ELABORACIÓN DEL PLAN DE IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2005 EN UNA EMPRESA DEL SECTOR RETAIL

ANDRÉS AUGUSTO JÁCOME LOBO

UNIVERSITAT OBERTA DE CATALUNYA
MASTER EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES
BOGOTÁ - COLOMBIA
2014

ELABORACIÓN DEL PLAN DE IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001:2005 EN UNA EMPRESA DEL SECTOR RETAIL

ANDRÉS AUGUSTO JÁCOME LOBO

Este trabajo es presentado como requisito para optar al título de Master en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Tutor

ANTONIO JOSE SEGOVIA HENARES

UNIVERSITAT OBERTA DE CATALUNYA

MASTER EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

BOGOTÁ - COLOMBIA

2014

TABLA DE CONTENIDO

INTRODUCCIÓN 8
1. ORIGEN E HISTORIA DE LAS NORMAS ISO/IEC 27001 y 27002 9
2. CONTEXTUALIZACIÓN 10
2.1. Descripción General de la empresa 10
2.2. Organización de la empresa 11
2.3. Procesos y organización de Tecnología 11
2.4. Organización de Seguridad de la información 13
2.5. Recursos tecnológicos 14
2.6. Principales aplicaciones y sistemas de información 19
2.7. Otros procesos de negocio 19
3. ALCANCE Y OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN 22
4. ANÁLISIS DIFERENCIAL 23
5. ESQUEMA DOCUMENTAL DEL SGSI 27
5.1. Tipos de documentos 27
5.2. Control de versiones 28
5.3. Codificación de documentos 28
6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 29
7. ROLES Y RESPONSABILIDADES 30
8. PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN 31
9. AUDITORÍAS INTERNAS DEL SGSI 32
9.1. Planificación de las auditorías 32
9.2. Metodología de revisión de los controles y requerimientos 34
9.3. Informe de auditoría 36
9.4. Requisitos para conformar el equipo de auditoría Interna 36
10. METODOLOGÍA DE ANÁLISIS DE RIESGOS 38
10.1. Cómo identificar activos de información 39
10.2. Cómo valorar activos de información 41
10.3. Cómo clasificar activos de información 43
10.4. Identificación de Amenazas 44
10.5. Valoración de Amenazas (Frecuencia e Impacto) 45
10.6. Determinación del Riesgo Inherente 46
10.7. Determinación del Riesgo Residual 48
10.8. Aceptación del Riesgo 48
11. DECLARACIÓN DE APLICABILIDAD 49
12. GESTIÓN DE INDICADORES 50
13. PLAN DE TRATAMIENTO DE RIESGOS 51
14. INFORME DE AUDITORÍA INTERNA DE CUMPLIMIENTO 56
14.1. Introducción 56
14.2. Metodología empleada 57
14.3. Resultados de la evaluación del nivel de madurez de seguridad de la

información en la empresa 58
14.4. Listado detallado de los hallazgos 60
14.5. Conclusiones y recomendaciones de la auditoria interna 63
14.6. Anexos del informe de auditoria interna 64
CONCLUSIONES 65
BIBLIOGRAFÍA 66

ÍNDICE DE ANEXOS

ANEXO 1. ANÁLISIS DIFERENCIAL RESPECTO A ISO 27001:2005 67
ANEXO 2. MODELO DE SEGURIDAD DE LA INFORMACIÓN 68
ANEXO 3. DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE REVISIÓN DEL SGSI POR LA DIRECCIÓN 69
ANEXO 4. CRONOGRAMA DE ACTIVIDADES DE AUDITORÍA INTERNA DEL SGSI 70
ANEXO 5. LISTA DE VERIFICACIÓN DE ACTIVIDADES DEL ANÁLISIS DE RIESGOS DE UN PROCESO 71
ANEXO 6. CRITERIOS DE VALORACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 72
ANEXO 7. MATRIZ DE ACTIVOS DE INFORMACIÓN 73
ANEXO 8. DECLARACIÓN DE APLICABILIDAD (SOA) 74
ANEXO 9. MÉTRICAS E INDICADORES DEL SGSI 75
ANEXO 10. DOCUMENTO F-GSI-001 DILIGENCIADO PARA EL ANÁLISIS DE RIESGOS REALIZADO EN EL PRIMER SEMESTRE DE 2014 76
ANEXO 11. DOCUMENTO R-GSI-001 DILIGENCIADO PARA LOS PROCESOS DENTRO DEL ALCANCE DEL SGSI EN EL PRIMER SEMESTRE DE 2014 77
ANEXO 12. EJEMPLO DE APLICACIÓN DE MÉTODO DE ANÁLISIS DE RIESGOS 78
ANEXO 13. CRONOGRAMA DETALLADO DE IMPLEMENTACIÓN DE PROYECTOS DE SEGURIDAD 84
ANEXO 14. ANÁLISIS DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN RESPECTO A ISO 27002 85

