del sistema de información de la compañía, aportando información actualizada en el tiempo de un SGSI generado.

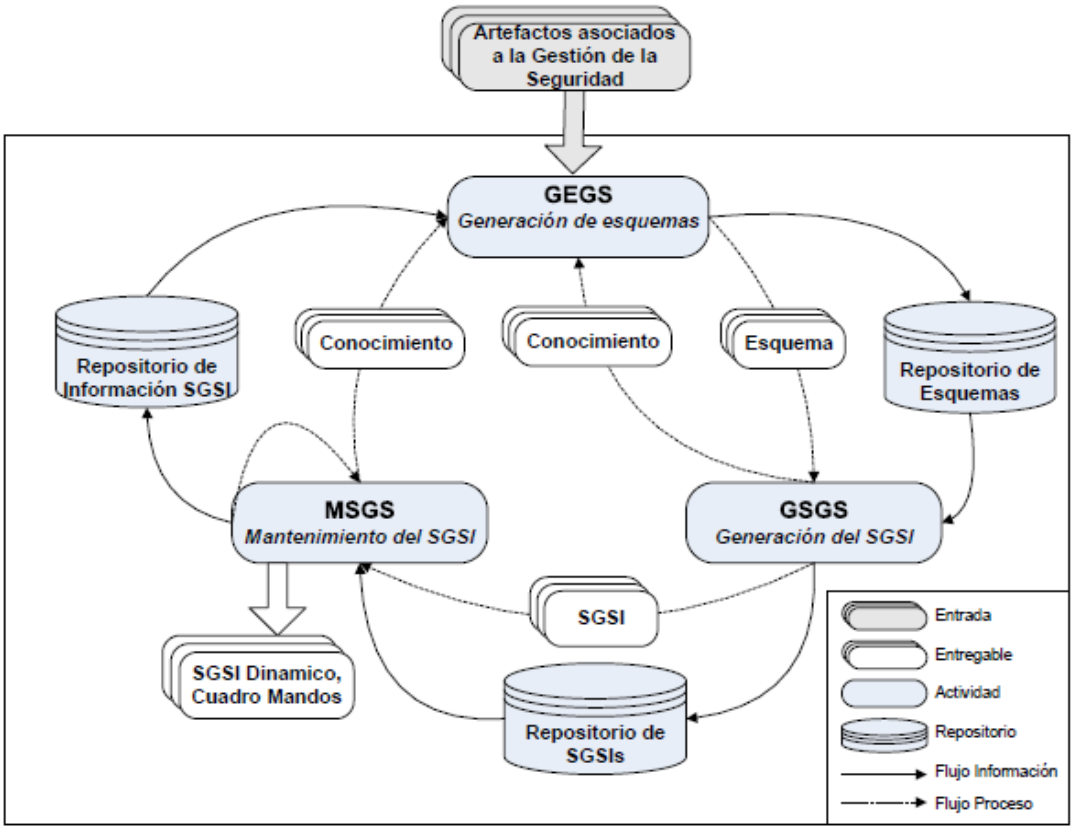


Ilustración 10 Subproceso y productos del proceso de desarrollo MGSM-PYME

MGSM-TOOL es una aplicación web, con un entorno compuesto por ASP.NET para la capa de presentación, C# para la capa de aplicación y SQL Server 2005 para la capa de almacenamiento.

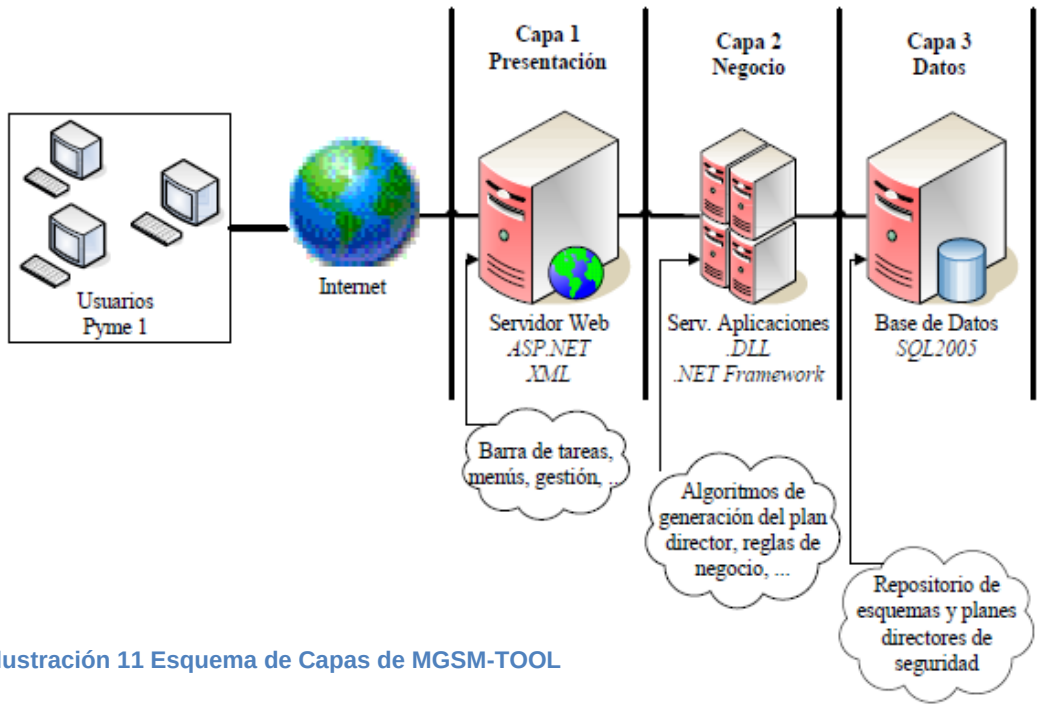


Ilustración 11 Esquema de Capas de MGSM-TOOL

La implementación de esta herramienta, tiene un costo inicial bajo según refieren y una cuota mensual baja, no se establece el término bajo dentro de la tesis que describe la metodología, pero declara que son montos accesibles por las PYMES.

2.9.2 Otras Metodologías enfocadas en Pymes para implementación ISO 27001

En la misma tesis de Luis Fernando (Sánchez, 2009), se ha realizado una síntesis de otras metodologías que se han buscado resolver el problema de la implementación de los SGSI en las PYMES se va a comentar rápidamente a manera de resumen, los aspectos relevantes tomados de la misma tesis, ya que Luis Fernando realiza fuertes críticas a cada una, justificando la creación de su metodología, como solución a las falencias que presentan las demás metodologías. Por lo tanto, ilustrar los aspectos relevantes de cada una, permitirá sacar conclusiones de si estas críticas son verdades absolutas, o por el contrario permiten una relación complementaria de unas con otras.

Eloff (Ellof & Ellof, 2003)

Aporta una mejora a la norma ISO/IEC 17799, utiliza el ciclo PDCA, definiendo cuatro clases distintas de protección que permiten ir incrementando de forma progresiva los niveles de seguridad, basado en las secciones de la norma ISO/IEC 17799.
Clase 1: Protección inadecuada. No cubre ninguna sección de la norma ISO/IEC 17799
Clase 2: Protección mínima. Cubre aspectos legales y de continuidad del negocio.
Clase 3: Protección razonable. Le suma a la clase 2 aspectos organizativos, control de activos y gestión de accesos.
Clase 4: Protección adecuada. Cubre todas las secciones de la ISO/IEC 17799.

Dojkovski (S. Dojkovski, S. Lichtenstein, & M. J. Warren, 2006)

Este es un modelo basado en construcción de un SGSI orientado a las PYMES teniendo como punto central la cultura de la seguridad y para desarrollarlo propone un marco de trabajo formado por los siguientes elementos:

Aprendizaje organizativo e individual: Difundir la cultura de seguridad de la información a todos los niveles de la organización (A. Martins & J. H. P. Eloff, 2003). Según (Van Niekerk & Von Solms, 2003) podría ser útil utilizar un enfoque de aprendizaje organizativo.

***E–Learning*:** (cooperación, colaboración e intercambio de conocimientos): las PYMES pueden realizar aprendizaje electrónico (e–learning) (Furnell, Warren A, & Donwland P.S., 2004) y también pueden cooperar y colaborar electrónicamente en las comunidades y foros de seguridad de los sistemas de la información (Helokunnas T. & Kuusisto R., 2003b) con el objetivo de mejorar la cultura de la seguridad entre los usuarios del sistema de información.

Gestión: Los programas de sensibilización (respaldo de la dirección, amenazas de medidas disciplinarias, cláusulas en los contratos de trabajo, etc.), la formación, la educación ó el valor del liderazgo (Dutta y McCrohan, 2002) contribuyen a la construcción de la cultura de la seguridad de la información (Lichtenstein y Swatman, 2001b, Furnell y Clarke, 2005).

Cultura de la seguridad: Procedimientos para responder a nuevos sucesos (como violaciones de seguridad) ayudarán a subrayar la importancia de la seguridad de la información a los trabajadores(OECD, 2002). Los incentivos también pueden ser útiles para modificar el comportamiento de los empleados. Sin embargo, (Rosanas & Velilla, 2005) advierten que los controles de la gestión debe estar basados en valores éticos.

Comportamiento: Gestión de iniciativas destinadas a desarrollar los rasgos deseables de comportamiento respecto a la responsabilidad, integridad, confianza y ética del personal (Dhillon, G., & Backhouse, 2001c). Sin embargo, valores fuertes son necesarios para apoyar las iniciativas de gestión (Rosanas & Velilla, 2005). Cuando los valores fuertes son difundidos entre entidades colaboradoras, empleados y otras partes interesadas, la seguridad de la información se fortalece (Helokunnas T. & Kuusisto R., 2003b). El desarrollo de la motivación intrínseca es importante (Siponen, 2000) y puede ser apoyada por la promoción al personal que cumpla las normativas de seguridad de forma adecuada (Detert, Schroeder, & Mauriel, 2000).

• ***Ética nacional y cultura organizacional***: Según (Helokunnas T. & Kuusisto R., 2003b), la creación de foros de seguridad dentro del ámbito nacional puede favorecer la creación de una cultura de la seguridad de la información.

Según las investigaciones realizadas por (S. Dojkovski et al., 2006) los principales retos en el desarrollo de la cultura de seguridad de la información en las PYMES incluyen:

• Motivar a los propietarios para que asignen un presupuesto adecuado a la seguridad de la información.
• Convencer a los propietarios de realizar un análisis formal de los riesgos.

• Velar para que los propietarios desarrollen una política de seguridad de la información, desarrollen procedimientos y asignen responsabilidades.
• Desarrollar una postura proactiva hacia la seguridad de la información.
• Identificar y establecer una serie de actividades de sensibilización para adaptarse a los entornos de las PYMES.

IS2ME (Linares & Paredes, 2007)

Es un método de implementación de la seguridad de la información en las medianas empresas, que conjuga, por una parte, las necesidades de cumplimiento y desarrollo de un sistema de gestión de la seguridad de la información, según estándares internacionales y por otra, la obtención de resultados a corto plazo para disminuir el riesgo alto inicial que estas organizaciones están asumiendo, proporcionando resultados rápidos a la alta dirección.

IS2ME hace una evaluación inicial mediante entrevistas, realiza pruebas de campo y análisis técnicos y realiza la presentación de un informe del estado de implantación de las distintas medidas de seguridad técnicas y organizativas, para pasar a la elaboración y propuesta de un plan de acción que tras ser aprobado por la alta dirección, se procederá a desarrollar e implementar, sentando la base y comenzando el camino hacia el cumplimiento e implantación de la seguridad de la información, según ISO/IEC 27001.

Actividades de la metodología IS2ME:

- Identificación de interlocutores.
- Recolección general de la información.
- Recolección técnica de información.
- Análisis de información.
- Desarrollo de informe SEIS (Estado de la seguridad de la información de compañía.
- Presentación del informe SEIS a la alta dirección.
- Desarrollo del documento IASSAP (Plan de Acción de Seguridad y Protección de la Información).
- Presentación del documento IASSAP a la alta dirección.
- Implantación de IASAP.

ASD - Agile Security Development (Wiander & Holappa J., 2007)

Desarrolla un método simplificado de análisis de riesgos, incluyendo el desarrollo de un prototipo y un caso de estudio. Han dividido los dominios de la ISO/IEC17799, por niveles de madurez que utilizan para el modelo ASD.

Expectativas del estándar de gestión de seguridad de la información		
Objetivos prioritarios	1	Aplicar mejores prácticas.
	2	Evaluar el estado de los controles.
	3	Establecer objetivos para la seguridad de la información.
	4	Reducir la frecuencia y el impacto de incidentes importantes.
Objetivos importantes	5	Cumplir con la política interior.
	6	Añadir un programa de gestión de riesgos.
	7	Cumplir los requerimientos legales de la industria.
	8	Maximizar las inversiones existentes.
Otros objetivos	9	Obtener ventajas competitivas.
	10	Cumplir los requerimientos del gobierno de las IT.
	11	Responder a los requerimientos de terceras partes.
	12	Lograr ahorros de costes.

Ilustración 12 División en niveles de madurez de la ISO/IEC 17799 por ISF

La implantación de un SGSI siguiendo el modelo ASD, se basa en ir desarrollando, dominio a dominio de la norma ISO/IEC 17799 hasta alcanzar niveles de madurez adecuados.

Carey - Smith (Carey-Smith, Nelson, & May, 2007)

Aplica una serie de iteraciones de ciclos AR en espiral para desarrollar un SGSI, en la que cada final de fase sirve para obtener un aprendizaje que sirve de diagnóstico para la siguiente fase. Es un modelo híbrido, basado en la norma AS/NZS ISO/IEC 17799 de Australia, orientado a seleccionar sólo aquellos conocimientos de seguridad que son requeridos por las empresas sin ánimo de lucro.

Tiene dos aspectos fundamentales:

- Las múltiples iteraciones de AR en cada ciclo, se traducirá en un mayor rigor y transferencia de conocimientos a otras organizaciones.
- El diseño de la metodología es participativa, garantizando el compromiso de los participantes y su formación.

Tawileh (Tawileh, Hilton, & McIntosh, 2007)

Sistema basado en una metodología para sistemas simples (SSM), con un enfoque sencillo para la gestión de la seguridad en PYME basado en las cuatro fases del ciclo PDCA (Ilustración 11) . Se basa en la existencia de un ciclo de retroalimentación negativa: entre menos es la conciencia del problema de seguridad, más abajo de la lista de prioridades para inversión se ubica, por lo que se reducen los recursos que le han sido asignados y deriva en menor conciencia.

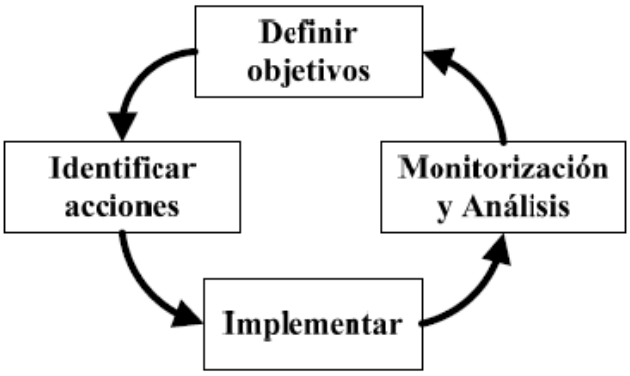


Ilustración 13 Etapas de gestión de la seguridad (Tawileh, et al., 2007)

La captura de los objetivos de la seguridad de la información en el sistema de gestión de una PYME, según la propuesta de Tawileh, constará de cuatro fases:

Fase I: Definición de los elementos raíz, a partir de las respuestas de las preguntas de la ilustración 12.

SSM sugiere una meta - concepto llamado RD "Definición Raíz", cuyo objetivo es proporcionar una clara e inequívoca definición textual del sistema. Este metaconcepto, cuenta con 6 componentes que se enumeran en la siguiente tabla, mapeados para que coincidan con los propósitos de gestión de la seguridad en la PYME y para facilitar el proceso de desarrollo.

Elemento	Descripción original	Seguridad de la PYME
C	Clientes del sistema	¿En qué organizaciones va a ser implementado el SGSI?
A	Actores del sistema	¿Quién va a implementar y mantener el SGSI?
T	Proceso de transformación que el sistema debería realizar	¿Cuál es el principal objetivo que debe lograrse con el SGSI?
W	Visión en que el sistema estará basado	¿Cómo logrará la compañía los objetivos de seguridad?
O	Propietario del sistema	¿Quién es el propietario de la organización?
E	Limitaciones del entorno	¿Cuáles son las limitaciones que afectan al SGSI dentro de la organización?

Ilustración 14 Elementos de la definición raiz (Tawileh, et al., 2007)

Fase II: Determinar las medidas que deberían adoptarse, para lograr los objetivos definidos en la fase I.

Fase III: Determinar las acciones que deben realizarse para la gestión. Incluye programas de capacitación en seguridad.

Fase IV: Se refiere a la naturaleza cambiante del entorno empresarial. Es decir, adaptar el SGSI para responder a los cambios en los requerimientos del negocio.

Sneza (Sneza, Shrman, & Matthew, 2007)

La construcción del SGSI se basa en la cultura de la seguridad de la información y el comportamiento y pensamiento de las personas.
Se consideran en este marco, tres influencias externas:

- Ética nacional y cultura organizacional.
- Las iniciativas del gobierno.
- Proveedores.

Los elementos que conforman este marco de trabajo son:

- Liderazgo y gobierno corporativo.
- Cultura organizativa.
- Gestión.
- Aprendizaje individual y organizativo.
- Concienciación de seguridad de la organización.
- Revisión y evaluación.
- Comportamiento.

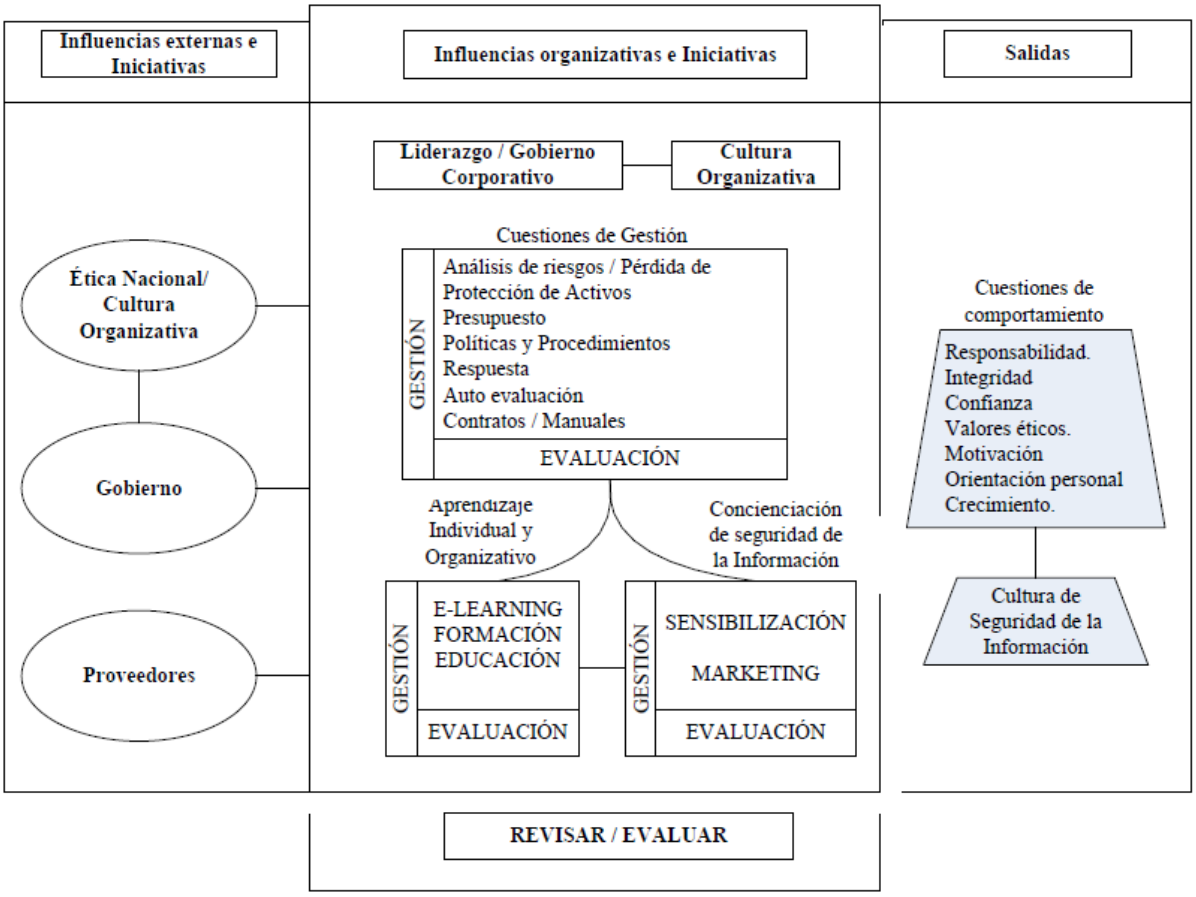


Ilustración 15 Marco para fomentar la Cultura de la Seguridad en las PYMES (Sneza, et al.,2007)

Conclusión: Como se plantea al inicio de este apartado, luego de analizar las diferentes metodologías aquí expuestas, y criticadas individualmente en la tesis de Luis Fernando (Sánchez, 2009), se concluye que tanto la metodología desarrollada por Luis Fernando en su tesis MGSM, como la de Eloff, la de Dojkouski, la de Linares y Paredes, la de Wiander y Holappa, la de Carey - Smith, la de Tawiteh y la de Sneza, tienen componentes que enriquecen este trabajo y que se relacionan en la siguiente tabla.