ÍNDICE DE FIGURAS

Figura 1. Estructura organizacional de la empresa 11
Figura 2. Esquema de interconexión de red de las sedes de la empresa 15
Figura 3. Topología de red y principales recursos tecnológicos – Sede Principal..... 16
Figura 4. Topología de red y principales recursos tecnológicos – Sede Regional..... 18
Figura 5. Estado general de implementación de controles del anexo A - ISO 27001. 25
Figura 6. Diagrama de radar implementación controles el Anexo A - ISO 27001..... 26
Figura 7. Codificación de documentos para el esquema documental 28
Figura 8. Etapas y actividades del método de análisis de riesgos 38
Figura 9. Dependencia entre activos superiores e inferiores..... 41
Figura 10. Diagrama de barras de la mejora causada en dominios ISO 27002 por proyectos de SI 53
Figura 11. Diagrama de radar de la mejora causada por proyectos en la implementación de dominios ISO 27002 54
Figura 12. Diagrama de radar del nivel de madurez actual respecto al esperado (en porcentaje %) 59
Figura 13. Nivel de madurez actual respecto al esperado (en escala CMM) 60

ÍNDICE DE TABLAS

Tabla 1. Relación de los principales sistemas de información de la empresa..... 19
Tabla 2. Marco utilizado para el análisis diferencial respecto a ISO 27001..... 23
Tabla 3. Estado de implementación de requisitos generales de la ISO 27001..... 24
Tabla 4. Estado general de implementación ISO 27001 por dominios..... 25
Tabla 5. Objetivos, controles y requisitos auditados..... 33
Tabla 6. Escala de medición de madurez de seguridad..... 35
Tabla 7. Clasificación de impacto para los hallazgos de auditoría Interna del SGSI . 35
Tabla 8. Campos que componen la matriz de activos de información..... 40
Tabla 9. Relación entre valores Cualitativos y Cuantitativos de activos 41
Tabla 10. Relación entre el valor del activo y su clasificación..... 43
Tabla 11. Criterios para calificar la frecuencia de ocurrencia de una amenaza..... 45
Tabla 12. Criterios para la evaluación de la degradación del activo..... 45
Tabla 13. Determinación cualitativa del impacto 46
Tabla 14. Estimación cualitativa del riesgo 47
Tabla 15. Estimación cuantitativa del riesgo 47
Tabla 16. Criterios para determinar efectividad de los controles..... 48
Tabla 17. Marco utilizado para la declaración de aplicabilidad (SOA) 49
Tabla 18. Mejora en la implementación de requisitos generales de la ISO 27001 por los proyectos..... 52
Tabla 19. Mejora en la implementación de dominios ISO 27001 por los proyectos .. 53
Tabla 20. Clasificación de hallazgos de auditoría..... 56
Tabla 21. Resultado de la evaluación del nivel de madurez por dominios ISO 27002 58

INTRODUCCIÓN

Se presenta inicialmente una breve inducción a la norma ISO 27001 y una contextualización general de la empresa Tu Hogar con Estilo S.A., presentando entre otras, una descripción general del entorno empresarial, de su cultura organizacional, de los procesos de negocio y del estado de la seguridad de la información.