Tabla 2 Consideraciones importantes de metodologías orientadas a las PYMES

Metodología	Planteado por	Concepto Relevante
MGSM - PYME	Luis Fernando Sánchez - 2009	- Elaboración de Plantillas para la generación de documentos de forma automática.
Propuesta de Eloff	Eloff - 2003	Plantea 4 niveles de seguridad basado en el cumplimiento de la ISO

		27001, donde 1 no cumple con nada y 4 cumple completamente.
Propuesta de Dojkouski	Dojkouski 2006	Cultura de la Seguridad.
Propuesta ADS	Wiander y Holappa - 2007	División de Dominios de la ISO 17799 por niveles de madurez.
SGSI en Empresas sin ánimo de lucro	Carey - Smith - 2007	Múltiples ciclos de AR cuyo final de uno es el insumo de entrada para el siguiente.
SSM - Metodología de Sistemas Simples.	Tawitech - 2007	Simplicidad de Enfoque PDCA. Importancia de la Seguridad vs Presupuesto asignado.
Propuesta de Sneza	Sneza 2007	Considera tanto la cultura de la seguridad como el comportamiento y el pensamiento humano, dentro de la construcción del SGSI.

Guía de Aplicación de la Norma UNE-ISO/IEC 27001, sobre seguridad en sistemas de información para pymes. (Gómez Fernández & Andrés Álvarez, 2012)

En esta publicación AENOR pretende facilitar a las PYMES, la comprensión de los diversos conceptos involucrados en un sistema de gestión normalizado y ofrece recomendaciones generales para la implementación de un SGSI, tanto para la norma UNE-ISO/IEC 27001, UNE-ISO/IEC 27002, como del ENS (Esquema Nacional de Seguridad).

Empieza por definir conceptos importantes, realiza una explicación de cada uno de los puntos de la norma, sus requisitos de documentación y su implementación. Ejemplifica con un caso práctico, la implementación de los apartados y documentos explicados. Este proceso lo realiza tanto para la ISO/IEC 27001 como para el ENS.

Es una valiosa herramienta, que si bien no está gratuitamente disponible, si se adquiere por un bajo precio. Aún con esta disponibilidad de esta guía, para una persona sin conocimiento sobre sistemas de gestión y seguridad, se le dificulta la implementación de la norma.

Pero es otro insumo valioso para el diseño del objeto de este trabajo, que pretende sumar los esfuerzos de los antecesores, para encontrar una alternativa que facilite el trabajo de las PYMES y que minimice los costos de implementación de las buenas prácticas que conduzcan a contar con un SGSI normalizado, bajo la norma ISO/IEC 27001.

2.10. Marco Normativo

2.10.1 Legislación Española

Directiva 95/46/CE del parlamento europeo y del consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El Artículo 18 de la Constitución Española, donde se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. En él se dice que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

La Sentencia del Tribunal Constitucional STC 292/2000, de 30 de noviembre de 2000, en el que se dice que el derecho fundamental a la protección de datos personales no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo.

La Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD). El Reglamento RD 1720/2007 por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal, vigente a partir del 19/4/2008.

La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).

En España se aplica de forma general la Directiva 2010/45/UE, cuyos principales objetivos son reducir las cargas administrativas de los sujetos pasivos, garantizar la igualdad de trato entre las facturas en papel y las facturas electrónicas, facilitar las transacciones económicas y contribuir a la seguridad jurídica de los agentes económicos; si bien esta normativa está adoptada al ordenamiento nacional, en el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, que sustituye al Reglamento de facturación aprobado por el Real Decreto 1496/2003.

Ley 25/2013 impulso facturación electrónica y creación del registro contable de facturas en el Sector Público aplicable a las facturas emitidas en el marco de las relaciones jurídicas entre proveedores de bienes y servicios y las administraciones públicas.

2.10.2 Legislación Colombiana

Ley Estatutaria 1581 de 2012, por el cual se dictan disposiciones generales para la protección de datos personales. Desarrolla el derecho constitucional que tienen todas la personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política Colombiana. así como el derecho a la información consagrado en el artículo 20 de la misma.

Decreto 1377 de 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012, sobre la protección de datos personales.

Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

3. Objetivos Concretos y Metodología del Trabajo

3.1. Hipótesis

¿Se puede generar una metodología de implementación de seguridad de la información para las PYMES, que esté al alcance de sus recursos económicos y humanos?.

3.2. Objetivos Específicos

- Estudiar y analizar la norma ISO 27001 y sus documentos complementarios.
- Investigar el estado del arte y reunir información suficiente para determinar lo más recomendable en la metodología a desarrollar.
- Identificar buenas prácticas de seguridad de la información que puedan aplicarse a las PYMES.

- Hacer un análisis de dos PYMES que permitan identificar los problemas actuales presentes en las mismas.
- Investigar casos de ataque que hayan sufrido las PYMES y posibles formas de evitarlas.
- Concluir a partir de estos ataques, errores de implementación o falta de controles.
- Generar una metodología de implementación de un sistema de gestión de seguridad de la información, que pueda ser aplicable fácilmente a las PYMES.
- Verificar si las propuestas de este trabajo pueden generalizarse a grandes compañías.

3.3. Metodología del Trabajo

Como en todo proceso de investigación, se ha seguido el método científico para el desarrollo de este trabajo.

3.3.1 Descripción Detallada de los Métodos de Investigación

El método científico está compuesto de varios pasos que deben seguirse en un orden y completa rigurosidad. Estos son:

- **Observación:** investigación o recolección previa de datos relacionados al tema a investigar, los cuales se analizan y organizan, de forma de ofrecer información confiable que lleve al siguiente paso
- **Proposición:** establecer la duda que se quiere resolver o aquello que se desea estudiar

- **Hipótesis:** la posible solución o respuesta que queremos comprobar y que basa en una suposición en base a investigación. Puede ser o no verdadera y, mediante los siguiente pasos, se trata de demostrar su posible validez.

- **Verificación y experimentación:** se trata de probar o desechar la hipótesis mediante la experimentación o aplicación de investigaciones válidas y objetivas.

- **Demostración o refutación de la hipótesis:** se analiza si ésta es correcta o incorrecta, basándose en los datos obtenidos durante la verificación.

- **Conclusiones:** se indican el porqué de los resultados, enunciando las teorías que pueden surgir de ellos y el conocimiento científico que se genero mediante la aplicación correcta del método.

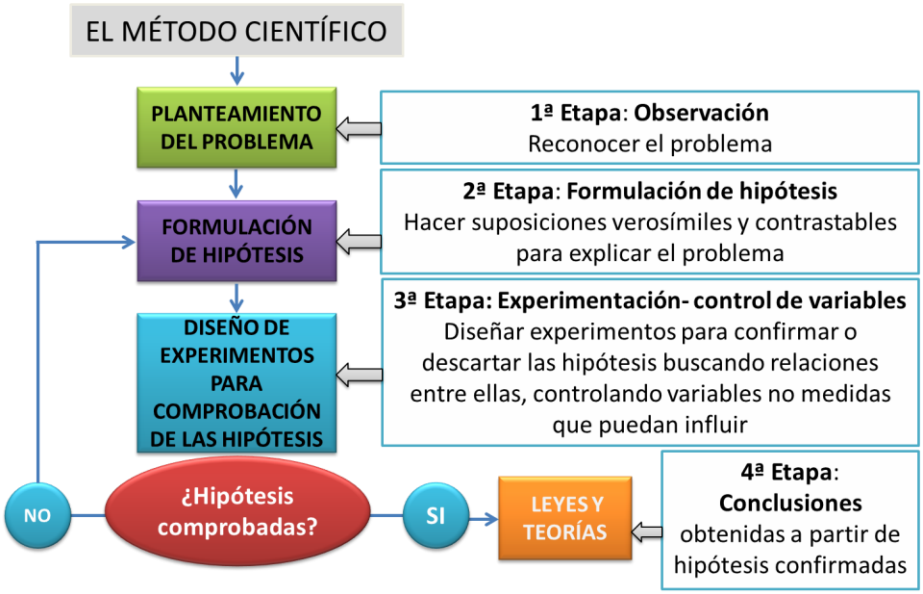


Ilustración 16 El Método Científico

El **método hipotético-deductivo** es el procedimiento o camino que sigue el investigador para hacer de su actividad una práctica científica. El método hipotético-deductivo tiene varios pasos esenciales: observación del fenómeno a estudiar, creación de una hipótesis para explicar dicho fenómeno, deducción de consecuencias o proposiciones más elementales que la propia hipótesis, y verificación o comprobación de la verdad de los enunciados deducidos comparándolos con la experiencia. Este método obliga al científico a combinar la reflexión racional o momento racional (la formación de hipótesis y la deducción) con la observación de la realidad o momento empírico (la observación y la verificación).

Fases del método hipotético-deductivo

1. Planteamiento del problema
2. Creación de hipótesis
3. Deducciones de consecuencias de la hipótesis
4. Contrastación: Refutada o aceptada

Y los pasos seguidos para la investigación fueron los que se muestran en la ilustración 15.

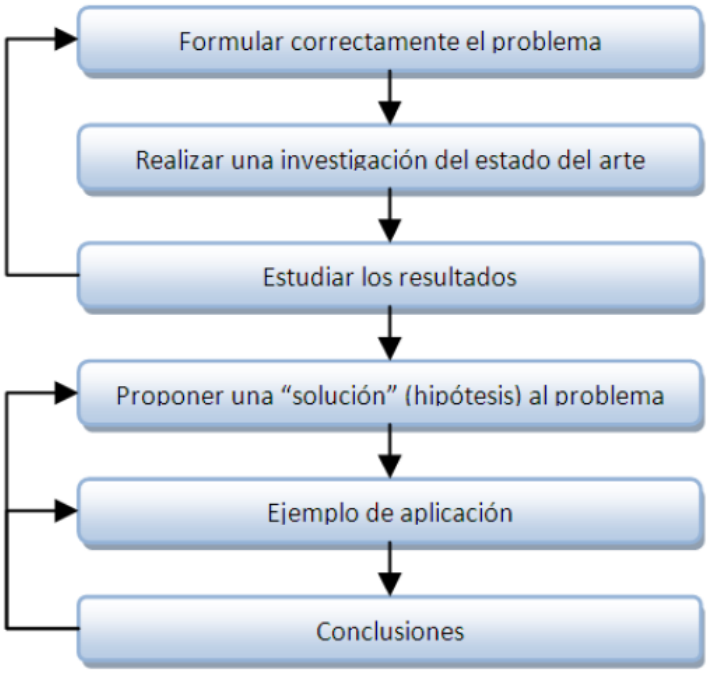


Ilustración 17 Método de investigación

En la primera actividad, se busca formular correctamente el problema y que en este caso es la dificultad que tienen las PYMES a la hora de implementar un SGSI. Luego se realiza una investigación del estado del arte, en esta se encontraron varios estudios que tiene aportes importantes para considerar dentro de la metodología que se plantea como solución al problema. De manera sistémica se ha reunido, evaluado e interpretado toda la información disponible que está relacionada con el objeto a resolver.

Una revisión sistemática consta de varias actividades, como son:

1. **Planificación de la revisión**: se identifica la necesidad de la revisión, las preguntas de investigación son establecidas, y el protocolo de revisión es definido.

2. **Conducción de la revisión**: los estudios primarios son seleccionados, se definen los criterios de aseguramiento de calidad de los estudios primarios incluidos y se extrae y sintetiza la información.

3. **Presentación de resultados**: los resultados de la revisión son interpretados y presentados.

Una vez realizado el estudio del estado del arte y analizados los resultados, se puede pasar a la primera actividad o bien realizar una propuesta en base a los resultados obtenidos. La propuesta es aplicada y en función de los resultados se obtienen unas conclusiones que pueden llevar a replantear la propuesta o repetir la aplicación del método en otras condiciones.

4. Desarrollo Específico de la Contribución

La contribución define una metodología que pueda ser aplicable a las PYMES, para facilitar la implementación de Sistemas de Gestión de Seguridad de la Información, optimizando la inversión de recursos y tiempo de implementación.

Para la elaboración de la metodología se eligieron dos PYMES de tamaños diferentes, a las cuáles se les realizó un diagnóstico inicial a través de entrevistas, para determinar puntos críticos de atención a través de un cuadro comparativo. Posteriormente se entrega una plantilla en Excel que utiliza partes de las indicaciones de las guías de MAGERIT para la evaluación de riesgos, combinada con un método de valoración que resalta el nivel de riesgo usando colores verde, amarillo o rojo (los colores del semáforo), usando una fórmula de formato condicional en Excel (se utiliza el Excel porque es un software altamente difundido, pero puede ser reemplazado por cualquier recurso ofimático de hoja de cálculo), se utilizan estos tres colores, partiendo de que ya están internacionalmente identificados y concienciados de manera natural en el cerebro humano, identificando el verde como no peligro, amarillo cuidado o precaución, rojo atención, peligro o stop (Motorpasion, 2007), este aspecto es importante, dado que este enfoque busca hacer fácil lo que parece difícil y para esto entre más intuitivo y natural sea el proceso, más favorece la metodología. Luego se toma un listado de los controles de la ISO 27001:2005, para determinar los controles mínimos (es decir identificar cuáles son obligatorios o necesarios considerando los procesos del negocio) para implementarlos estableciendo un nivel inicial del SGSI.
En la investigación de conocimientos previos, se toman algunas características destacadas de diferentes metodologías propuestas por otros autores (**Tabla 2)**, para ser inspiradoras de algunas de las actividades propuestas en esta metodología.

Como se explica en la guía de implementación ISO 27001 para PYMES de Aenor (Gómez Fernández & Andrés Álvarez, 2012) se presentan tres niveles de documentación:

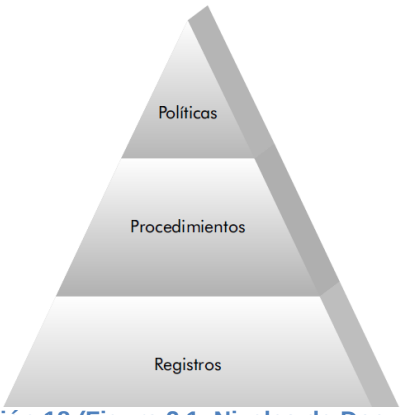


Ilustración 18 (Figura 2.1. Niveles de Documentación (Gómez Fernández & Andrés Álvarez, 2012)

Teniendo en cuenta estos tres niveles y el resultado del análisis de riesgos y selección de controles, se dejan unas plantillas de fácil modificación para ser implementadas por las PYMES, esto facilita la creación de documentos necesarios dentro del sistema de gestión y se entrega la asociación de los mismos a sus registros para el monitoreo y control.

Uno de los aportes importantes de este trabajo, es la entrega de la plantilla de análisis de riesgos que se presenta a continuación.

4.1. Metodología Análisis de Riesgos

4.1.1. Plantilla para el análisis de riesgos

La plantilla desarrollada en un Libro de Excel compuesto de varias hojas de cálculo.

La primera hoja llamada **Tipos de Activos**, contiene un listado general de posibles activos relacionados con la información, en esta hoja se pueden insertar los ítems adicionales que se consideren necesarios, sólo digitando en una nueva fila la información deseada **(ilustración 18)**; la información en esta hoja, está almacenada con un nombre, con el fin de que pueda ser usada en la siguiente hoja para elegir los activos desplegando una lista.

1	**EQUIPOS INFORMATICOS**
2	Computador Escritorio
3	Computador Portátil
4	Equipo Virtual
5	Tablet
6	Smart Phone
7	Servidor
8	**MEDIOS DE ALMACENAMIENTO**
9	Disco Duro Interno
10	Disco Duro Externo
11	Memoria USB

Ilustración 19 Hoja de Tipos de Activos

La segunda hoja llamada **Identificación y Valoración de activos**, consta de tres partes, en la primera, se realiza un listado - inventario de activos **(Ilustración 19)**, codificándolos, clasificándolos dentro de los tipos de activos de la lista de la hoja 1, asignando los responsables de cada activo y clasificándolos como de uso crítico o no (si es un activo de uso crítico, la celda se colorea en rojo). Puede observarse esta parte en la Ilustración 19.

	A	B	C	D	E	F	G
1							
2				ACTIVO			
3	ID	NOMBRE	DESCRIPCION	RESPONSABLE	TIPO	UBICACIÓN	USO CRÍTICO
4							
5	0001	DISEÑO4	COMPUTADOR ESCRITORIO	DISEÑADOR 1	Computador Escritorio	OFIC. DISEÑO	SI
6							

Ilustración 20 Primera Parte Hoja Ident y Valorac de Activos

La segunda parte de esta hoja, permite a cada uno de los activos que se ha identificado, realizar una primera valoración basado en el impacto que tiene sobre componentes básicos de la información, confidencialidad, integridad y disponibilidad,

Esta primera valoración, permite elegir, de entre tres valores con una escala de valoración de 1 a 3, el impacto que tiene este activo sobre los componentes de la información, y en la disponibilidad, su impacto de acuerdo al tiempo en que permanezca no disponible. De las celdas se despliega una lista que permite al usuario elegir la valoración y un cuadro de ayuda que le indica la escala de valoración. Esta es una facilidad incluida en la hoja de cálculo, a través de la función de validación de campos.

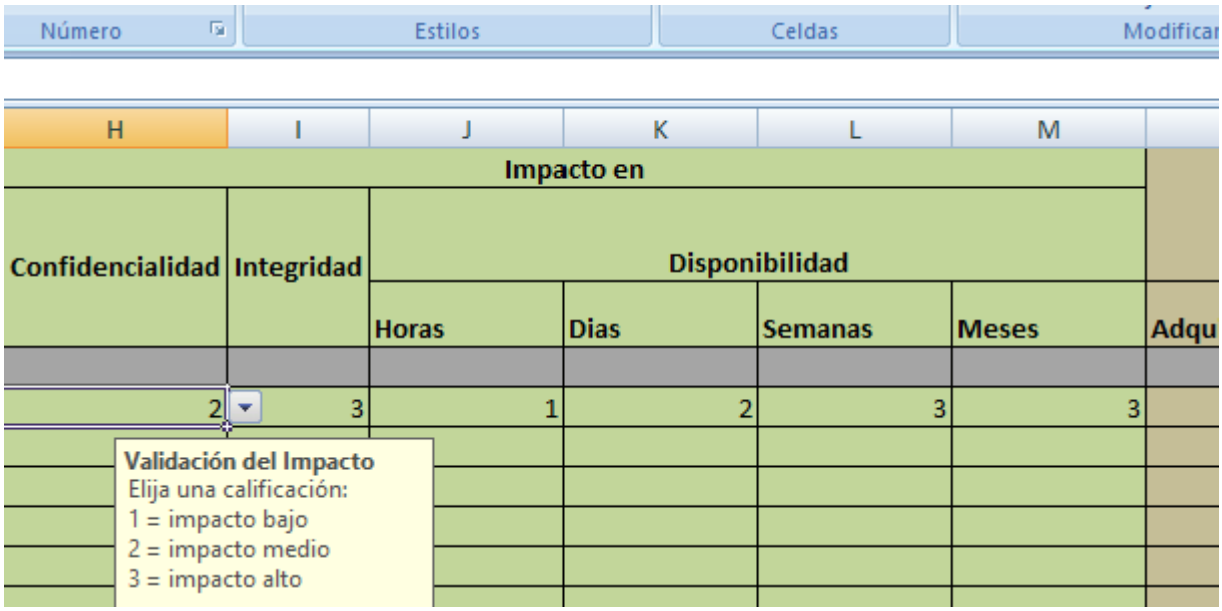
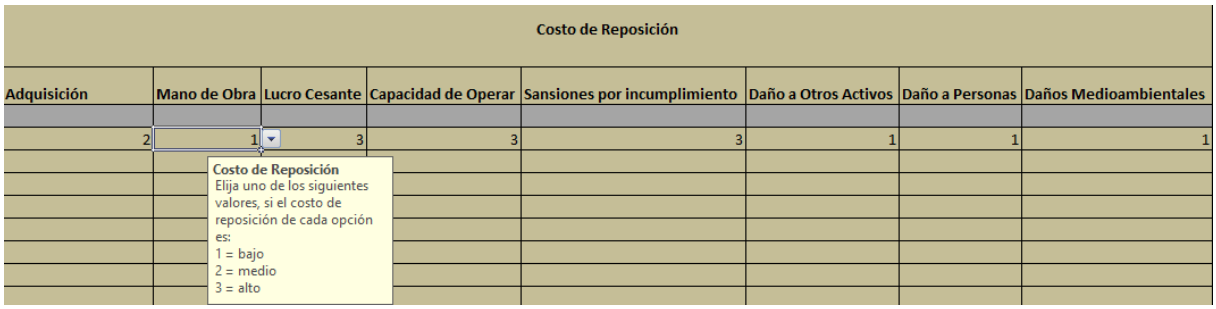


Ilustración 21 Segunda Parte Hoja Ident y Valorac de Activos

La tercera parte de esta hoja, permite hacer una valoración del activo, según su costo de reposición.



Costo de Reposición							
Adquisición	Mano de Obra	Lucro Cesante	Capacidad de Operar	Sansiones por incumplimiento	Daño a Otros Activos	Daño a Personas	Daños Medioambientales
2	1	3	3	3	1	1	1

Costo de Reposición
Elija uno de los siguientes valores, si el costo de reposición de cada opción es:
1 = bajo
2 = medio
3 = alto

Ilustración 22 Parte tres Hoja de Identi y Valorac de Activos

de 3 valores y un cuadro explicativo para su ayuda.

Una vez se ha realizado la valoración de la parte uno y la parte dos, se da una valoración total en la última columna:

V
TOTAL VALORACIÓN Muy Alto = 36 a 42 Alto = 28 a 35 Medio = 21 a 34 Bajo = 14 a 20
29
0
0

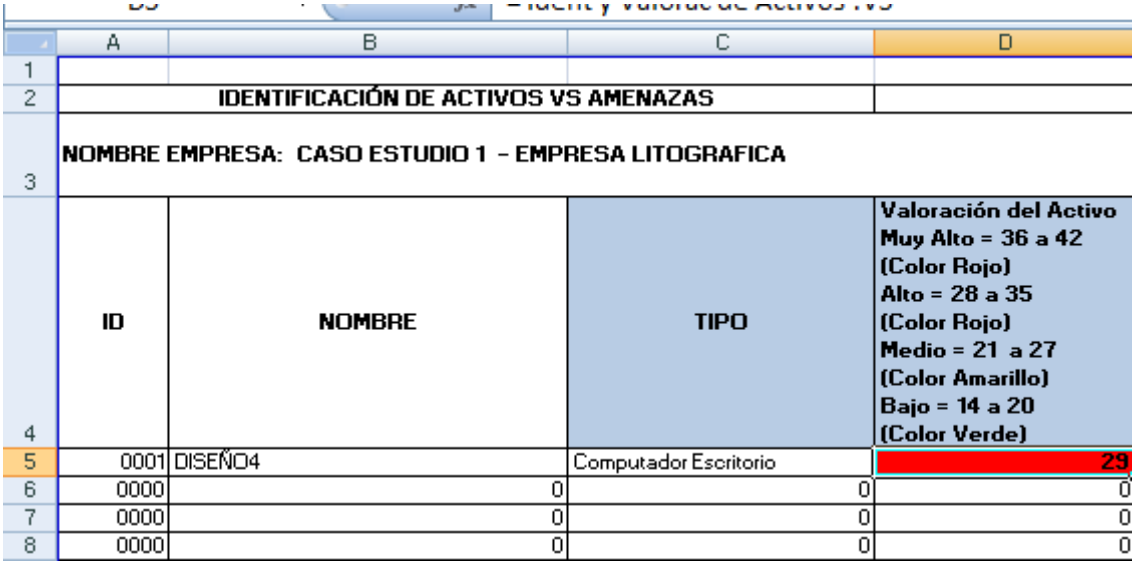
Ilustración 23 Columna Valoración Total

En este caso, la celda se coloreara, de rojo si el valor da como resultado un rango alto o muy alto. De amarillo si su resultado da una valoración del rango medio y en verde si la valoración da un resultado bajo.

Para esta coloración se utiliza la función de la hoja de cálculo de Formato condicional, aplicando tres reglas, una para cada uno de los colores especificados. Es el mismo tratamiento que se le da a la celda de la parte uno donde se clasifica el activo como crítico o no en cuyo caso sólo es necesario una regla de formato condicional.

Esta coloración en la valoración, permite la posibilidad de primero buscar mitigar los riesgos de los activos críticos con valoración alta o media, por lo tanto ya entrega una priorización de la gestión de riesgos.

En la hoja 3, llamada **Identificación de Amenazas**, hay dos partes de información, la primera se compone de los activos identificados en la hoja anterior, y su calificación de valoración total (Ilustración 22), como entrada de la identificación de amenazas que se hace en la parte dos. En esta identificación de amenazas, se podría modificar el título de las amenazas si se consideran no pertinentes y reemplazarlas por las que se consideren oportunas o necesarias, el usuario sólo tendría que modificar el título de la columna.



	A	B	C	D
1				
2		IDENTIFICACIÓN DE ACTIVOS VS AMENAZAS		
3	NOMBRE EMPRESA: CASO ESTUDIO 1 – EMPRESA LITOGRAFICA			
4	ID	NOMBRE	TIPO	Valoración del Activo Muy Alto = 36 a 42 (Color Rojo) Alto = 28 a 35 (Color Rojo) Medio = 21 a 27 (Color Amarillo) Bajo = 14 a 20 (Color Verde)
5	0001	DISEÑO4	Computador Escritorio	29
6	0000	0	0	0
7	0000	0	0	0
8	0000	0	0	0

Ilustración 24 Parte 1 Identificación Amenazas.

En la segunda parte de esta hoja, se listan por columnas agrupadas amenazas Físicas, naturales, servicios esenciales, técnicas, Otras. Cada una de estas agrupaciones presenta las siguientes opciones:

Amenazas Físicas:

- Fuego.
- Agua.
- Polvo.
- Temperatura.
- Accidente.
- Destrucción.
- Robo.

Amenazas Naturales:

- Movimientos Sísmicos.
- Inundaciones.
- Fenómenos Volcánicos.
- Derrumbes.

Amenazas en Servicios Esenciales:

- Falta de Agua.
- Falta de Aire Acondicionado.
- Falta de Suministro Eléctrico.
- Falta de Internet.

Amenazas Técnicas:

- Falla del Equipo.
- Falla del Software.
- Virus Informático.
- Pérdida de Información.
- Corto Circuito.

Otras Amenazas:

- Uso no autorizado del Equipo.
- Uso de Software sin Licencia.
- Error en uso.
- Abuso de Derechos.

Para cada una de estas amenazas, se hace una valoración de probabilidad de ocurrencia vs impacto que tendría su ocurrencia, generando un valor del riesgo, clasificado con el siguiente rango de valoración y formato de color condicional.

Riesgo Alto: Valores mayores que 5 color rojo

Riesgo Medio: Valores entre 3 y 5 color amarillo

Riesgo Bajo: Valores Menores a 3 color verde.

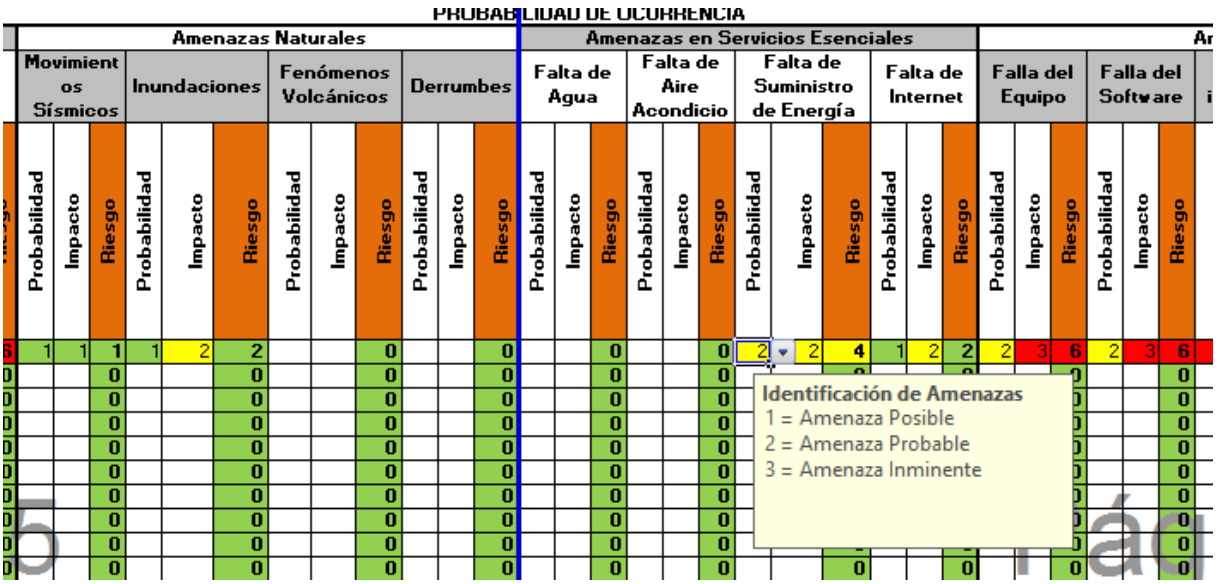


Ilustración 26 Parte 2. Valoración del Riesgo (Amenaza vs Probabilidad de Ocurrencia)

Una vez realizada esta identificación de amenazas y valoración del riesgo, se pasa a la fase de selección de controles para mitigar estos riesgos.

La siguiente hoja, llamada vulnerabilidad, permite identificar qué tan vulnerable esta la organización, respecto a ciertos hitos de control que fueron los realizados en la encuesta de revisión inicial de la organización. La encuesta sólo pretende identificar si existen ya algunos controles implementados o si por el contrario se requiere la implementación de los mismos. Esta encuesta se llamó Check list y consta de 50 preguntas y se presenta en el **Anexo B**.

Plantilla de Análisis de Riesgos.xlsx

4.2. Elección de controles de la ISO 27002

En la siguiente hoja de la plantilla, se presenta el listado de los controles de la ISO 27002, con el fin de una vez haber realizado el análisis de riesgos y se haya analizado el resultado del check list, se facilite la elección de los controles necesarios, considerando los riesgos y los recursos con los que cuente la organización. Se resaltan algunos que pueden considerarse para implementación inicial, aunque esto lo determinarán las necesidades de los procesos de cada organización. Esto no significa que los demás controles no se consideren, pero como se trata de una PYME que cuenta con recursos limitados, lo que se propone es que los demás controles se vayan implementando de acuerdo al plan de gestión de riesgos y como plan de mejora continua de manera progresiva si son aplicables.

Aquí se presenta un listado de controles tomado del portal de la ISO 27001:

Nota: La numeración aquí empieza en 5 porque se hace referencia a los controles del anexo A de la ISO 27001 que contiene los controles de la ISO 27002 (ISO 17799) numerales 5 a 15.

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información.

5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.

6.1.2 Coordinación de la seguridad de la información.

6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información.

6.1.5 Acuerdos de confidencialidad.

6.1.6 Contacto con las autoridades.

6.1.7 Contacto con grupos de especial interés.

6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.

6.2.2 Tratamiento de la seguridad en la relación con los clientes.

6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.

7.1.2 Propiedad de los activos.

7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

7.2.1 Directrices de clasificación.

7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

8.1.1 Funciones y responsabilidades.

8.1.2 Investigación de antecedentes.

8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

8.2.1 Responsabilidades de la Dirección.

8.2.2 Concienciación, formación y capacitación en seguridad de la información.

8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.

8.3.2 Devolución de activos.

8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.

9.1.2 Controles físicos de entrada.

9.1.3 Seguridad de oficinas, despachos e instalaciones.

9.1.4 Protección contra las amenazas externas y de origen ambiental.

9.1.5 Trabajo en áreas seguras.

9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos.

9.2.2 Instalaciones de suministro.

9.2.3 Seguridad del cableado.

9.2.4 Mantenimiento de los equipos.

9.2.5 Seguridad de los equipos fuera de las instalaciones.

9.2.6 Reutilización o retirada segura de equipos.

9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.

10.1.2 Gestión de cambios.

10.1.3 Segregación de tareas.

10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

10.2.1 Provisión de servicios.

10.2.2 Supervisión y revisión de los servicios prestados por terceros.

10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

10.3.1 Gestión de capacidades.

10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

10.4.1 Controles contra el código malicioso.

10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.

10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

10.7.1 Gestión de soportes extraíbles.

10.7.2 Retirada de soportes.

10.7.3 Procedimientos de manipulación de la información.

10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.

10.8.2 Acuerdos de intercambio.

10.8.3 Soportes físicos en tránsito.

10.8.4 Mensajería electrónica.

10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.

10.9.1 Comercio electrónico.

10.9.2 Transacciones en línea.

10.9.3 Información públicamente disponible.

10.10 Supervisión.

10.10.1 Registros de auditoría.

10.10.2 Supervisión del uso del sistema.

10.10.3 Protección de la información de los registros.

10.10.4 Registros de administración y operación.

10.10.5 Registro de fallos.

10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.

11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.

11.2.1 Registro de usuario.

11.2.2 Gestión de privilegios.

11.2.3 Gestión de contraseñas de usuario.

11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.

11.3.1 Uso de contraseñas.

11.3.2 Equipo de usuario desatendido.

11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.

11.4.1 Política de uso de los servicios en red.

11.4.2 Autenticación de usuario para conexiones externas.

11.4.3 Identificación de los equipos en las redes.

11.4.4 Protección de los puertos de diagnóstico y configuración remotos.

11.4.5 Segregación de las redes.

11.4.6 Control de la conexión a la red.

11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.

11.5.1 Procedimientos seguros de inicio de sesión.

11.5.2 Identificación y autenticación de usuario.

11.5.3 Sistema de gestión de contraseñas.

11.5.4 Uso de los recursos del sistema.

11.5.5 Desconexión automática de sesión.

11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.

11.6.1 Restricción del acceso a la información.

11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.

11.7.1 Ordenadores portátiles y comunicaciones móviles.

11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.

12.2.2 Control del procesamiento interno.

12.2.3 Integridad de los mensajes.

12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.

12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

12.4.1 Control del software en explotación.

12.4.2 Protección de los datos de prueba del sistema.

12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.1 Procedimientos de control de cambios.

12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

12.5.3 Restricciones a los cambios en los paquetes de software.

12.5.4 Fugas de información.

12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.

13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.1 Responsabilidades y procedimientos.

13.2.2 Aprendizaje de los incidentes de seguridad de la información.

13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

14.1.2 Continuidad del negocio y evaluación de riesgos.

14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

14.1.4 Marco de referencia para la planificación de la continuidad del negocio.

14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.

15.1.2 Derechos de propiedad intelectual (DPI).

15.1.3 Protección de los documentos de la organización.

15.1.4 Protección de datos y privacidad de la información de carácter personal.

15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.

15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.

15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información.

4.3. Políticas y Procedimientos

En esta parte se definen unas plantillas con el fin de generar la estructura básica que sea complementada por las organizaciones, adecuándola a sus procesos de negocio. Esta no es una lista exhaustiva de todas las políticas que pueden existir en una organización, sino que considera unas esenciales que si pueden tener todas las organizaciones. Una vez se tiene claridad de la estructura de las mismas se facilita que las organizaciones puedan crear nuevas o adaptar las aquí propuestas a sus necesidades.

En el Anexo D se presenta una plantilla para el desarrollo de la política de seguridad de la información, esta política de seguridad, está compuesta por los siguientes apartados:

1. **INTRODUCCIÓN:** En este apartado se hace una introducción de la importancia de la información, sus amenazas y necesidades de protegerla y garantizar la seguridad del negocio.
2. **OBJETIVOS:** Que persigue o busca la organización proteger con la implementación de la seguridad de la información.
3. **ALCANCE:** A qué parte, partes o a toda la organización voy a aplicar todo lo que se defina dentro de la política.
4. **RESPONSABILIDADES:** Cuál es la función y responsabilidad de cada cargo existente, en el área de alcance, para con la seguridad de la información y la política definida.
5. **ASPECTOS GENERALES:** Detalla aún más pero de manera general, tópicos que se tendrán en cuenta para dar cumplimiento a la política de seguridad de la información.
6. **POLÍTICAS ESPECÍFICAS:** Enumera sin detallar, las políticas específicas que se desarrollarán y se deberán cumplir, para lograr el alcance de la política de seguridad de la información.

En este apartado se considera el caso de estudio 2 que es de un hotel, para desarrollar la política de seguridad de la información que sirve como plantilla, los campos sombreados, se refiere a información que se deberá adecuar para cada organización. Los responsables hacen referencia a los cargos que existen en el hotel del Caso de Estudio, por lo que será

cada organización quién identifique los cargos relevantes y le asigne responsabilidades en la política de seguridad de la información.

En el Anexo E se presentan plantillas de políticas específicas para:

- Acuerdos de confidencialidad
- Riesgos relacionados con terceros
- Uso adecuado de los activos
- Acceso a Internet
- Correo electrónico
- Recursos tecnológicos
- Seguridad del Recurso Humano
- Control de acceso físico
- Protección y ubicación de los equipos
- Segregación de funciones
- Protección contra software malicioso
- Copias de respaldo
- Gestión de medios removibles
- Intercambio de información
- Control de acceso lógico
- Gestión de contraseñas de usuario
- Escritorio y pantalla limpia
- Segregación de redes
- Identificación de requerimientos de seguridad
- Política de seguridad de Recursos Humanos

Estas políticas específicas, definen las consideraciones apoyando el desarrollo de algún control de seguridad que se quiere implementar para minimizar o mitigar los riesgos que se le asocien.

Una vez definidas las políticas, es importante definir los procedimientos que describan la manera como se realizará una actividad específica para el cumplimiento de las políticas, en los procedimientos se define cómo se hace algo, para que pueda ser ejecutado por los funcionarios a quienes les corresponda.

En el anexo F Se da un ejemplo de procedimientos que podrían ser implementados con el fin de dejar definido la forma en que estas actividades son desarrolladas:

- Procedimiento de backups.

- Procedimiento de configuración de computador.
- Procedimiento para la utilización de dispositivos externos USB y descarga de archivos del correo electrónico.

Los procedimientos deben definir la forma como estos controles van a ser evidenciados, por lo que se requiere almacenar registros que permitan analizar la información, registrar incidentes de seguridad y retroalimentar el sistema a través de implementación o modificación de controles y permitir una mejora continua del sistema de gestión de seguridad de la información.

En el Anexo G Se presentan plantillas para llevar registros que permitan realizar un seguimiento para retroalimentar el sistema y mantener una tendencia de mejoramiento continuo.

En el Anexo H Se presentan los incidentes de seguridad que han tenido estas empresas, y posibles controles para evitarlos.

En el Anexo I Se presenta la plantilla para elaborar la carta de compromiso de la dirección.

A todas las plantillas presentadas, se les debe adicionar el encabezado y hoja de control que se plantea en el procedimiento de control de documentos del Anexo J.

4.4. Descripción de los Resultados.

Análisis de los incidentes de seguridad de las empresas caso de estudio. Posibles soluciones.

En el Anexo H se presenta un cuadro comparativo de los incidentes de seguridad de las dos empresas que se han usado como caso de estudio.
Ambas compañías han tenido situaciones de ataque por virus, aún cuando la compañía Litográfica usa software diferente en cada computador y versiones gratuitas, y la compañía Hotelera, tiene un antivirus de pago controlado por consola y que se actualiza permanentemente. Cuando se analiza esta primera situación, se encuentra que hay varios factores que hacen posible que esto impacte a ambas compañías a pesar de sus diferentes cuidados.

A continuación se muestra una tabla que nos muestra las prácticas que ellas usan y el error que su corrección se convierte en una de las posibles soluciones.

LITOGRAFÍA	
PRÁCTICA ACTUAL	**ERROR Y SOLUCIÓN**
Antivirus de versión gratuita, diferente para cada equipo.	No hay una política de antivirus que defina los lineamientos con los que se implementa el mismo en la organización. No existe un procedimiento que le indique al usuario las precauciones para el manejo de archivos adjuntos a correos o dispositivos de almacenamiento externo. Los computadores no cuentan con usuarios, todos trabajan con el usuario administrador y adicional no tienen una contraseña de acceso, está en blanco. El sistema operativo y el software de producción está desactualizado, no licenciado, por lo tanto se tienen las actualizaciones automáticas desactivadas, pero se tiene acceso a internet. Los clientes en ocasiones traen sus propios dispositivos USB para suministrar información para ser usado en su diseño.
HOTEL	
PRACTICA ACTUAL	**ERROR Y SOLUCIÓN**
Antivirus de pago, el mismo en todos los equipos y controlado por consola	No hay una política de antivirus que defina los lineamientos con los que se implementa el mismo en la organización, sin embargo hay un control central que informa a los usuarios de las detecciones encontradas en sus equipos. No existe un procedimiento que le indique al usuario las precauciones para el manejo de archivos adjuntos a correos o dispositivos de

	almacenamiento externo. (por lo tanto el equipo siempre se contagia y el antivirus lo detecta, pero el usuario no tiene prácticas para prevenir). Los equipos pertenecen a un controlador de dominio. Allí cada usuario tiene un perfil asociado a su cargo, pero en el equipo del usuario todos los usuarios están configurados como administradores, por lo tanto en el equipo pueden ejecutar cualquier programa. Los usuarios usan dispositivos de almacenamiento removibles USB para transporte de información.

Como se observa en la tabla, ninguna de las dos empresas tiene políticas, ni procedimientos definidos para el uso, instalación o actualización del antivirus, tampoco hay una capacitación en seguridad del usuario que le permita discernir antes de abrir un archivo de su origen y contenido. Los usuarios tanto en la litografía donde no existen usuarios definidos como en el hotel donde existe un controlador de dominio, tienen demasiados privilegios en el computador del usuario, por lo tanto se debe restringir, de acuerdo a las funciones y perfiles de los mismos. En el caso de la litografía es importante estandarizar el antivirus que se va a usar en todos los equipos, y evaluar si existen los recursos para la adquisición de un antivirus de pago para mayor seguridad.