Una vez se ha establecido el contexto general de la empresa, en este trabajo se surten todas las etapas necesarias para establecer un sistema de seguridad de la información (SGSI) basado en la norma ISO 27001:2005, abordando inicialmente la definición del alcance y los objetivos trazados para el plan director de seguridad de la información en la empresa, continuando con la presentación de los resultados de un estudio de análisis diferencial en relación a los principales requerimientos, objetivos de control y controles establecidos en dicha norma, con el cual, se podrá conocer el estado inicial de la seguridad de la información en la empresa.

Adicionalmente, durante el presente trabajo se desarrolla el esquema documental requerido por el SGSI, incluyendo entre otras el documento maestro de política de seguridad de la información, la metodología de análisis de riesgos que será implantada, la declaración de aplicabilidad que permite conocer aquellos controles que la empresa ha definido como requeridos y aplicables en su SGSI y un esquema para la gestión de métricas e indicadores asociados a dichos controles. Adicionalmente se surten las etapas de identificación, valoración y clasificación de activos de información, con su correspondiente etapa de identificación y valoración de riesgos asociados, de acuerdo al método definido.

Posteriormente se aborda una propuesta de proyectos y planes de mejora para incrementar el nivel de madurez del SGSI en la empresa y se finaliza con una relación de los resultados del proceso de auditoría de cumplimiento a la empresa respecto a la norma ISO 27001, presentando los resultados y conclusiones generales del trabajo realizado.

1. ORIGEN E HISTORIA DE LAS NORMAS ISO/IEC 27001 y 27002

La ISO[1] (Organización Internacional de estándares) y la IEC[2] (Comisión Electrotécnica Internacional) son actualmente las principales organizaciones a nivel mundial para la estandarización de aspectos técnicos, de seguridad, entre otros. Dichas organizaciones, junto con otros organismos internacionales públicos o privados, participan en la realización de comités técnicos para establecer acuerdos y estándares en áreas específicas del conocimiento.

Las normas conocidas como ISO/IEC 27001 y 27002, que proporcionan un marco de gestión para la seguridad de la información aplicable por cualquier tipo de organización sin importar su naturaleza o tamaño, surgieron como resultado del Comité Técnico conjunto ISO/IEC JTC 1, llamado de las Tecnologías de la Información, subcomité 27 (SC 27), asociado con Técnicas de seguridad. Estas normas se encuentran basadas en la antiguamente denominada norma BS 7799, elaborada por la BSI[3] (Institución de estándares Británica) en 1995.

La BSI publicó su norma 7799 en dos partes, la primera conocida como BS 7799-1, se elaboró como una guía de buenas prácticas de seguridad de la información y no se encontraba enmarcada en un sistema de seguridad de la información ni se encontraba diseñada para ser una norma certificable. Posteriormente en 1998, la BSI publicó la segunda parte de su norma, conocida como BS 7799-2, en la cual definió los requisitos que permitirían obtener una certificación del sistema de seguridad de la información (SGSI) por parte de una entidad independiente.

Posteriormente, en el año 2000, la ISO adoptó la norma BS 7799-1 y la denominó ISO 17799, sin cambios representativos respecto a su predecesora de la BSI, y fue hasta el año 2005 donde la ISO adoptó y publicó la norma BS 7799-2 bajo el nombre de ISO 27001, revisando al mismo tiempo la norma ISO 17799 y renombrándola posteriormente como ISO 27002 en el año 2007.

En su versión de 2005, la norma ISO 27001 contenía 11 dominios, cobijando 33 objetivos de control y 133 controles, sin embargo en la última revisión, realizada el 25 de septiembre de 2013, se han establecido un total de 14 Dominios, abordando 35 objetivos de control y 114 Controles.

Dado que la última actualización de la norma es aún muy reciente, el presente trabajo se enfocará en los requisitos y controles establecidos en su versión anterior, dejando como precedente que las empresas certificadas en la versión de 2005 estarían en capacidad de ajustarse y optar por la certificación en su versión de 2013.

[1] De sus siglas en inglés: International Standards Organization
[2] De sus siglas en inglés: International Electrotechnical Commission
[3] De sus siglas en inglés: British Standards Institution

2. CONTEXTUALIZACIÓN

2.1. Descripción General de la empresa

La empresa escogida como objeto de este estudio es "Tu hogar con estilo S.A.[4]", perteneciente al sector Retail, específicamente dedicada a las ventas al detal de productos para el mejoramiento del hogar, incluyendo muebles, utensilios para cocina y baños, materiales para remodelación de pisos, paredes, puertas, ventanas, además de electrodomésticos, gasodomésticos, lencería para habitaciones y baños, productos para limpieza de cocinas, baños, entre otros.