Otro incidente que ambas empresas han sufrido es la pérdida de información, ya sea por ataque de virus, por discos dañados o porque los usuarios retirados la han borrado intencionalmente con el objetivo de hacer daño, se muestra a continuación una tabla con las prácticas actuales de cada una de las compañías y los errores y posibles soluciones.

LITOGRAFÍA	
PRÁCTICA ACTUAL	**ERROR Y SOLUCIÓN**
Pérdida de información por daño en disco duro o por ataque de virus que no permite leer los archivos. No se realiza backup de la información, sólo se realiza backup del	No hay políticas ni procedimientos de backups definidos, tampoco responsables de realizarlos. No se realizan backups en dispositivos

software contable, y se realiza en el mismo disco sobre el que funciona.	externos que puedan almacenarse en diferentes lugares y que sirvan para recuperar la información en caso de fallo.
HOTEL	
PRACTICA ACTUAL	**ERROR Y SOLUCIÓN**
Solo se hace backup de la información que se encuentra en la red corporativa. La información almacenada en los equipos localmente no cuentan con backup.	No existen políticas ni procedimientos de backup de la información en los equipos de los usuarios. No hay capacitación al usuario para que realice copia de su información importante en la red corporativa para que sea incluida en el backup de la organización. No hay capacitación al usuario para que haga un uso eficiente de sus archivos del correo almacenados en archivos .pst y haga un guardado aparte para recuperar o usar en caso de daño del mismo. No se hace un bloqueo del usuario o seguimiento al mismo antes de salir de la organización, una vez se reciba la renuncia o se programe su desvinculación de la misma por parte de la administración.

En este caso es necesario que se creen e implementen políticas de backup y procedimientos de backup de la información que se almacena en los equipos de los usuarios.
También se deben realizar contratos de responsabilidad de los usuarios sobre la información que por sus funciones, entran en su custodia, durante su permanencia en la organización.
Se deben generar procedimientos que definan los protocolos de retiro de funcionarios, eliminando la oportunidad de borrar los datos durante este proceso.

Otro incidente que afecta a ambas organizaciones a pesar de sus diferencias tanto a nivel de infraestructura como de formación de los usuarios, es el correo malicioso y phishing, en este caso hay tres estrategias importantes que se deben implementar:

La primera, es limitar los privilegios de los usuarios sobre el equipo local.

La segunda, capacitar a los usuarios en este tipo delictivo de delitos informáticos y seguridad de la información, para despertar en él la habilidad de discernir ante el origen y contenido de un correo electrónico.
La tercera, definir políticas y procedimientos del uso y manejo del correo electrónico, que incluya el protocolo para revisar un archivo adjunto.

Errores en conexiones eléctricas que generan daños en los equipos electrónicos, en estos casos se debe tener bien identificadas las líneas de las diferentes redes eléctricas, con el fin de evitar confusiones entre la red regulada y normal, se debe contar con personal especializado para realizar labores de este tipo, y adicionalmente se debe realizar una supervisión y documentación del trabajo realizado, con el fin de poder corregir situaciones posteriores que se presenten.

Los incidentes de la planta telefónica del Hotel, se resolvieron con ayuda del ISP quien realizó una adecuación del router y listas de control de acceso, sin embargo, es importante contar con una contraseña de la planta que controle el acceso a la misma y prevenga que personas no autorizadas puedan realizar cambios sobre la misma.

4.4.1. Ataques .vs. Mitigación

Los ataques pueden ser básicos o sofisticados, al igual que las soluciones, sin embargo las propuestas preventivas de esta metodología, pretenden dar soluciones básicas de bajo costo para las pymes que minimicen las vulnerabilidades que se tengan, aunque puedan existir otras más sofisticadas con costos económicos mayores, pero muy efectivas.
Aún así las propuestas de este trabajo van enfocadas a la mitigación de riesgos, limitando o concienciando al usuario, que es finalmente uno de los puntos críticos para la prevención de ataques, potencialmente peligrosos.
En la **tabla 3**, se relacionan, algunos de los tipos de ataques presentados en el apartado **2.6**, .vs. actividades que proponen controles para mitigarlos, siempre considerando que esta metodología pretende dar herramientas para iniciar un proceso de gestión de seguridad de la información, cuando las empresas carecen de los controles mínimos, pero teniendo en cuenta que es el inicio de un ciclo de mejora continua, que podrá en cada momento tener una mejora en las estrategias y métodos usados.

Tabla 3 Ataques vs Mitigaciones

Tipos de Ataques	Mitigación - Controles iniciales
Denegación de Servicio: ,Generalmente las puertas al ataque se abren en el equipo del usuario, por lo tanto es un punto a reforzar en la estrategia de defensa, y es la versión menos costosa de la solución, ya que en las pymes no siempre se cuenta con router administrables o firewalls avanzados. Las grandes compañías, pueden contar con soluciones más avanzadas que permiten una detección temprana de intentos de saturar los recursos, revisar las configuraciones de los routers y firewalls para detener IPs inválidas, realizar el filtrado de protocolos no necesarios, prevenir inundaciones (floods) en los protocolos TCP/UDP, habilitar los logs del loggin para llevar control de las conexiones existentes con los routers, Configuraciones de QoS como limitar tasas de transferencias provenientes de un único host, limitar las conexiones concurrentes al servidor, restringir el uso del ancho de banda por un host, monitorear las conexiones TCP/UDP que se llevan a cabo en el servidor para identificar patrones de ataque, instalar dispositivos de detección y prevención de intrusiones y un gran etcétera que tendrá valores económicos de implementación y conocimiento técnico diferentes en función de lo que se quiera proteger.	• Uso de antimalware y antivirus. • Procedimiento de uso del correo electrónico y dispositivos de almacenamiento removible. • Capacitación de seguridad que genere hábitos de discernimiento frente a tentadoras url, archivos, etc. • Procedimiento de Configuración Estandarizada de equipos. • Prevención de equipos zombis. botnet que puedan servir para atacar otros equipos o para realizar APT.
Man in the middle	

Técnica de phishing e ingeniería social son usados para hacer que el usuario realice acciones convenientes para el atacante. Se debe entrenar al usuario para desarrollar en él habilidades de discernimiento frente a estas amenazas. Esto aplica para las PYMES y para las grandes compañías aunque también se pueden implementar conexiones con SSL para cifrar los datos y crear conexiones privadas seguras.	Capacitación de seguridad que genere hábitos preventivos de seguridad.
Ataque de día Cero Esto aplica tanto a grandes compañías como a PYMES. Seguramente una gran compañía invertirá más recursos en protegerse, pero este principio básico es útil para todos los tipos de empresas.	Hay algunos antivirus comerciales que traen módulos complementarios de protección como firewall, antimalware, zero day. Adicional a esto, se debe estar atento a la publicación de este tipo de ataques y realizar las protecciones que se requieran mientras dura la ventana de vulnerabilidad y se liberen actualizaciones para corregirla.
Ataque por Fuerza Bruta Aquí nuevamente tenemos aplicación tanto en PYMES como en grandes compañías, puesto que puede haber importantes esfuerzos en configuración de los sistemas, pero si el usuario, no hace parte de esta cadena de protección, es el punto vulnerable.	• Las políticas y procedimientos de manejo de contraseñas , puede prevenir éxito de un ataque de fuerza bruta. • Capacitación de los usuarios, para concienciarlos del tipo de contraseña que deben usar.
Ingeniería Social	• Capacitación de los usuarios,

Es un punto neurálgico para la prevención de otros ataques, por lo tanto es un punto estratégico en la seguridad de cualquier compañía grande o PYME.	sensibilización y concienciación. • Limitación de privilegios del usuario.
Amenazas Internas Presentes en todas las compañías de cualquier tamaño, requiere importantes esfuerzos en todo el ciclo de la contratación de personal, desde el reclutamiento hasta el cese del empleo.	• Los procesos de selección de empleados. • Los contratos con cláusulas de responsabilidad. • Los procesos de capacitación de los usuarios. • La limitación de privilegios y segregación de funciones. • El procedimiento de finalización del empleo.

4.4.2. Ataques en grandes compañías y mitigación

Hay dos ataques de grandes compañías a los que se hizo mención en el apartado 2.6.1 y que se referencian nuevamente en esta sesión:

"**AOL: 92 millones de usuarios:** Este ataque comenzó desde dentro en 2004. Un ingeniero de la compañía que había sido despedido utilizó sus conocimientos de la empresa para infiltrarse en la red interna de AOL, y robar la lista con los correos de sus 92 millones de usuarios. Después vendió la lista online a un grupo de *spammers*.

Veteranos de EE.UU.: 76 millones de usuarios: Un disco duro que se envió a un servicio técnico en 2009 fue el punto por el que se robaron 76 millones de fichas personales de veteranos de guerra estadounidenses, incluyendo sus números de la seguridad social."

Ya que aunque fueron grandes ataques y a compañías de gran envergadura, aplican a dos procedimientos importantes que se sugieren en esta metodología, y es en el caso de AOL, el procedimiento de cesión del empleo, donde se debe realizar una acompañamiento permanente al empleado, desde el momento que se le notifica la decisión de la empresa de cesar el contrato, hasta su salida de la compañía. Realizando inmediatamente todo el proceso de cancelación de cuentas, devolución de equipos tecnológicos, en custodia del

empleado, cambio de contraseñas de su conocimiento, recordación de las clausulas de confidencialidad del contrato de inicio y sus consecuencias.

En el caso de los Veteranos de EEUU, el ataque se dio por un disco duro que se envió a soporte técnico, por lo tanto aquí también aplicaría el protocolo de retiro de equipos de la compañía, su cadena de custodia, las cláusulas de confidencialidad que se firmen con los proveedores y contratistas.

En general se puede decir, que definir y cumplir adecuadamente protocolos que permitan controlar los riesgos a los que se expone una compañía, no necesariamente requiere inversiones de dinero cuantiosas, sino una adecuada implementación de procesos suficientes dentro de las compañías y el control de su ejecución, la supervisión de los mismos, para prevenir consecuencias como las de estos dos casos, que afectaron grandes compañías y que no es exclusiva de ellas, porque como se demuestra en el Anexo H, la PYME hotelera, sufrió dos incidentes de borrado de información, por dos de sus empleados de confianza, uno por retiro voluntario y otro por despido, ambos borraron la información de sus computadoras, generando pérdida de información importante para la compañía.

4.5. Casos de Estudio

Se realizaron dos casos de estudio en dos pymes de diferentes sectores y diferentes tamaños. Una de ellas es una empresa litográfica de 12 trabajadores y la otra es un hotel de 84 trabajadores.

En primer lugar se realiza un levantamiento de las características de cada una de las empresas **Anexo A**, para luego realizar un diagnóstico inicial de la situación actual, respecto a la seguridad de la información mediante un check list **(Anexo B)** y los resultados de las dos empresas, se comparan para encontrar falencias comunes **(Anexo C)** y detectar un nivel mínimo aceptable de inicio del proceso. A partir del **Anexo D hasta el Anexo J**, se presentan diferentes plantillas que pueden ser usadas para implementar políticas, procedimientos y registros, que son base documental de la ISO 27001 y que ayudan a ejercer control sobre las falencias encontradas en la fase de diagnóstico de estas dos empresas. Ambas empresas, tienen recursos económicos, tecnológicos y de personal diferentes en cantidad y valor de inversión, sin embargo se presenta una falencia común sobre el control de los equipos de los usuarios, que permite que se pueda vulnerar desde adentro la organización y que por lo tanto es el punto de concentración del desarrollo de este trabajo.

5. Conclusiones y Trabajo Futuro

A través de esta investigación, se exploran diferentes trabajos y teorías sobre la implementación de la iso27001 en pymes, encontrando aportes que inspiraron y orientaron el desarrollo de este trabajo.

- Las pymes caso de estudio en este trabajo, tienen particularidades de infraestructura tecnológica diferente, sin embargo es común en ambas, la libertad que se tiene en el equipo del usuario, ya que no hay limitaciones de privilegios sobre el equipo, posibilitando ataques desde el interior de la organización.

- Las grandes compañías pueden tener más desarrollo en infraestructura tecnológica, pero también deben hacer esfuerzos importantes en la capacitación de los usuarios, para concienciarlos de los riesgos potenciales que tienen en sus manos, por el simple hecho de tener acceso a la tecnología.

- No es suficiente tener muchas implementaciones de medidas de seguridad, si estas no van acompañadas de políticas y procedimientos, que ayuden a consolidar mecanismos de defensa, en favor de la seguridad informática.

- Las grandes compañías deben asegurarse, que hasta la más mínima célula de la organización, está cubierta por los procedimientos de seguridad, ya que una zona descubierta, se convierte en la entrada potencial de ataques informáticos.

- Se requieren grandes esfuerzos en capacitación y control de los usuarios finales para poder detener los ataques que ingresan a través de los equipos que ellos manejan.

- Los ataques sufridos por las pymes de los casos de estudio, en su mayoría puede subsanarse con mejores prácticas de configuración de los equipos y concienciación del usuario.

- Entre las dos pymes analizadas en este trabajo, había importante diferencia en tamaño y capacidad de inversión, y se evidencian que esto marca el entorno tecnológico que estructura a cada organización, sin embargo ninguna tienen un procedimiento de backup, que permita que el usuario se pueda recuperar de un

incidente sin pérdida importante de información y los privilegios de los usuarios finales son altos.

- Hubo muchos acercamientos de investigaciones previas, hacia cómo debe una pyme implementar un sistema de gestión de la información, sin embargo es importante enfocarse en el público objetivo y facilitar su entendimiento y acceso a los recursos, motivo de este trabajo.

- - Se pueden generalizar los procedimientos y políticas a todos los tipos de empresas, realizando las adecuaciones que las personalicen, ya que complementan las que existan en las empresas, aunque se tengan soluciones costosas y sofisticadas.

- Este trabajo contribuye a la implementación de un sistema de gestión de la seguridad de la información, en cualquier compañía, especialmente en PYMES, facilitando herramientas para el análisis de riesgos y creación de la documentación.

- Al inicio de este trabajo, se planteó la siguiente hipótesis:
  ¿Se puede generar una metodología de implementación de seguridad de la información para las PYMES, que esté al alcance de sus recursos económicos y humanos?.

  Se puede concluir que la hipótesis es afirmativa, ya que en el desarrollo de la investigación, se demuestra que existen mecanismos de control que dan tratamiento a los riesgos de seguridad que sufren las PYMES, además, que las implementaciones evolucionarán a medida que el sistema madura, y podrán incrementarse en costo y complejidad, pero que puede iniciarse a la medida de la organización y como base de un sistema de gestión de mejora continua de los procesos, optimizando el uso de los recursos económicos y humanos con los que cuenta una organización. Se buscó recabar información de las grandes compañías para encontrar modelos de implementación a seguir, ya que cuentan con muchos más recursos de todo tipo, sin embargo, el acceso a estos modelos es aún muy hermético, encontrando incluso sorpresas de empleados al preguntar por esta información que decían no conocer; no hay medios de comunicación efectivos para este tipo de consultas, por lo que no se contó con material para sustraer información relevante. En los ataques analizados a grandes compañías, se puede demostrar que las propuestas de este trabajo son incluso vigentes en la prevención de algunos de estos ataques. Las PYMES pueden optar por métodos como los mencionados en el

desarrollo de este trabajo, y enfocar en principio sus esfuerzos en la concienciación de los empleados y la limitación de privilegios, tanto a nivel de perfiles de usuarios como configuración de equipos, esto ayuda a tener un punto de inicio con un bajo costo de inversión y poder ir avanzando progresivamente con un ciclo de mejora continua, hacia inversiones futuras más sofisticadas, cuando el costo beneficio, sea en favor de la PYME y se vaya generando una cultura de seguridad de la información, que permita visualizar los beneficios de ocuparse de este tema.

6. Bibliografía y Webgrafía

A. Martins, & J. H. P. Eloff. (2003). Information security culture. (IFIP TC11 17th International Conference on Information Security (SEC2002), Cairo, Egipt.)

Alineando COBIT 4.1, ITIL V3, e ISO/IEC 27002 en beneficio del negocio. (2008). (). Impreso en los Estados Unidos de América y publicado simultáneamente en las websites de ITGI, ISACA, OGC y TSO en Inglaterra y Estados Unidos de América: IT Governance Institute.

Carey-Smith, M. T., Nelson, K. J., & May, L. J. (2007). Improving information security management in nonprofit organisations with action research.

CNI. (2012). MAGERIT V3
Metodología de análisis y gestión de riesgos de los sistemas de información, Libro I: Método
Libro II: Catálogo de elementos, Libro III: Guía de técnicas. Retrieved from

https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

Compendio seguridad de la información (Marzo 2013). (ICONTEC ed.). Bogotá: Legis.

Detert, J. R., Schroeder, R. G., & Mauriel, J. J. (2000). A framework for linking culture and improvement initiatives in organizations. *Academy of Management Review, 25*(4), 850-863.

Dhillon, G., & Backhouse, J. (2001c). "Current directions in information systems security research: Toward socio-organizational perspectives.".*Information Systems Journal 11(2)*, 127-153.

Ellof, J., & Ellof, M. (2003). *"Information security management - A new paradigm."

Annual research conference of the south african institute of computer scientists and information

 . (technologists on Enablement through technology SAICSIT´03) 130-136.*

Escalera, C. M. E. (2007). *El impacto de las características organizacionales e individuales, de los dueños o administradores de las pequeñas y medianas empresas, en la toma de decisiones financieras, que influyen en la maximización del valor de la empresa.*

Furnell, S., Warren A, & Donwland P.S. (2004). *Improving security awareness and training through computer-based training. . (3rd World Conference on Information Security Education (WISE 2004), Monterey, California.)*

Giorgetty, A. (2010). *El guardián informático*

Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes*. España: AENOR - Asociación Española de Normalización y Certificación.

Helokunnas T., & Kuusisto R. (2003b). *Information security culture in a value net. 2003 IEEE . (International Engineering Management Conference (IEMC 2003), Albany, New York, USA, 2- 4 November 2003.)*

Juliá, S.(nc) *Los 5 fallos de seguridad informáticos más comunes en las PYMES.* Retrieved from http://www.gadae.com/blog/los-fallos-de-seguridad-mas-comunes-en-las-pymes/

Katz, J. E., & Rice, R. E. (2006). *Consecuencias sociales del uso de internet* Editorial UOC.

Linares, S., & Paredes, I. (2007). *IS2ME seguridad de la información a la mediana empresa. un método para acercar e implementar la seguridad de la información en las pequeñas y medianas empresas.*

CNI. (2012). MAGERIT V3

metodología de análisis y gestión de riesgos de los sistemas de información, Libro I: Método libro II: Catálogo de elementos, Libro III: Guía de técnicas. Retrieved from https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

NTC-ISO/IEC 27005: 2009 (2009). [ISO/IEC 27005:2008] (ICONTEC ed.). Bogotá: ICONTEC.

OECD. (2002). *OECD guidelines for the security of information systems and networks: Towards a culture of security. O. f. E. C.-o. a. D. (OECD). .* (). Paris: OECD.

Pallas, M. G. (2009). *Metodología de implantación de un SGSI en un grupo empresarial jerárquico*

Roa Buendía, J. F. (2013). *Seguridad informática*. España: McGraw-Hill España.

Rosanas, J. M., & Velilla, M. (2005). *The ethics of management control systems: Developing technical and moral values." . In Business Ethics 53 (Ed.), (pp. 87-96)*

S. Dojkovski, S. Lichtenstein, & M. J. Warren. (2006). Challenges in fostering an information security culture in australian small and medium sized enterprises. . (5th European Conference on Information Warfare and Security, Helsinki, Finland, 1-2 June.)

Sánchez, L. E. (2009). *Metodología para la gestión de la seguridad y su madurez en las PYMES*

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Sneza, D., Shrman, L., & Matthew, W. J. (2007). *Fostering information security culture in small and medium size enterprises: An interpretive study in australia. the fifteenth european conference on information systems, university of st. gallen, st. gallen*.

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: A holistic approach. *ISSE/SECURE 2007 securing electronic business processes* (pp. 331-339) Springer.

Van Niekerk, J. C., & Von Solms, R. (2003). *Establishing an information security culture in organisations: An outcomes-based education approach*. (ISSA 2003:3rd Annual IS South Africa Conference, , Johannesburg, South Africa, 9-11 July 2003.)

Wiander, T., & Holappa J. (2007). Managing information security in small and medium-sized organization. Handbook of research on information security and assurancence.*24*

Alto Nivel. (17 de 02 de 2014). Obtenido de http://www.altonivel.com.mx/3278-las-10-empresas-mas-valiosas-del-mundo.html

Andrés Cardenal. (17 de 02 de 2014). *Alto Nivel*. Obtenido de http://www.altonivel.com.mx/40965-apple-google-y-amazon-la-triada-accionaria-mas-valios.html

Banco Mundial. (2014). *Indicadores Banco Mundial*. Obtenido de http://datos.bancomundial.org/indicador/IT.NET.USER.P2

Cano, J. J. (2011). *Journal Online*. Obtenido de La Gerencia de la Seguridad de la Información: http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Documents/jolv5-11-LaGerencia.pdf

González, J. (06 de 10 de 2011). *Seguridad para Todos*. Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

ISO/IEC17799 (2005). (2005). *Information Technology - Security techniques - Code*.

Motorpasion. (15 de 03 de 2007). *Motorpasion*. Recuperado el 22 de 01 de 2015, de http://www.motorpasion.com/otros/por-que-son-asi-los-colores-de-un-semaforo

Portal Wap de Personal. (23 de 08 de 2012). *Publicidad*. Obtenido de https://www.youtube.com/watch?v=N6dmI7_XEh0

Semana. (11 de 06 de 2014). Obtenido de http://www.semana.com/tecnologia/novedades/articulo/los-peores-ataques-informaticos-de-2014/391376-3

Tori, C. (2008). *Hacking Ético.* Rosario, Argentina.

Ucelay, R. C. (28 de 06 de 2013). *Ucelay.* Recuperado el 13 de 01 de 2015, de http://www.ucelay.es/acuerdo-de-confidencialidad/

Wallis, G. (04 de 06 de 2013). *Las pymes no están preparadas para ataques informáticos*. Obtenido de Periódico El nuevo día: http://www.elnuevodia.com.co/nuevodia/opinion/columnistas/184201-pymes-no-estan-preparadas-para-ataques-informaticos

Wikipedia. (2002-2015). Obtenido de http://es.wikipedia.org/wiki/Microsoft

Wikipedia. (2003 - 2013). Obtenido de http://es.wikipedia.org/wiki/IBM

Wikipedia. (2003-2015). Obtenido de http://es.wikipedia.org/wiki/Apple

Wikipedia. (2004 - 2015). Obtenido de http://es.wikipedia.org/wiki/Hewlett-Packard

Wikipedia. (2006 - 2015). Obtenido de http://es.wikipedia.org/wiki/Amazon.com

Wikipedia. (01 de 02 de 2015). Obtenido de http://es.wikipedia.org/wiki/Ataque_de_d%C3%ADa_cero

Zahumenszky, C. (22 de 05 de 2014). *GIZMODO*. Obtenido de http://es.gizmodo.com/los-10-mayores-ataques-informaticos-de-la-historia-1580249145

ANEXO A (Descripción Empresas Casos de Estudio)

EMPRESA 1: LITOGRAFÍA

Descripción

Esta es una pequeña empresa, que cuenta con 12 trabajadores. En la parte administrativa 1-secretaria, 1-administradora-propietaria, 3-diseñadores gráficos. Y tiene una parte operativa con 7 operarios de máquinas o acabados litográficos.
La litografía produce papelería comercial, académica y publicitaria, contando con clientes de todos los tamaños, incluso el periódico local más importante. Allí se hace la impresión de libros académicos, tarjetas personales o para fiestas sociales, documentación comercial como facturación, recibos de caja, etc, material publicitario como volantes, plegables, afiches, vayas, pasacalles, pendones, boletería de ingreso para eventos privados, se tienen contratos con entidades gubernamentales, trabajan tanto para empresas del estado como privadas.

Obligaciones Legales

Este tipo de empresa, además de sus obligaciones tributarias, debe tener en cuenta, que la cobija legislación como: Protección de datos personales, Protección de la propiedad intelectual, Presentación de formato de medios magnéticos con las facturas pre impresas que se emiten para la actividad comercial de otras empresas, está sujeta a los contratos que se celebren con las entidades gubernamentales y las privadas, respecto a los cumplimientos, plazos, condiciones establecidas en las mismas.

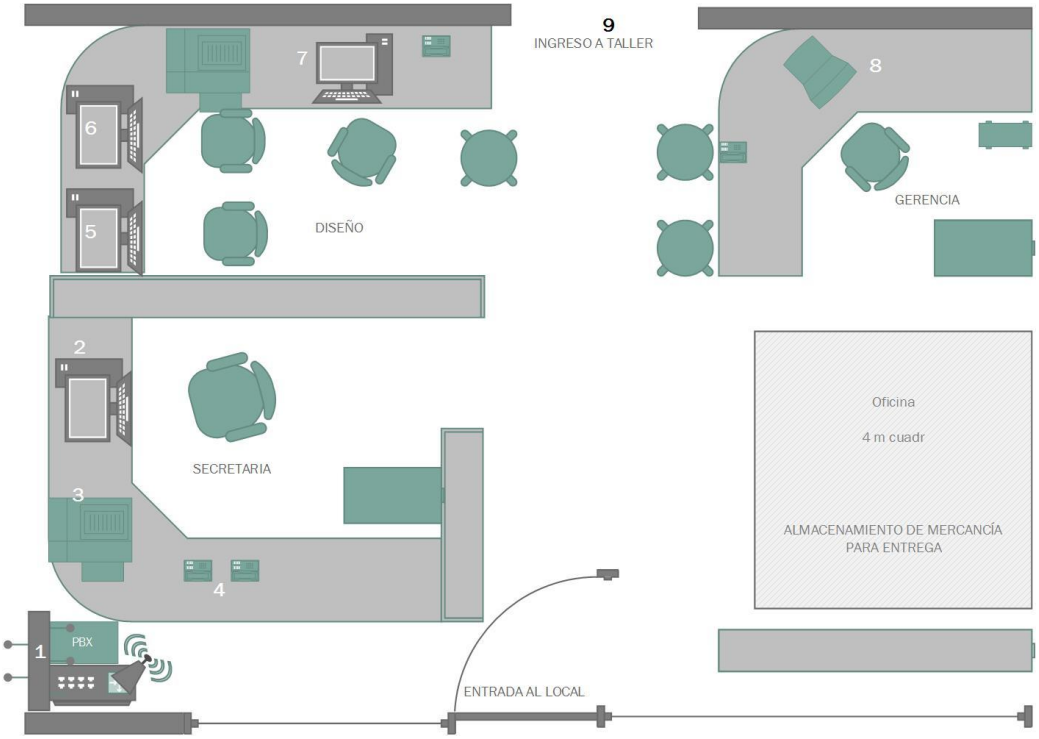
Plano Distribución de equipos en la empresa:

Este plano es una ilustración para graficar la empresa y sus procesos de negocio:

Secretaria: Es la encargada de contestar las llamadas, realizar la facturación, la comunicación directa con clientes y proveedores.

Gerencia: Se encarga de programar los trabajos para el taller, realizar las cotizaciones de los clientes, manejo de dinero, tener el suministro de materia prima para la producción, hacer la gestión para garantizar la operatividad de las máquinas.

Diseño: Es donde se hace la creación gráfica preliminar que es la base para la producción en las máquinas del taller.



Taller: Consta de dos procesos:

Producción: Consta de las máquinas que realizan la producción.

Acabados: Realizan toda la parte de terminado y detalles de la producción para poder ser entregada al cliente.

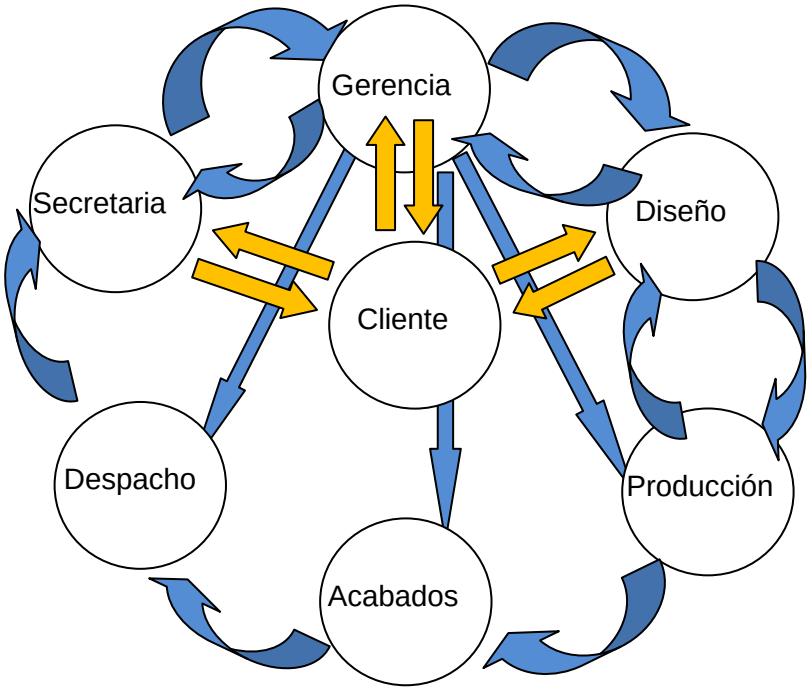
Zona de almacenamiento y despacho: Manejada por la secretaria o gerencia y se realizan envíos con el mensajero, por transportadora terrestre o aérea en caso de otros países.

Descripción física

El lindero inferior es una puerta tipo reja, con separaciones de barrotes de 10 cm, y una puerta batiente en el medio para el ingreso y salida del lugar. En la esquina inferior izquierda de la figura, hay un acopio de dispositivos, que son PBX, modem operador de internet, con opción de conexión LAN y WIFI, un switch DLINK de 16 puertos que conecta la red y distribuye el acceso a internet que recibe el modem vía LAN. En la noche se baja una

puerta replegable, que es adicional a la reja. Durante el día, la reja permanece cerrada y se abre mediante botón eléctrico. La primera oficina a la izquierda que se encuentra al ingresar es la oficina de la Secretaria, en la cual hay un computador, dos teléfonos, un archivador, esta oficina está rodeada por unas estanterías altas, en las que al llegar un cliente, debe estar de pie y el escritorio queda en el fondo a unos 70 cm de la altura de atención al cliente. contiguo a la secretaria queda el área de diseño, allí hay 3 puestos de trabajo, para los diseñadores gráficos. El primer espacio que se encuentra de la entrada a la derecha es la zona de almacenamiento y despacho, y contigua a esta está la gerencia, la cual también dispone de un computador y un archivador. Justo en el medio está el ingreso al taller, allí se encuentra toda la maquinaria de impresión, cortado, laminado, y el área de acabados.

Diagrama de Procesos

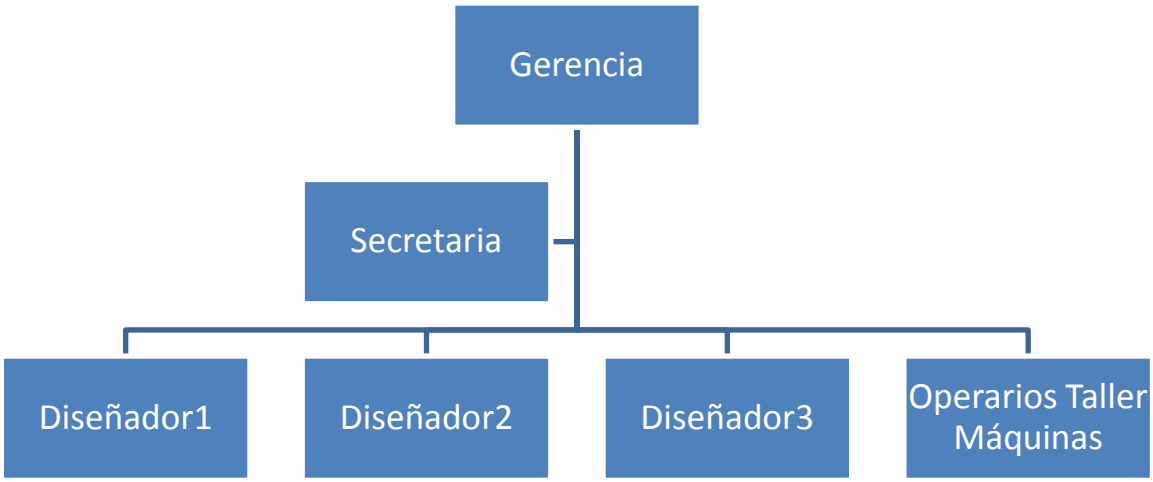


Actividades de los Procesos

Secretaria	Gerencia	Diseño	Producción	Acabados	Despacho
• Atención telefónica de clientes y Proveedores.	• Cotización de trabajos. • Asesoría al cliente. • Revisión de trabajos de los	• Realización de diseño gráfico, según especificaciones del cliente, la gerencia o	• Realizar el trabajo según la orden de producción. • Llevar	• Realizar las actividades de terminación del trabajo producido, como	• Revisar que el producto se encuentre en calidad y cantidad solicitada por el cliente.

Secretaria	Gerencia	Diseño	Producción	Acabados	Despacho
• Primera atención personal del cliente. • Facturación de trabajos. • Backup de programa de facturación. • Lectura de correo electrónico de la empresa. • Otras actividades ordenadas por la gerencia. • Gestión de recaudo de cartera. • Archivo de planchas y muestras de trabajos entregados.	diseñadores. • Programación de producción del taller. • Supervisión de trabajos en producción. • Administración de recursos financieros. • Contratación de personal. • Pago de nómina. • Programación de despacho.	incluso con acompañamiento del cliente. • impresión de planchas, o envío a impresión externa cuándo se requiere. • Separación adecuada de colores para la impresión de planchas. • Pasar a gerencia para programación en producción.	muestra a gerencia para aprobación. • Entregar a acabados para terminación. • Entregar plancha a secretaria para archivo.	laminados, emblocados, troquelados, argollados, corte, etc. • Entregar a despachos. • Entregar muestra a secretaria para archivo.	• Coordinar con el cliente la entrega del producto terminado.

Organigrama



EMPRESA 2: HOTEL

Descripción

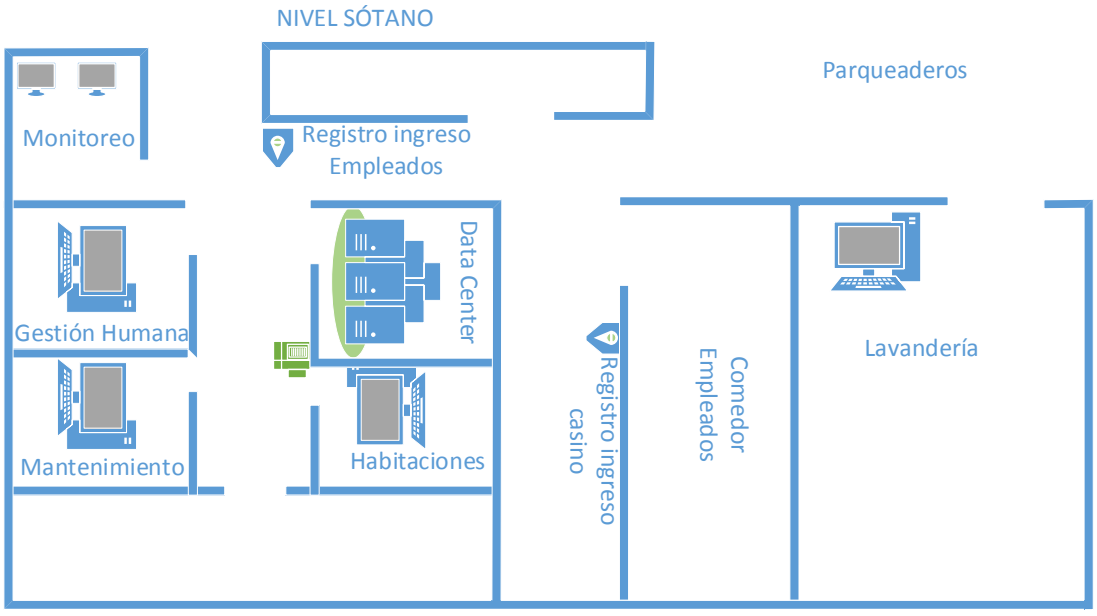
El hotel evaluado es un hotel de lujo, ubicado en una zona prestigiosa de la ciudad de Medellín, rodeado de zonas comerciales y de negocios.

Dentro del hotel se ofrecen servicios de alojamiento, alimentos y bebidas y lavandería. Para lograr la oferta de estos servicios, se tienen áreas administrativas como: Financiera, Compras, Gerencia, Mantenimiento, Gestión Humana, Información y Tecnología, Seguridad, Mercadeo y Ventas. Y áreas operativas como: Recepción y Reservas, Alimentos y Bebidas (A&B), Habitaciones, Lavandería.

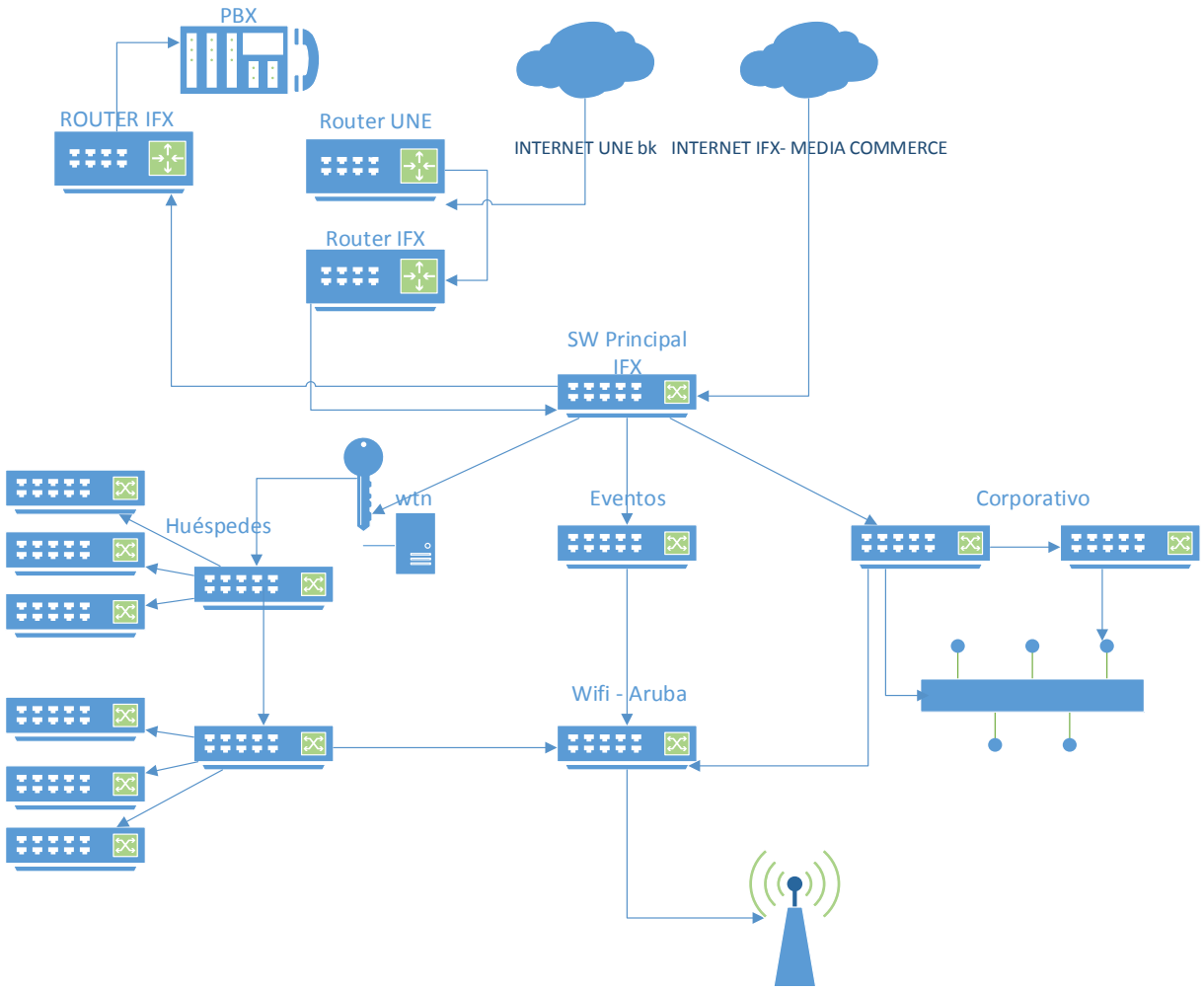
Obligaciones Legales

Este tipo de empresa, además de sus obligaciones tributarias, debe tener en cuenta, que la cobija legislación como: Protección de datos personales, Protección de la propiedad intelectual. El hotel está certificado en una norma Colombiana de Turismo Sostenible, que abarca Aspectos Culturales, Sociales, Culturales y Ambientales, que obliga al hotel a cumplir con toda la normativa que aplique a cualquiera de los aspectos de la norma.