La empresa, que cuenta actualmente con presencia en 5 países de Centroamérica y Sudamérica, dispone de varios canales de venta puestos a disposición de sus clientes, incluyendo los tradicionales almacenes, cuyas instalaciones físicas superan los 10 mil metros cuadrados de área cada uno, pero adicionalmente cuenta con canales de venta telefónicos y a través de su página web www.tuhogarconestilo.com[5]. Vale la pena resaltar que los clientes cuentan con la posibilidad de iniciar y terminar su compra en cualquier canal (compras multicanal), por ejemplo, si el cliente desea comprar algún producto del almacén, y no desea hacer largas filas en caja o si no desea cargar con su producto hasta su hogar, puede dejarlo chequeado y pagarlo ya sea por teléfono o por la página web, escogiendo la opción de despacho a domicilio el siguiente día hábil.

El lema de la empresa es "Mejor imposible", poniendo a disposición de sus clientes una garantía en los productos equivalente al doble de la que ofrecen sus competidores, permitiéndole convertirse en la empresa que ofrece los productos con mayor calidad y durabilidad del mercado.

La casa matriz de la empresa está ubicada en Costa Rica, y desde allí se coordina la operación de todos sus canales de venta (presenciales y no presenciales), y actualmente cuenta con 52 almacenes distribuidos entre Costa Rica, México, Panamá, Colombia y Brasil. Su principal meta para los próximos 5 años es llegar a 100 tiendas y expandir su comercio en otros 3 países de Sudamérica, lo que le debería permitir alcanzar el doble de sus ventas actuales. Para ello la empresa se mantienen en constante movimiento y expansión, siempre en la búsqueda de oportunidades para abrir nuevos almacenes con el formato actual y adicionalmente con miras de incursionar en nuevos formatos que le permitan acercarse a sus objetivos y metas, incluyendo a mediano plazo la incursión en el mercado de las ventas al por mayor de materiales para construcción y la prestación de servicios especializados de instalación, reparación, mantenimiento y construcción, que le permitan a sus clientes materializar sus ideas más fácilmente, ayudándolos a acercarse a lo que la empresa llama "El hogar de tus sueños".

[4] El nombre de la empresa proviene de la imaginación del autor de este trabajo y al momento de seleccionarlo no se encuentra asociado con una empresa real, ni con la empresa descrita en el presente documento.
[5] Este dominio se encuentra disponible al momento de la realización de este trabajo y no corresponde con un sitio web real.

2.2. Organización de la empresa

Como se puede observar en la figura 1, la empresa está liderada por un Presidente corporativo y un Presidente regional en cada uno de los países donde se encuentra ubicada. Se encuentra organizada en siete (7) grandes vicepresidencias, las cuales son: Operaciones, Comercial, Tecnología, Gestión Humana, Jurídica, Riesgo y Financiera, cada una de ellas con varias Gerencias, Direcciones y Jefaturas. Adicionalmente cuenta con un área de auditoría Interna en cada país, la cual reporta directamente de Presidencia.