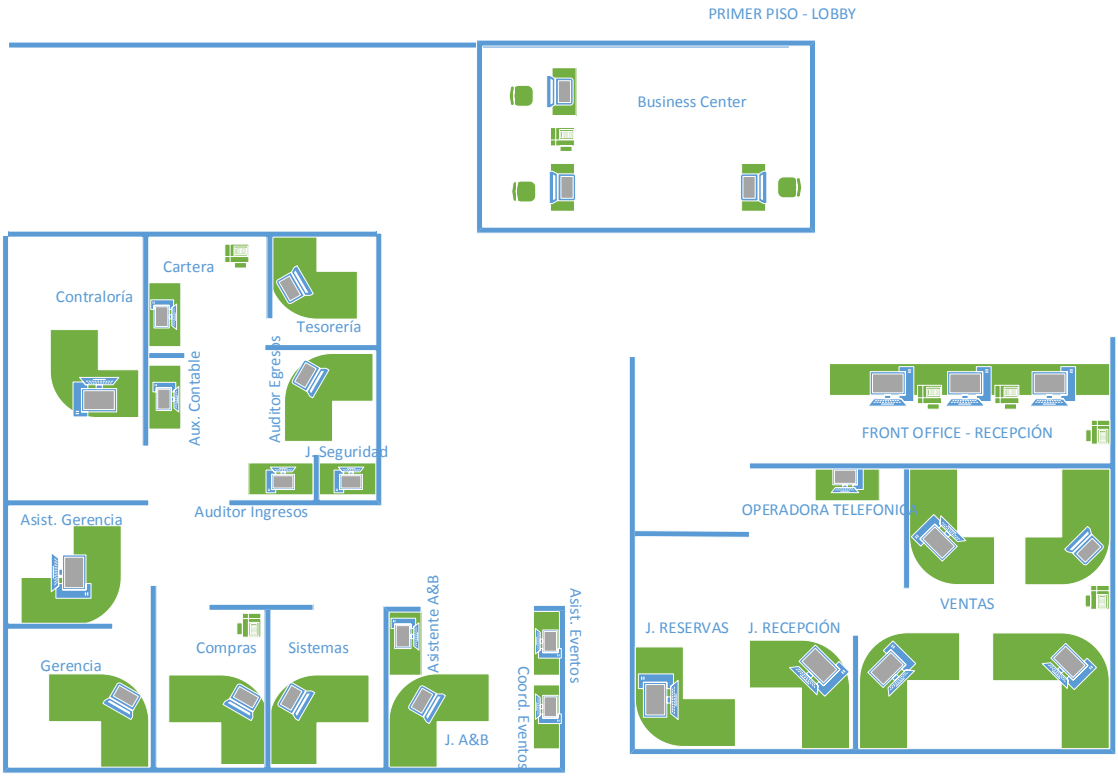
Plano Distribución de equipos en la empresa:



Al interior del Data Center e infraestructura de Tecnología y Comunicaciones.



Nivel 1



Nivel 2

En el nivel 2 sólo hay un computador en el área de cocina y una estación touch para facturación de punto de ventas.

Nivel 3 a 11

Son los niveles de habitaciones del hotel, hay 4 access point distribuidos en los pasillos que están compuestos por 15 habitaciones cada uno.

HAB 12	**HAB 11**	**HAB 10**	**HAB SUIT 09**		**HAB 08**	**HAB 07**	**HAB 06**	**HAB 05**
								
ASCEN. SERVIC	**HAB 13**	**HAB 14**	**HAB 15**	**ASCEN HUESP**	**HAB 01**	**HAB 02**	**HAB 03**	**HAB 04**

Descripción física

Es un edificio Comercial – Sector Hotelero, construcción moderna. Que tiene 7 años de construido y cuenta con un sótano destinado a parqueaderos y once pisos distribuidos de la siguiente forma:

- **Sótano:** Lavandería, Comedor de Empleados, Almacén, almacén de mantenimiento, oficina de sistemas, oficina de compras, oficina de mantenimiento, porcionamiento, cava, oficina de seguridad y data center.

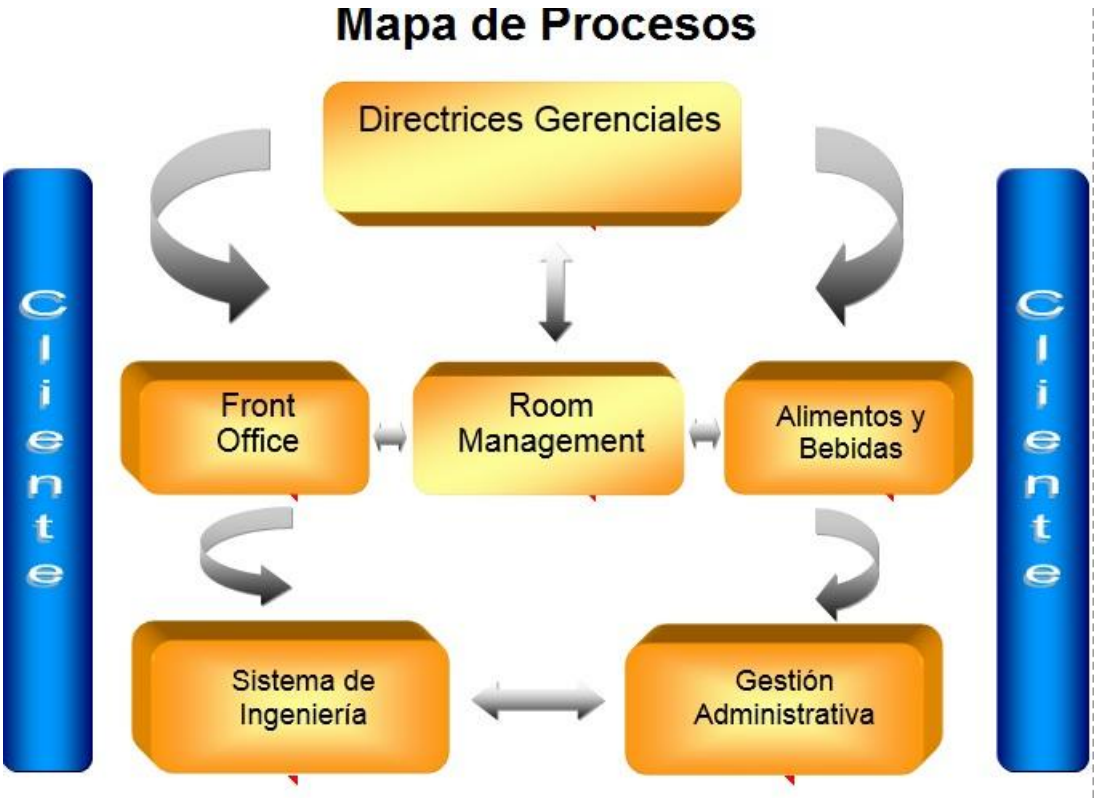
- **Piso 1:** Lobby 1, Recepción, Bar Pegasus, Business Center, Baños Públicos, Oficina de ventas, Oficinas Administrativas, Salón Centaurus, salón Lacerta, salón Lyra, salón Ara, planta emergencia.

- **Piso 2:** Restaurante Signus, Spa, Área Húmeda, Baños Públicos, Piscina, Cocina, Room Service, Steward.

- **Piso 3:** 14 habitaciones.

- **Pisos 4 al 11:** 15 Habitaciones en cada uno de los pisos.

Diagrama de Procesos



Actividades de los Procesos

Departamento de Habitaciones

Mantener en perfectas condiciones de limpieza, decoración y armonía el conjunto de elementos que determinan el confort en las habitaciones y áreas públicas. Esto implica: Garantizar habitaciones limpias, confortables y con la dotación completa que logre la satisfacción del huésped además de mantener en excelente estado de limpieza las áreas públicas, recreativas y administrativas.

Ejercer el control de la distribución de la lencería a los linos y control de consumo de suministros de aseo y de huéspedes. Entregar y recibir uniformes y mantelería de los respectivos usuarios y aplicar el control de inventario.

Asegurar y garantizar el lavado de lencería, mantelería, uniformes y ropa huésped acorde a los estándares de calidad establecidos.

A partir de éstos objetivos se configuran áreas funcionales y cargos que identifican determinados procesos y procedimientos bajo la responsabilidad del director de habitaciones, estas áreas son:

- Habitaciones (supervisores y camareras)
- Aseo áreas públicas
- Lavandería

Departamento de Recepción

Front Operations es el término que identifica un conjunto de actividades que apuntan a la atención permanente de las necesidades del huésped en cuanto a reserva de alojamiento, traslado del aeropuerto al hotel, registro (Check In), solicitudes durante la estadía y salida (Check Out). Por lo tanto el objetivo es asegurar que el ciclo de estadía del huésped (Guest Cicle) se cumpla con excelencia, eficacia y eficiencia.

Para cubrir este objetivo se definen funciones que cubren la pre-venta de habitaciones (reservas), transporte, Check In, atención a las solicitudes (Guest Service) y Check Out. Se configuran las siguientes áreas funcionales que identifican determinados procesos y procedimientos bajo la responsabilidad del director de recepción.

Front office operations: Reservas, Portera, Conserjes (Recepcionistas), Botones.

En RESERVAS se asegura que el primer contacto entre el huésped y el hotel al solicitar alojamiento sea eficiente y satisfaga las necesidades, garantizando que el servicio ofrecido se cumpla. Son procesos de información que aseguran la venta de alojamiento.

En RECEPCION los conserjes, reciben al huésped con excelente atención y expresando una sincera bienvenida. Se aplica el proceso de registro eficientemente asegurando que la información facilite el control de ocupación, facturación y forma de pago (check in); se asegura que el estado de la cuenta (folio) se haya registrado adecuadamente los cargos (débitos) y sus soportes. Aplicar en forma eficiente el proceso de cancelación con excelente atención para que se lleve a feliz término el check out del huésped.

En BOTONES se ofrece al huésped una calurosa bienvenida, asistiendo en la manipulación de equipaje. Acompañarlo a la habitación y enseñarle los servicios ofrecidos por el hotel. Se maneja en forma correcta los mensajes, fax y encomiendas.

Departamento de Alimentos y Bebidas

Asegura que las especificaciones del producto y los estándares de servicio de A&B se cumplan con excelencia, eficacia y eficiencia. Para lograr este objetivo es requisito aplicar las siguientes responsabilidades:

- Manipulación y conservación de materia prima de alimentos y bebidas.
- Sistema de producción de alimentos y bebidas.
- Control del consumo de alimentos y bebidas.
- Sistema de servicio de alimentos y bebidas.
- Control de activos de operación, muebles y equipos.

Para cumplir con estas responsabilidades es necesario aplicar tres importantes logísticas:

- Organización del servicio (Capitanes de servicio, barman y cajero).
- Sistema de producción (cocina caliente – primeros cocinero y auxiliares; cocina fría – primeros cocineros y porcionador).
- Stewar.

Departamento de Mercadeo y Ventas

Se encarga principalmente, de generar y mantener la demanda requerida que conduzca al aprovechamiento de la capacidad instalada y a la colocación de productos a precios competitivos. La función de mercadeo para lograr el objetivo descrito se centra en aplicar estrategias de producto, precio, promoción, publicidad y comercialización.

Departamento de Gestión Humana

Debe disponer de un recurso humano comprometido que logre un buen nivel de competencia. Para tal efecto es requisito aplicar esfuerzos administrativos que conduzcan al mejoramiento del recurso humano buscando el objetivo de crear una cultura de servicio.

Para esto es necesario aplicar una serie de programas que apunten al incremento del bienestar social (mejoramiento del nivel de vida), beneficios y salud ocupacional (mejoramiento de condiciones de trabajo), desarrollo del personal (entrenamiento y capacitación) y sistema de vinculación & contratación (selección, contratación e inducción).

Departamento de Mantenimiento

Debe optimizar la capacidad operativa del activo (edificio, muebles y equipos) y la conservación del mismo a través de planificar, organizar y ejecutar los programas de mantenimiento preventivo y curativo que garanticen el funcionamiento de los sistemas hidráulico, eléctrico, refrigeración, aire mecánico, calefacción, comunicación y transporte vertical.

El derecho de uso del activo que se le concede al huésped involucra que dicho recurso se muestre en estado óptimo y seguro. Es un compromiso integral mantener este activo en la forma que espera el huésped y los mismos anfitriones. Para cumplir con estos objetivos se configura la estructura organizacional de mantenimiento compuesta por el jefe de mantenimiento, auxiliares de mantenimiento

Departamento de Seguridad

Se encarga de prevenir el delito y contravenciones a la vida y bienes de los huéspedes, anfitriones y proveedores. La acción de seguridad debe adaptarse a las actuales necesidades y exigencias que impone la delincuencia organizada. Es un compromiso global el minimizar riesgos y garantizar el normal funcionamiento del hotel.

La planificación, organización y ejecución de los procedimientos necesarios para cumplir el objetivo descrito está bajo la responsabilidad del jefe de seguridad que tiene la colaboración de los supervisores y agentes de vigilancia.

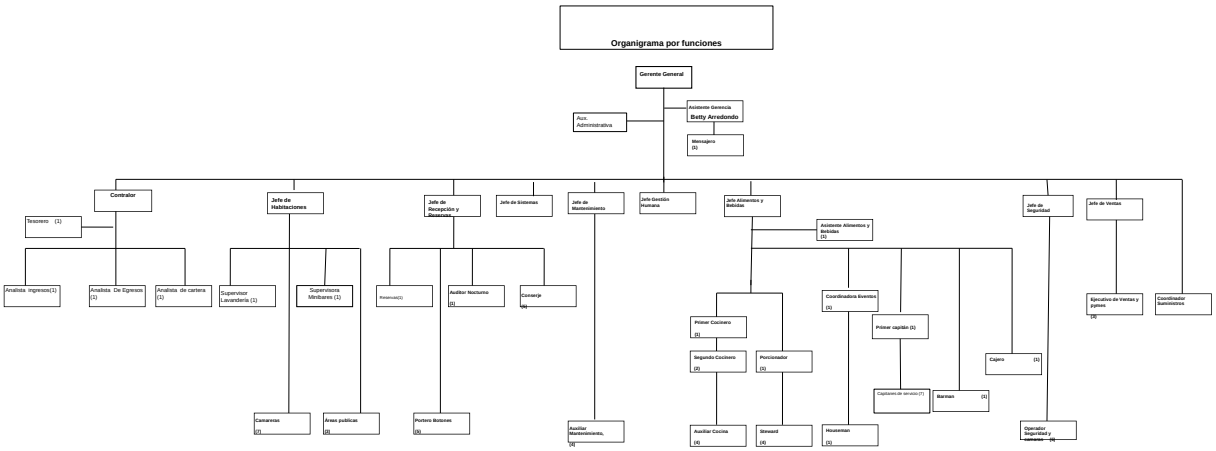
Departamentos de Contraloría y Sistemas

Se encargan de planificar, organizar, dirigir y controlar las áreas de gestión (control operacional & financiero, mercadeo, mantenimiento, quality assurance o operación, recurso humano, comunicación y seguridad) que hacen posible y garantizan la optimización de la operación.

Gerencia General

Debe planificar, organizar, dirigir y controlar las áreas de gestión (control operacional & financiero, mercadeo, mantenimiento, quality assurance u operación, recurso humano y seguridad) que hacen posible y garantizan la optimización de la operación.

Organigrama



ANEXO B. CHECK LIST

1. Se tiene implementada en la organización una política de seguridad?
2. Se tiene identificada y clasificada por escrito la información sensible e importante de la organización?
3. Se tienen procedimientos documentados de las tareas importantes?
4. Se tiene inventario de las licencias de software y su vigencia?
5. Se tiene un sistema de antivirus instalado?
6. Se cuenta con un procedimiento de uso de memorias USB?
7. Se realizan controles de acceso a los computadores?
8. Se tiene un procedimiento escrito de política de contraseñas?
9. Se realizan actualizaciones al sistema operativo y software de uso de la organización?
10. Se tienen perfiles de usuario y sus funciones?
11. Se tiene una red de computadoras configurada?
12. Existen procedimientos escritos que definan los parámetros de configuración de la red?
13. Se tiene firewall para proteger el sistema?
14. Se realizan contratos de confidencialidad con los empleados?
15. Se realizan contratos de confidencialidad con los clientes?
16. Se realizan contratos de confidencialidad con los proveedores?
17. Se tienen programas de mantenimiento preventivo de los equipos de cómputo?
18. Se realizan copias de seguridad de la información?
19. Existen procedimientos definidos para las copias de seguridad?
20. Se tienen protecciones eléctricas para los equipos de cómputo?
21. El acceso físicos a los equipos críticos se encuentra controlado?
22. Se tiene acceso a internet?
23. Se tiene control sobre el contenido que puede ser visitado en internet?
24. Se tiene un procedimiento que indique las actividades permitidas y prohibidas del uso del internet?
25. Se hace uso del correo electrónico en la organización?
26. Se tiene una política de uso del correo electrónico?
27. Se realizan capacitaciones de seguridad al personal de la organización?
28. Se tienen responsabilidades asignadas a los funcionarios respecto a la seguridad de la información?
29. Se realiza una investigación de seguridad al personal que se requiere contratar?

30. Se realiza la restricción de los permisos y accesos al personal que es desvinculado de la organización, y está por escrito en un procedimiento?
31. Se tienen dispositivos que controlen los flujos y cortes de energía que usan los computadores?
32. Se tienen sistemas de extinción de incendios en las diferentes zonas de la organización?
33. Saben los empleados el uso de estos dispositivos de extinción de incendios y se realiza capacitación sobre su uso?
34. Existe un procedimiento de uso y revisión de los extintores?
35. Se tiene contrato de vigilancia para las instalaciones?
36. Se tienen seguros que cubran daños y pérdidas de la organización?
37. Se tiene control sobre las personas que abren y cierran la organización y registro de los tiempos que permanecen solos?
38. Se tiene identificada la legislación aplicable a la organización?
39. Se tiene un análisis de riesgos de seguridad en la organización?
40. Considera que tiene controles de seguridad implementados? cuáles?
41. Considera que un incidente de seguridad puede poner en peligro la continuidad del negocio y por qué?
42. Tiene un funcionario designado responsable de la seguridad física y/o lógica de la organización.
43. Se tienen implementados procedimientos que definan los parámetros para la retirada de equipos de las instalaciones de la organización?
44. Considera importante implementar controles de seguridad complementarios a los existentes?
45. Se llevan registros de los incidentes de seguridad que suceden en la organización?
46. Se tiene un procedimiento definido con las indicaciones a seguir cuándo se presenta un incidente de seguridad?
47. Se tienen políticas de escritorio y pantalla limpias?
48. Se permite el soporte externo por acceso remoto a los equipos de cómputo?
49. Se cuenta con equipos portátiles que ingresen y salgan frecuentemente de la organización?
50. Se tiene procedimiento definido para el uso de los equipos portátiles o discos removibles que salen y entran de la organización?

ANEXO C. COMPARACIÓN CHECK LIST CASOS DE ESTUDIO

Pregunta del check list	Litografía	Hotel
1	NO	NO
2	NO	NO
3	NO	NO
4	NO, usan software sin la licencia adecuada. Y el programa contable ya no tiene soporte.	SI
5	SI, versiones gratuitas diferentes en cada uno de los 5 computadores existentes.	SI, symantec, controlado por consola desde la oficina central.
6	NO	NO
7	NO	SI, por contraseña (controlador de dominio)
8	NO	NO
9	NO	SI
10	NO	SI
11	SI	SI
12	NO, no hay nomenclaturas ni direcciones ip definidas claramente.	NO, solo se tiene definido el uso de nombres e ip en un procedimiento.
13	NO	SI, Fortiguard controlado desde oficina central
14	NO	NO
15	NO	NO
16	NO	NO
17	NO	SI
18	NO, se hace una sólo del programa contable que la hace automáticamente en el mismo equipo al salir de la aplicación.	NO, sólo se hace backup de la información que se almacene en el file server y esto programado desde la oficina central, pero no de los equipos locales.

19	NO	NO
20	NO	SI, Están conectados a una red regulada alimentada por UPS.
21	NO	SI, hay un Data Center con control de acceso físico.
22	SI	SI
23	NO	SI, controlado por el firewall desde la oficina central.
24	SI	SI
25	NO	NO
26	NO	NO
27	NO	NO
28	NO	NO
29	NO	SI
30	SI, no por escrito	SI, no por escrito
31	NO	N/A, se trabaja con energía regulada por UPS
32	SI	SI
33	SI, no se da capacitación.	SI, se hace capacitación anual.
34	NO	NO
45	SI	SI
36	NO	SI
37	SI	SI
38	NO	SI
39	NO	NO
40	SI, la alarma de seguridad con clave, las llaves solo se le entregan a personal de confianza y la puerta reja permanece cerrada y tiene acceso por botón eléctrico.	SI, algunos implementados desde oficina central como las contraseñas de los usuarios, los controles de acceso a áreas restringidas, el acceso de internet a sitios inadecuados.
41	SI, si se perdiera la información de los computadores, sería como quedar en cero y sería un inconveniente muy grande.	SI, la falta de información, la no disponibilidad de los equipos en el momento que se requiere, el acceso a internet, son aspectos esenciales del funcionamiento del

		negocio.
42	NO, sólo hay un celador que cuida en las noches y la compañía de la alarma de seguridad.	SI, hay un jefe de seguridad física y hay un jefe de sistemas, y en oficina central hay personas que administran los accesos de usuarios y controlan el firewall.
43	NO	NO, pero si hay un formato de control de salida de activos.
44	SI, casi no tenemos.	SI, es fundamental.
45	NO	NO
46	NO	NO
47	NO	NO
48	SI, por team viewer	SI, se accede por una VPNSSL por los funcionarios de sistemas desde el exterior, o internamente por Ultra VNC.
49	NO	
50	NO	NO

ANEXO D - MODELO DE POLÍTICA DE SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN <<NOMBRE DE LA EMPRESA>>

INTRODUCCIÓN

La información es un activo importante para la organización, el cuál debe ser protegido adecuadamente. Con el avance tecnológico y la creciente interconexión, este activo se ve cada vez más amenazado, e independientemente de su forma, impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, se expone a una gran variedad de amenazas y vulnerabilidades.

Con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daños y asegurar el eficiente cumplimiento de los objetivos de la organización, se implementan controles que gestionen la seguridad de la información, los cuales incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario, para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

OBJETIVOS

- Proteger los recursos de Información de <<NOMBRE DE LA ORGANIZACIÓN>> y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- Proporcionar a la gerencia, la dirección y soporte, para la seguridad de la información, en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.
- Mantener la Política de Seguridad actualizada, con el fin de asegurar su vigencia y nivel de eficacia.

ALCANCE

Esta Política se aplica en <<toda la organización o especificar qué partes>>, a sus recursos y a la totalidad de los procesos, ya sean internos o externos, vinculados a la entidad a través de contratos o acuerdos con terceros.

RESPONSABILIDADES

Todos los directivos de <<NOMBRE DE LA ORGANIZACIÓN>>, son responsables de la implementación de esta Política de seguridad de la información, dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha política por parte de su equipo de trabajo.

La Política de Seguridad de la Información, es de aplicación obligatoria para todo el personal de la organización, de todas las áreas y sea cualquiera que sea el nivel de tareas que desempeñe.

Es responsabilidad de La **Gerencia General** aprobar esta Política y es responsable de la autorización de sus modificaciones.

La **Dirección de Información y Tecnología corporativa** procederá a revisar y proponer a la Gerencia General <<NOMBRE DE LA ORGANIZACIÓN>>, la aprobación de la Política de Seguridad de la Información, y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información, evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la organización y coordinar el proceso de administración de la continuidad de las actividades de la organización.

El **Director de Tecnología y Jefe del Data Center**, serán los responsables de coordinar las acciones de los Jefes de Sistemas y Coordinadores y de impulsar la implementación y cumplimiento de la presente Política.

Los **Jefes de Sistemas y Coordinadores** cumplirán funciones relativas a la seguridad de los sistemas de información de la organización, incluyendo la supervisión e implementación correspondiente de todos los aspectos a los temas tratados en la presente Política. Deberán implementar y supervisar el cumplimiento de las políticas, procedimientos y prácticas definidas en el marco de ésta política.

Los **Propietarios de la Información** (desde el punto de vista técnico no jurídico)**,** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable del Área de Recursos Humanos** o quién desempeñe estas funciones, cumplirá la función de notificar a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cago la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de Confidencialidad y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la organización con sus empleados y con terceros. Así mismo, asesorará en materia legal a la organización, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de la Seguridad de la Información vigente.

El responsable de la **Auditoría Interna** o quién sea propuesto por el equipo de Seguridad de la Información, es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

ASPECTOS GENERALES

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos.

- Los activos de información de <<NOMBRE DE LA ORGANIZACIÓN>>, serán identificados y clasificados para establecer los mecanismos de protección necesarios.
- <<NOMBRE DE LA ORGANIZACIÓN>> definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la organización.

- Todos los funcionarios y/o contratistas, serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la organización.
- Es responsabilidad de todos los funcionarios y contratistas de <<NOMBE DE LA ORGANIZACIÓN>>, reportar los incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Las violaciones a las Políticas y Controles de Seguridad de la información serán reportadas y se tratarán según las disposiciones contractuales y legales.
- <<NOMBRE DE LA ORGANIZACIÓN>> contará con un Plan de Continuidad del Negocio, que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.
- <<NOMBRE DE LA ORGANIZACIÓN>> implantará todos los controles destinados a impedir infracciones y violaciones de las leyes del derecho civil y penal de las obligaciones establecidas por las leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

POLÍTICAS ESPECÍFICAS

En aras de generar los controles necesarios para cumplir con las políticas generales, se generan políticas específicas, las cuales podrán contar con procedimientos, lineamientos o directrices con el fin de que sea claro para todo el personal de la organización:

- **Acuerdos de confidencialidad**
- **Riesgos relacionados con terceros**
- **Uso adecuado de los activos**
- **Acceso a Internet**
- **Correo electrónico**
- **Recursos tecnológicos**
- **Seguridad del Recurso Humano**
- **Control de acceso físico**
- **Protección y ubicación de los equipos**
- **Segregación de funciones**
- **Protección contra software malicioso**
- **Copias de respaldo**
- **Gestión de medios removibles**

- **Intercambio de información**
- **Control de acceso lógico**
- **Gestión de contraseñas de usuario**
- **Escritorio y pantalla limpia**
- **Segregación de redes**
- **Identificación de requerimientos de seguridad**
- **Política de seguridad de Recursos Humanos**

ANEXO E. POLÍTICAS ESPECÍFICAS

(ISO/IEC17799 (2005), 2005)

POLÍTICAS ESPECÍFICAS <<NOMBRE DE LA ORGANIZACIÓN>>

Acuerdos de confidencialidad

[ISO/IEC 27001:2005 A.6.1.5]

Todos los funcionarios de <<NOMBRE DE LA ORGANIZACIÓN>> y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la organización, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de <<NOMBRE DE LA ORGANIZACIÓN>> a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Riesgos relacionados con terceros

[ISO/IEC 27001:2005 A.6.2.2]

<<NOMBRE DE LA ORGANIZACIÓN>> identifica los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Uso adecuado de los activos

[ISO/IEC 27001:2005 A.7.1.3] [Acuerdos 047 y 056 de 2000 Archivo General de la Nación]

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de Área o Dependencia.

Todos los funcionarios y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un “acuerdo de confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerado como un “incidente de seguridad”.

Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de <<NOMBRE DE LA ORGANIZACIÓN>>, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a) No está permitido:

El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de <<NOMBRE DE LA ORGANIZACIÓN>>.

El intercambio no autorizado de información de propiedad de <<NOMBRE DE LA ORGANIZACIÓN>>. de sus clientes y/o de sus funcionarios, con terceros.

La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b) <<NOMBRE DE LA ORGANIZACIÓN>>. debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

c) Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d) Los funcionarios y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre de <<NOMBRE DE LA ORGANIZACIÓN>>. posiciones personales en encuestas de opinión, foros u otros medios similares.

e) El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de <<NOMBRE DE LA ORGANIZACIÓN>>.

Correo electrónico

Los funcionarios y terceros autorizados a quienes <<NOMBRE DE LA ORGANIZACIÓN>> les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a) La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de <<NOMBRE DE LA ORGANIZACIÓN>>. así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

b) Los mensajes y la información contenida en los buzones de correo son propiedad de <<NOMBRE DE LA ORGANIZACIÓN>> y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

c) El tamaño de los buzones de correo es determinado por la Dirección de Tecnología de acuerdo con las necesidades de cada usuario y previa autorización del Jefe de la dependencia correspondiente.

d) El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por la Dirección de Tecnología.

e) No es permitido:

Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Organización, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

Utilizar la dirección de correo electrónico de <<NOMBRE DE LA ORGANIZACIÓN>> como punto de contacto en comunidades interactivas de contacto social, tales como *facebook* y/o *myspace*, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

El envío de correos que superen los 10 MB de tamaño de archivos adjuntos.

El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y la Dirección de Tecnología.

La configuración del correo electrónico en celulares, ipad, portátiles y equipos tecnológicos en general que no sean del propiedad de <<NOMBRE DE LA ORGANIZACIÓN>>. Ver numeral G de recursos tecnológicos.

f) El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que <<NOMBRE DE LA ORGANIZACIÓN>> proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

g) El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Oficina Asesora de Comunicaciones y la autorización de la Dirección de Tecnología. Además, para terceros se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia,

realizar envío de correo masivo, de manera frecuente, éste debe ser canalizado a través de la Dirección de Tecnología, con el fin de garantizar el cumplimiento de la Ley de Protección de Datos Personales (Habeas Data)

h) Toda información de <<NOMBRE DE LA ORGANIZACIÓN>> generada con los diferentes programas computacionales, que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Dirección de Tecnología. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información. Se debe garantizar en todo momento el cumplimiento de la Ley de Datos Personales.

i) Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por <<NOMBRE DE LA ORGANIZACIÓN>> y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por <<NOMBRE DE LA ORGANIZACIÓN>> a sus funcionarios y/o terceros se reglamenta bajo los siguientes lineamientos:

a) La instalación de cualquier tipo de software o hardware en los equipos de cómputo de <<NOMBRE DE LA ORGANIZACIÓN>> es responsabilidad de la Dirección de Tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por <<NOMBRE DE LA ORGANIZACIÓN>> a través de esta Dirección.

b) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por la Dirección de Tecnología.

c) La Dirección de Tecnología debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d) Únicamente los funcionarios y terceros autorizados por la Dirección de Tecnología, previa solicitud escrita por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica de <<NOMBRE DE LA ORGANIZACIÓN>>.

e) No está permitido el uso de equipos tecnológicos personales en las redes corporativas de <<NOMBRE DE LA ORGANIZACIÓN>>.

f) Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de <<NOMBRE DE LA ORGANIZACIÓN>>; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Dirección de Tecnología.

g) La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Dirección de Tecnología y podrá llevarse a cabo sólo en dispositivos provistos por la organización, para tal fin.

Seguridad de Recursos Humanos

[ISO/IEC 27001:2005 A.8 A.8.1 Antes de la contratación Laboral]

El personal contratado para labores donde tenga acceso a información sensible o confidencial, deberá ser analizado bajo los parámetros específicos de seguridad definidos para el perfil, firmar los acuerdos de confidencialidad a los que haya lugar, y en sus contratos de trabajo deberá hacerse referencia expresa a sus responsabilidades en materia de seguridad.

[ISO/IEC 27001:2005 A.8 A.8.2 Durante la contratación Laboral]

Los accesos a la información se asignarán con base al cargo a desempeñar y sólo para sus funciones específicas.

Se le dotará de los activos necesarios para su actividad, y su uso deberá realizarse con base en las políticas de seguridad definidas.

Deberá realizarse una capacitación continuada en temas de seguridad de la información, con especial atención a aquellas personas que tengan acceso a datos de información de carácter contemplado en la ley.

[ISO/IEC 27001:2005 A.8 A.8.3 Terminación o cambio de contratación Laboral]

El retiro del personal deberá realizarse de una manera ordenada, con el fin de corroborar todas las acciones requeridas para garantizar que la información se regirá bajo los acuerdos de confidencialidad y responsabilidades definidas en el contrato laboral, con el fin que evitar los riesgos de robo, pérdida o corrupción de la información. Esto aplica a empleados, contratistas o terceras personas.

Es responsabilidad de Recursos Humanos el proceso de terminación general y trabaja junto con el director a cargo de la persona, para manejar los aspectos de seguridad de los procedimientos relevantes.

Se debe informar a los usuarios empleados, contratistas o terceras personas, de los cambios de personal y los acuerdos de operación.

Todos los usuarios empleados, contratistas y terceras personas, deben devolver los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo.

Se debe devolver dispositivos de cómputo móviles, teléfonos, tarjetas de crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

En casos donde el usuario empleado, contratista o tercera persona compra el equipo de la organización o utiliza su propio equipo, se debe garantizar la transferencia y eliminación del equipo, de la información de la organización antes del retiro del funcionario.

En los casos donde el usuario empleado, contratista o tercera persona tiene conocimiento que es importante para las operaciones actuales, esa información deberá ser debidamente documentada y transferida a la organización.

Los derechos de acceso en caso de terminación deberán ser eliminados en el momento que se considere justo para proteger la confidencialidad e integridad de la información. Si se trata de un cambio de cargo, se deben hacer los ajustes para el nuevo cargo, limitando lo

que no corresponda con las nuevas funciones para garantizar la segregación de funciones. Esta restricción incluye acceso físico y lógico, llaves, tarjetas de identificación, medios de procesamiento de información, suscripciones y retiro de cualquier documentación que identifique a la persona como miembro actual de la organización.

Si el usuario que se retira conoce las claves secretas para las cuentas aún activas, éstas se deben cambiar a la terminación del contrato o acuerdo.

Los derechos de acceso para los activos de información y los medios de procesamiento de información se deben retirar o reducir antes de la terminación, dependiendo de la evaluación de los factures de riesgo como:

a) si la terminación o cambio es iniciado por el usuario empleado, contratista o tercera persona, o por la gerencia y la razón de la terminación;
b) las responsabilidades actuales del usuario empleado, contratista o cualquier otro usuario;
c) el valor de los activos actualmente disponibles.

En casos de terminaciones iniciadas por la gerencia, los empleados, contratistas o terceros descontentos pueden corromper la información deliberadamente o sabotear los medios de procesamiento de la información. En caso de las personas que renuncian, pueden tratar de recolectar información para su uso futuro.

Control de acceso físico
[ISO/IEC 27001:2005 A.9.1]

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos

que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Protección y ubicación de los equipos
[ISO/IEC 27001:2005 A.9.2]

Los equipos que hacen parte de la infraestructura tecnológica de <<NOMBRE DE LA ORGANIZACIÓN>> tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los funcionarios y terceros, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de <<NOMBRE DE LA ORGANIZACIÓN>> no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

<<NOMBRE DE LA ORGANIZACIÓN>> mediante mecanismos adecuados monitoreará las condiciones ambientales de las zonas donde se encuentren los equipos (Centros de Cómputo).

Segregación de funciones
[ISO/IEC 27001:2005 A.10.1.3]

Toda tarea en la cual los funcionarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la organización.

En concordancia:

Todos los sistemas de disponibilidad crítica o media de la Organización, deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Deben estar claramente segregadas las funciones de soporte técnico, planificadores y operadores.

Protección contra software malicioso
[ISO/IEC 27001:2005 A.10.4]

<<NOMBRE DE LA ORGANIZACIÓN>> establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad de la Dirección de Tecnología autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

Así mismo, <<NOMBRE DE LA ORGANIZACIÓN>> define los siguientes lineamientos:
a) No está permitido:

La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por <<NOMBRE DE LA ORGANIZACIÓN>>.

Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

Copias de respaldo
[ISO/IEC 27001:2005 A.10.5]

<<NOMBRE DE LA ORGANIZACIÓN>> debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Dirección de Tecnología y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la organización, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

La Dirección de Tecnología establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Gestión de medios removibles
[ISO/IEC 27001:2005 A.10.7]

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información de <<NOMBRE DE LA ORGANIZACIÓN>>, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

La Dirección de Tecnología es responsable de implementar los controles necesarios para asegurar que en los sistemas de información de <<NOMBRE DE LA ORGANIZACIÓN>>. sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información de <<NOMBRE DE LA ORGANIZACIÓN>> que éste contiene.

Intercambio de información
[ISO/IEC 27001:2005 A.10.8]

<<NOMBRE DE LA ORGANIZACIÓN>> firmará acuerdos de confidencialidad con los funcionarios, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la organización. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de <<NOMBRE DE LA ORGANIZACIÓN>> es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

Control de acceso lógico
[ISO/IEC 27001:2005 A.11.1]

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de <<NOMBRE DE LA ORGANIZACIÓN>> debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Organización, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de <<NOMBRE DE LA ORGANIZACIÓN>> asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por la Dirección de Información y Tecnología de <<NOMBRE DE LA ORGANIZACIÓN>>.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros e implementada por la Dirección de Tecnología.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de <<NOMBRE DE LA ORGANIZACIÓN>>, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

Gestión de contraseñas de usuario
[ISO/IEC 27001:2005 A.11.2.3]

Todos los recursos de información críticos de <<NOMBRE DE LA ORGANIZACIÓN>> tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por la Dirección de Tecnología.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información de <<NOMBRE DE LA ORGANIZACIÓN>> debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password)

asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas, y garantizar que utiliza contraseñas con base a las condiciones de seguridad establecidas en forma y contenido, no usar contraseñas de fácil adivinación.

Escritorio y pantalla limpia
[ISO/IEC 27001:2005 A.11.2.4]

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios de <<NOMBRE DE LA ORGANIZACIÓN>> deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Segregación de redes
[ISO/IEC 27001:2005 A.11.4.5]

La plataforma tecnológica de <<NOMBRE DE LA ORGANIZACIÓN>> que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones de redes de huéspedes, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Dirección de Tecnología es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

<<NOMBRE DE LA ORGANIZACIÓN>> establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red

específicos hacia las plataformas donde operan los sistemas de información de la Organización.
Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Identificación de requerimientos de seguridad
[ISO/IEC 27001:2005 A.12.1.1]

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en <<NOMBRE DE LA ORGANIZACIÓN>>, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad de la Dirección de Tecnología y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre <<NOMBRE DE LA ORGANIZACIÓN>> y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información. Es responsabilidad de la Dirección de Tecnología garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y establecer estos aspectos con las obligaciones contractuales específicas.

ANEXO F PLANTILLA PROCEDIMIENTOS

Este procedimiento está diseñado para la empresa de estudio uno, la Litografía, ya que carecen de procedimientos de backup adecuados para el manejo de la información.

Aquí se describe la platilla para este procedimiento, pero este tendrá que tener el formato del encabezado, con la codificación definida y la hoja de control de distribución y cambios definidos en el procedimiento de control de documentos.

PROCEDIMIENTO DE BACKUPS

OBJETIVO

Realizar actividades de respaldo de la información, que permita garantizar la disponibilidad e integridad de la misma, en caso de sufrir algún incidente de seguridad que implique un proceso de recuperación.

RESPONSABLES

Secretaria: Para los backups del software administrativo.

Diseñador Jefe: Para los backups de la información de los diseños gráficos.

APLICACION

[ISO/IEC 27001:2005 A.10.5]

CONTENIDO

Para la creación de backups se realizaran copias de la información de la siguiente manera:
Para el software administrativo. Este software permite las actividades de facturación y cartera, en su programación original, el software está configurado para realizar una copia automática, cada vez que se cierra el programa. Esta copia está configurada para realizarse en otra partición del disco duro del equipo donde el software está instalado, por lo tanto esta copia diaria seguirá permaneciendo allí.

Semanalmente se realizará una copia del último backup, y se almacenará en un disco duro externo, que permanecerá bajo la custodia de la gerencia, en una estantería bajo llave, el disco duro estará identificado. Mensualmente se realizará una copia del último backup del mes en este mismo disco duro externo y adicional se hará una copia en un DVD que será almacenado en un lugar externo a la empresa que será la residencia de la gerente. Estos medios deberán estar identificados, el disco duro, en cada carpeta lógica tendrá la

marcación de la semana, mes y año a que corresponde y el DVD tendrá la marcación del mes y año que está almacenando.

Para llevar el registro del backup, se llevará un formato, que contenga, la fecha de backup, el nombre del archivo, el lugar de almacenamiento que le corresponde y firma de la persona que realiza el backup. <<Se debe relacionar aquí, el nombre y código del formato que se usará para llevar el registro.>>

Para los archivos de diseño. Los archivos de diseño, son el insumo inicial de creación que da origen al todo el proceso productivo de la empresa, los archivos creados se guardan en el disco duro del equipo en que fueron creados, pero adicional a esto se guardan al final del día una copia de los diseños realizados en un disco duro externo y semanalmente de este disco duro se hará backup en el computador de la gerencia que contiene un disco duro adicional para realizar estos backups. Para los diseños más complejos se hará un backup del mismo, quemándolo en un DVD y almacenándolo en la carpeta del cliente, con la muestra impresa del diseño y con las planchas que sirvieron para la impresión.

Igualmente para llevar el registro del backup, se llevará un formato, que contenga, la fecha de backup, el nombre del archivo y , el lugar de almacenamiento que le corresponde y firma de la persona que realiza el backup. <<Se debe relacionar aquí, el nombre y código del formato que se usará para llevar el registro.>>

PROCEDIMIENTO DE CONFIGURACIÓN DE COMPUTADOR

OBJETIVO

Generar un estándar de configuración de los equipos, que genere una homogeneidad que permita el control, que facilite la reconfiguración, la comunicación y la administración de la red.

RESPONSABLES

Personal técnico encargado de la configuración de los equipos.

APLICACIÓN

Protección contra software malicioso *[ISO/IEC 27001:2005 A.10.4]*
Control de acceso lógico *[ISO/IEC 27001:2005 A.11.1]*
Gestión de contraseñas de usuario *[ISO/IEC 27001:2005 A.11.2.3]*

CONTENIDO

Para la configuración de los computadores de la compañía, se seguirán los siguientes estándares:
Se debe diligenciar el formato definido para configuración de equipos. <<referenciar nombre y código de formato>>

Nombres de los equipos definidos de la siguiente manera:
XXXYYY### donde
XXX: iniciales que identifiquen la organización.
YYY: Caracteres que identifiquen el área de proceso que utiliza el equipo.
###: Número del último byte de la dirección ip del equipo.

Las direcciones ip de los equipos de red, se configurarán, teniendo en cuenta los siguientes estándares:

192.168.1.### dónde ### hará referencia según las siguiente denominación:

010: Gerencia: << Si hubiera más equipos de personas asistentes a gerencia irían consecutivamente entre 011 y 015>>
015: Secretaria: << Si hubiera más secretarias, la numeración sería consecutivamente entre 016 y 019>>
020: Diseñadores: <<Inicia entre 020 y 030>>

Ejemplo del Nombre y dirección IP de un equipo:

Nombre Equipo: LAGDIS020
Dirección IP: 192.168.1.020

El Usuario administrador del equipo, tendrá un nombre compuesto por:
adminXXX dónde XXX serán las iniciales definidas para identificar la organización en los nombres de los equipos.
Ejemplo: adminlag

Y la contraseña del administrador será la composición de la iniciales de la empresa + la dirección ip y el símbolo %. XXX###%
Ejemplo: lag020%

<<Esta es sólo una propuesta para estandarizar, pero podría la organización definir su propio estándar y documentarlo en este procedimiento.>>

El usuario administrador, no es el usuario de trabajo normal de cada computador, ya que tendría demasiados privilegios y es una condición insegura.

Se debe crear un usuario estándar, sin características de administrador para que sea el usuario de uso del equipo.
El usuario que es el Diseñador Jefe, será el encargado de conocer la nomenclatura de las contraseñas de administrador, en caso de que sea necesario su uso.

Antivirus
Los computadores tendrán el antivirus Avast versión Free instalado. <<Se recomienda evaluar la compra de una versión de un antivirus de pago>>

Firewall de Windows y Actualizaciones Automáticas
Se realizará un proceso de legalización del sistema operativo, con el fin de que estas características como Firewall de Windows, Windows Defender y las Actualizaciones, estén activadas para que se realicen periódicamente.

Programas de archivos comprimidos
Sólo en el computador del Diseñador Jefe, estará instalado el software 7Zip, con el fin de filtrar la información que se permite ser descomprimida en los equipos, debido a que esta es una frecuente modalidad de contagio de virus.

Ejecución Automática de USB y discos externos
Se debe deshabilitar la ejecución automática de dispositivos de almacenamiento externo.

PROCEDIMIENTO DE USO DE DISPOSITIVOS EXTERNOS USB Y DESCARGA DE ARCHIVOS DEL CORREO ELECTRÓNICO

OBJETIVO
Generar hábitos preventivos en los usuarios, que permitan ejercer un control en las principales fuentes de contagio de virus informáticos.

RESPONSABLES

Usuarios de los equipos

APLICACIÓN

Protección contra software malicioso *[ISO/IEC 27001:2005 A.10.4]*

Gestión de medios removibles *[ISO/IEC 27001:2005 A.10.7]*

CONTENIDO

El uso de dispositivos removibles en el negocio de la litografía, es necesario debido al constante intercambio de archivos entre el cliente y la empresa, por lo tanto es muy importante, prevenir el contagio de virus, a través de ciertas prácticas al usar estos dispositivos.

1. Siempre se debe revisar el dispositivo con el antivirus, antes de ejecutar cualquier archivo de su interior.
2. Los computadores estarán configurados para no hacer ejecuciones automáticas, sin embargo si esto ocurriese, cancele de inmediato esta ejecución y vuelva al punto 1.
3. Evite la tentación de abrir archivos que le parezcan muy llamativos, generalmente esto es lo que busca un archivo malicioso para atraer a su víctima.
4. Sospeche de archivos que tengan doble extensión (.exe.pdf) o extensiones .exe
5. Si descubre que ha sido contagiado por algún virus, repórtelo inmediatamente a su técnico y aísle el equipo, para evitar el contagio de otros equipos de la red.
6. Cada que use un dispositivo removible de origen externo, se debe diligenciar el formato de uso de dispositivos removibles, ingresando la fecha, origen del dispositivo, archivo usado y responsable de uso. <<Indicar nombre y código del formato a usar, ver anexo de registros.>>

Al recibir archivos por correo electrónico:

1. Verifique con cuidado la dirección electrónica del remitente, si tiene dudas llámele o escríbale un correo para comprobar si le han enviado este mensaje intencionalmente.
2. Verifique la ortografía del remitente, muchas veces simulan direcciones electrónicas similares, por ejemplo, para suplantar a dhl pueden usar dgl que puede pasar desapercibido en un usuario que no tome precauciones.

3. Los asuntos muy llamativos, suelen ser sospechosos, ejemplos, denuncias, envíos por transportadora, información importante, fotos, mira mi foto, estos se usan para llamar la atención de la víctima.
4. Si encuentra un link indicando que de click, verifique al pararse sobre él sin presionarlo, que la ayuda de contexto que sale, indique la misma dirección que dice el link, de lo contrario, es un link falso, que puede llevar a un lugar malicioso.
5. Los archivos adjuntos que vengan con formato .zip, pueden contener archivos maliciosos en su interior. Verifique con el remitente si lo está enviando.
6. Los archivos extensión .exe pueden ser archivos dañinos, no los ejecute sin preguntar al remitente o técnico de qué se trata.
7. Los archivos con doble extensión .exe.pdf, .exe.zip, generalmente son archivos potencialmente peligrosos, que pueden contener con una alta probabilidad software malicioso, no los ejecute, repórtelos a su técnico o escriba al remitente.

MODELO DE CLÁUSULA DE CONFIDENCIALIDAD (Ucelay, 2013)

Este modelo se presenta como una orientación que sirve de guía, que deberá ser adaptada en cada contrato según el tipo de organización, contrato con empleado o proveedor, incluso se recomienda su revisión por un abogado, antes de la firma del contrato.

Tanto durante la vigencia como con posterioridad a la terminación del presente contrato, las partes preservarán la más estricta confidencialidad acerca de TODA la información y documentación relativa a la contraparte y, en particular (de manera no exhaustiva): sobre sus actividades, clientes, planes de negocio, proyectos, material formativo, Know How, herramientas de trabajo de la que cada una haya tenido conocimiento en virtud de la presente relación profesional o de la que puedan tener conocimiento de otro modo o que, por su naturaleza sea claramente confidencial.

Ambas partes reconocen que la información y documentación recibida en cualquier tipo de formato (digital o analógico etc.) por parte de la otra o a la que tenga acceso por ser necesario para prestar el servicio objeto del contrato que mantienen para la evaluación de los sistemas y soluciones, o tecnologías es de carácter sensible y altamente confidencial toda ella.

Ninguna de las partes divulgará información confidencial alguna a ninguna persona o entidad ajena a este contrato salvo autorización expresa y por escrito, reflejada en medio fehaciente, de la contraparte. Así mismo, dicha información solamente podrá ser tratada en cada una de las empresas firmantes por los cargos de nivel igual o superior al de los firmantes del contrato y, en este caso, sólo a aquellos que necesiten conocerla para el desempeño de sus funciones a efectos de la prestación del servicio objeto del contrato. Ambas partes accederán a la información confidencial con las medidas de seguridad que, al efecto, pueda establecer y definir la contraparte, que se podrán incorporar al presente contrato como un Anexo y que tendrán el carácter de instrucciones vinculantes,

A los efectos de la presente cláusula, se entenderá por información confidencial toda la información de confianza revelada o transmitida con seguridad por el CLIENTE por su importancia estratégica, relevancia o carácter sensible (ya sea por escrito, verbalmente o por cualquier otro medio, tanto directa como indirectamente) o de la que ambas partes puedan tener conocimiento por cualquier otro modo, ya sea con anterioridad o con posterioridad a la fecha de comienzo de la relación de profesional, incluidos a título meramente enunciativo y no limitativo: cualquier información, materiales o documentos

relacionados con los empleados, productos, metodología, procesos, planes o intenciones, información de productos, de Know How, presentaciones, informes, documentación, bases de datos informáticas, materiales de formación, invenciones, diseños, descubrimientos y las patentes, copyrights, secretos comerciales y otros derechos de propiedad intelectual e industrial, fórmulas de negocio, conversaciones, oportunidades de mercado y asuntos comerciales o propios de la organización empresarial, o de sus agrupadas o asociadas, o de sus clientes u otros contactos profesionales.

Sin perjuicio de lo anterior, no se considerará información confidencial aquella sobre la que la contraparte pudiera claramente demostrar que:

Sea o pase a ser del dominio público por acción u omisión ajena a la otra parte; o era accesible al público en el momento de haberle sido revelada, o hubiera adquirido tal condición después de dicha revelación; ó

1.- Obrara en poder legítimo de la parte antes de su divulgación por la contraparte y no haya sido obtenida de la parte ni directa ni indirectamente; ó
2.- Hubiera sido independientemente desarrollada por la parte, sin basarse en información confidencial de la contraparte; ó
3.- Sea revelada legítimamente a la parte por la contraparte sin restricciones en cuanto a su divulgación; ó
4.- Mediante previo consentimiento de la contraparte para la divulgación de la misma; ó
5.- Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, la contraparte notificará a la parte tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información
6.- En todo caso, tampoco se considera como información confidencial la referida a: ….
Cualesquiera otras que la contraparte califique como no confidenciales en el curso de las relaciones comerciales entre ambas empresas.
7.- Ambas partes tomarán cuantas medidas estén a su alcance para hacer que sus empleados, consultores y asociados queden vinculados por los términos y condiciones del presente contrato y por consiguiente de prestación de servicios.

De igual forma, ambas partes adoptarán, respecto a la información objeto de este contrato, las mismas medidas de seguridad que adoptarían normalmente para sí mismas respecto a su propia información confidencial acerca de la metodología y/o tecnología desarrollada evitando en la medida de lo posible cualquier tipo de pérdida, robo o sustracción.

En caso de que la información resulte revelada o divulgada o utilizada por cualquiera de las partes, de forma distinta al objeto de este contrato, ya sea de forma dolosa o por mera negligencia, habrán de indemnizar a la otra por los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que, en su caso, puedan corresponder a este último.

Las partes se obligan a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente contrato en el supuesto de que cese la relación entre las partes por cualquier motivo.

Esta obligación de confidencialidad subsistirá a la revocación, resolución o expiración del presente Contrato.

ANEXO G PLANTILLA DE REGISTROS

Los formatos de registros, deben llevar el encabezado y la codificación definida para ellos en el documento del procedimiento de control de documentos. A continuación muestran estructuras de los formatos, cuándo los formatos son diligenciados, estos se convierten en registros, que permiten evidenciar la ejecución y seguimiento de las actividades propuestas en el sistema de gestión.

FORMATO PARA REGISTRO DE BACKUPS

Fecha de Backup	Nombre del Archivo	Lugar de almacenamiento	Firma Responsable

FORMATO PARA REGISTRO DE BACKUPS

ITEM	DESCRIPCIÓN	OBSERVACIONES
NOMBRE EQUIPO		
SERIAL		
DIRECCIÓN IP		
FECHA COMPRA:		
FECHA INSTALACIÓN:		
USUARIO ADMINISTRADOR:		
CONTRASEÑA ADMINISTRADOR:		
AREA ASIGNADO		
SISTEMA OPERATIVO		
SW OFIMÁTICO		
RAM		
PROCESADOR		
MONITOR		
USUARIO AUTORIZADO		
PROGRAMAS INSTALADOS		

IMPRESORAS INSTALADAS		

FORMATO PARA CONTROL DISPOSITIVOS EXTERNOS

Fecha Uso	Origen – Propietario	Archivo usado	Responsable Uso

ANEXO H INCIDENTES DE SEGURIDAD SUFRIDOS POR LAS PYMES CASO DE ESTUDIO.

LITOGRAFIA	
INCIDENTE	**IMPACTO**
Ataques por Virus	Pérdida de información de archivos de diseños para clientes. Archivos que no abren.
	Equipos que funcionan muy lento y afectan el desempeño de las actividades.
Discos duros Dañados	Pérdida de información de archivos de diseños para clientes. Se pierde toda posibilidad de usar nuevamente esta información, incurriendo en molestias para el cliente, nuevo diseño de la necesidad, retraso en los tiempos de entrega.
Correos electrónicos con contenido malicioso y phising	Correos que traen archivos adjuntos que al ejecutarse no muestran nada, pero que luego de esto los computadores no tienen el desempeño deseado y se abren múltiples ventanas de internet, o trabajan muy lento.
	Correos que solicitan información de actualización bancaria para robo de información. Un usuario ingresó sus datos y tuvo un robo de $300.000 en su cuenta de banco.
	Correos que dicen que se ha ganado un boleto de lotería que no se compró. El usuario emocionado pidió ayuda y se logró evitar el engaño.
Programa contable se desprogramó su impresión de facturas.	No se cuenta con soporte del proveedor ya que esta versión del software ya fué descontinuada y la organización no se actualizó. Por lo tanto estuvieron casi un año realizando facturación por el programa pero repitiéndola manualmente para entregarla al

	cliente, luego se encontró con la ayuda de un ingeniero externo la manera de imprimir nuevamente.
Los equipos de cómputo no cuentan con software licenciado ni para el Sistema Operativo, ni para los programas usados.	Hay permanente incertidumbre, cuando en el sector hay controles por las entidades encargadas, una multa por esto podría significar el cierre de la empresa, ya que no tiene los recursos económicos para cubrirla.

HOTEL	
INCIDENTE	**IMPACTO**
Ataques por Virus	Archivos de Office que no se pueden abrir. Equipo secuestrado con virus cryptográfico. Equipo lento en su desempeño. Equipo que abre múltiples pop-ups y no se puede acceder a las aplicaciones web. Red lenta por saturación de tráfico en general impactando el desempeño de todos los equipos de la red, incluso generando denegación de servicio.
Correos electrónicos con contenido malicioso y phising	A través de un correo que llega por contacto del sitio web, llegan correos de phising a Gerencia, Mercadeo y Ventas, Contraloría y Recepción, estos correos con frecuencia usan información de entrega de mercancía, recibos de pago, demandas judiciales, etc, que hacen que estos funcionarios estén permanentemente en riesgo, ya que los títulos tienen que ver con sus funciones, y con frecuencia se contagian de virus y troyanos.
Archivos pst dañados	Se pierde la información histórica de comunicaciones importantes del usuario.
Archivos de la red borrados o dañados accidentalmente.	Se han recuperado en su mayoría con Backups de la oficina central. Algunas veces no se logra una recuperación exitosa.

Equipos que no encienden.	Descargas eléctricas que causan daños en Board del equipo, generando días de no disponibilidad del equipo para el usuario.
Errores en conexiones eléctricas	Error de conexión mezclando fase y neutro de la energía regulada y la normal, ocasionando retornos de hasta 100V generando alarmas y caidas de los equipos activos de la red.
Ataques IP a planta PBX	Extensiones de habitaciones sonando con frecuencia sin interloculor, causando incomodidad y disgusto en los clientes, tres días de ataque hasta que fue controlado.
Funcionarios que se retiran definitivamente de la empresa.	Estos funcionarios, han borrado toda la información de sus computadoras, causando problemas en algunos procesos que dependían de esta información, como recetas estándar en cocina, o procedimientos de seguridad.

ANEXO I PLANTILLA DE CARTA DE COMPROMISO DE LA DIRECCIÓN

COMPROMISO DE LA DIRECCIÓN SGSI

La Gerencia General de <<NOMBRE DE LA ORGANIZACIÓN>> manifiesta a través de éste documento su compromiso con el SGSI, a través de las siguientes acciones:

- Tener disponibilidad de recurso humano para el proyecto, incluyendo un líder por parte de la organización, que tenga toma de decisión.
- Disponer de recursos necesarios para el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, su mantenimiento y su mejora continua.
- Formulando la política del SGSI y promoviendo su cumplimiento al interior de la organización.
- Disposición para participar en cada una de las actividades del proyecto y aplicar las recomendaciones en beneficio del mismo.
- Velar por el cumplimiento de los objetivos y planes del SGSI.
- Promoviendo actividades de mejora continua y apoyando al Representante de Seguridad para liderar los procesos del SGSI.
- Velando por que se realicen las auditorías internas del SGSI.
- Decidiendo los criterios de aceptación de riesgos y los niveles aceptables de riesgos.
- Apoyando las capacitaciones que permitan que el personal sea conciencienciado respecto a las actividades de seguridad de la información.

Se firma en _____ a los ___ días, del mes de _____ del año ____ por

_____

Nombre y Firma

Gerente General

ANEXO J PLANTILLA PARA PROCEDIMIENTO DE CONTROL DE DOCUMENTOS

LISTA DE DISTRIBUCIÓN			
Área	**Responsable**	**Firma**	**Fecha**

CONTROL DE CAMBIOS

Fecha revisión	*Versión del documento*	*Cambio*	*Por qué*

REVISÓ	**APROBÓ**

OBJETIVO

Controlar, aprobar, revisar, conservar y actualizar los documentos y registros (internos y externos) del Sistema de Gestión de <<NOMBRE ORGANIZACIÓN>>, para asegurar la eficacia de sus procesos.

RESPONSABLES

<<Personas que realizan el procedimiento>>.

APLICACION

<< Ítem de la norma o control al que se apunta con este procedimiento>>

CONTENIDO

Creación y modificación de documentos.

- Cuando se identifica la necesidad de elaborar o actualizar un documento dentro del Sistema de Gestión, se informa al jefe del proceso quien es el encargado de transmitir esta necesidad al responsable de seguridad del sistema de gestión.
- El responsable de seguridad analiza y evalúa con el jefe del proceso la justificación para la creación o modificación del documento y establece las bases y responsabilidades para la elaboración del mismo.
- Una vez elaborado según los requerimientos de este procedimiento (verificar que incluya encabezado, esquema general, etc.) el responsable de seguridad le asigna el código correspondiente y diligencia las tablas de control de cambios (se registra las razones por las cuales se modifica el documento) y lista de distribución (personas a las cuales se entregara copia física del documento).
- El documento es revisado y aprobado mediante la firma del responsable de seguridad y la gerencia general en la primera página.
- El responsable de seguridad actualiza la lista maestra de documentos.
- Las copias de los documentos se entrega según la lista de distribución en documentos electrónicos para quienes tienen acceso a un computador y en documentos físicos para el resto del personal, en cuyo caso se hace firmar la lista de distribución por parte de quien recibe el documento.
- De todos los documentos se tiene una copia física original en oficina de sistemas (la cual tendrá las firmas de revisión, aprobación y recepción de documentos) y una copia electrónica en el PC de sistemas, cada proceso tiene una carpeta en la cual

tiene una copia actualizada de los documentos que le competen directamente y que son entregados por el responsable de seguridad.

- En la carpeta de red \\<<definir ruta>> hay acceso a los documentos que cada proceso maneja y allí se encuentran en red los formatos, procedimientos, programas y registros que conforman el programa, cada semana se realiza la copia de la carpeta del Sistema de Gestión en <<Definir pc o disco extraíble o procedimiento de backups>> como backup en caso de algún incidente.
- El responsable de seguridad es el encargado de identificar y desechar los documentos obsoletos inmediatamente se publique la nueva versión, exceptuando aquellos de manejo especial por exigencias legales.
- El jefe de cada proceso evalúa la necesidad de aplicar algún documento externo que tenga incidencia en la seguridad del sistema de gestión y lo notifica al responsable de seguridad para adquirirlo y registrarlo en el Listado Maestro de Documentos y Registros. Cada dueño de proceso es responsable de notificar la actualización de los documentos externos al responsable de seguridad.
- Los registros son controlados en el Listado Maestro de Documentos y Registros. En este formato se define el tipo de registro y lugar de almacenamiento. En la casilla de almacenamiento se hace un comentario que detalla el Acceso (abierto o restringido), Tiempo de Conservación y Disposición.

INSTRUCCIONES PARA ELABORACIÓN DE DOCUMENTOS

La base documental del Sistema de Gestión de Seguridad de la Información, está conformada por los siguientes niveles:

- **Políticas (PO)**: Son líneas generales de actuación de la organización, en una declaración que estará firmada por la dirección y que será de aplicación según el alcance definido del Sistema de Gestión.

- **Procedimientos (PR)**: Son documentos que definen y describen de forma detallada los procesos o actividades de la organización y aseguran el buen desarrollo y funcionamiento del Sistema de Gestión de Seguridad de la Información. Este documento contiene: encabezado, lista de distribución, control de cambios, firma de revisión y aprobación, objetivo, responsable, normas asociadas, contenido y documentos anexos.
- **Formatos (FR) y anexos (AX):** Son los documentos de soporte y ayuda a los procedimientos, los cuales son de libre configuración a excepción del encabezado.

Permite generar una estructura que sirva para el ingreso de información que se considerará como registro.

- **Registros:** Son el resultado de diligenciar los formatos, con los que se demuestra el cumplimiento legal y las especificaciones del Sistema de Gestión, algunos podrían ser de una configuración específica según su origen o según la ley.

- **Documentos externos:** Existen documentos y registros de origen externo que son controlados pero mantienen su estructura documental original.

Codificación: se realiza de la siguiente manera:

- Primero se coloca el código del tipo de documento (PO, PR, FR, AX).
- Luego se escribe la sigla del proceso al que aplica: <<En este caso las iniciales identifican al proceso de la organización al que corresponde el documento, aquí se ponen los del hotel caso de estudio>>
    - RS: Responsable de Seguridad
    - DG: Directrices gerenciales
    - GA: Gestión administrativa
    - SI: Sistemas de ingeniería
    - RM: Room management
    - AB: Alimentos y bebidas
    - FO: Front Office
- Finalmente se escribe un número consecutivo de tres cifras el cual inicia en 001 para cada proceso.

Encabezado: se realiza según la siguiente plantilla:

<table>
<tr><td rowspan="2">LOGO DE LA EMPRESA</td><td rowspan="2">NOMBRE DEL PROCEDIMIENTO</td><td>Versión: 0</td></tr>
<tr><td>Fecha de entrada en vigencia: Febrero 08 de 2015</td></tr>
<tr><td>PR-RS-001 <<CODIFICACIÓN>></td><td>Página 147 de 147</td></tr>
</table>