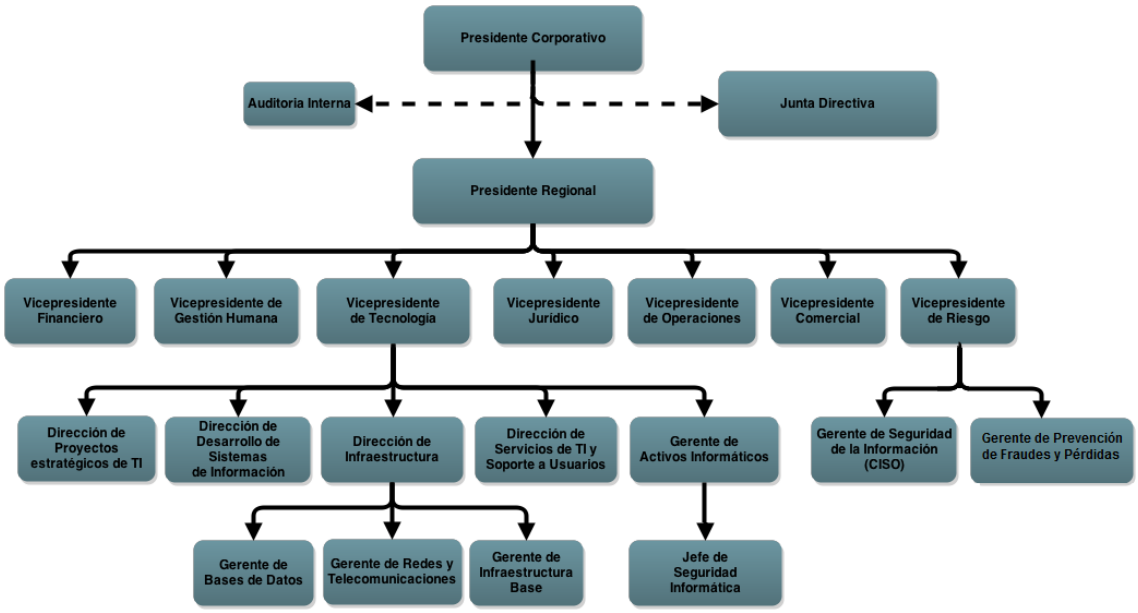


Figura 1. Estructura organizacional de la empresa

A nivel de recurso humano se habla de un total de más de seis mil (6.000) empleados directos y otros mil (1.000) tercerizados en modalidad de outsourcing distribuidos entre los diferentes países.

2.3. Procesos y organización de Tecnología

La empresa ha invertido una buena cantidad de recursos en el diseño, implementación, soporte y mantenimiento de su infraestructura tecnológica y en las instalaciones físicas que la resguardan, contando adicionalmente con personal idóneo interdisciplinario bajo la dirección de la Vicepresidencia de Tecnología. Sin embargo la empresa dentro de su política corporativa exige que toda esta infraestructura tecnológica y física requerida por el área de Tecnología no sea adquirida sino que sea subcontratada o arrendada mediante modalidades como el leasing tecnológico, llevando a que actualmente la empresa disponga de contratos con terceros estratégicos que prestan los servicios de hospedaje de servicios de internet, alquiler de servidores, alquiler de espacio de almacenamiento, alquiler de equipos de cómputo (portátiles y de escritorio), Seguridad perimetral administrada, servicio de mesa de ayuda y soporte a usuarios tercerizado, entre otras.

Todos los servicios de alquiler de servidores y alquiler de espacio de almacenamiento son contratados con un único proveedor, escogido mediante un proceso estricto de licitación pública, el cual ofrece a la empresa un servicio de Data Center administrado, garantizando la disponibilidad de los servicios en adecuados niveles de seguridad física y ambiental, de acuerdo a los niveles de servicio y condiciones pactadas contractualmente con la empresa.

La Vicepresidencia de Tecnología de cada regional cuenta con cuatro (4) Direcciones y una (1) Gerencia que dependen directamente del Vicepresidente de TI, cada una de ellas con funciones bien diferenciadas, las cuales se relacionan a continuación:

- Gerencia de Activos Informáticos: Es un área relativamente nueva y que se encuentra en crecimiento, sobre la cuál recaen responsabilidades directas relacionadas con la gestión de activos de hardware y software (licenciamiento), documentación de procesos de TI, gestión de presupuesto de inversión y gasto de TI y finalmente, sobre esta Gerencia recae la responsabilidad de administrar la función de Seguridad Informática de la empresa, la cual actualmente está en cabeza del Jefe de Seguridad Informática.

- Dirección de Infraestructura: se encarga de todo lo relacionado con instalación, pruebas y puesta en producción de servidores (Windows, Linux y AIX), Bases de Datos (SQL y Oracle) y lo relacionado con redes y telecomunicaciones. En esta Dirección se establece una relación directa con el proveedor de Data Center administrado y se vela por el cumplimiento del contrato relacionado. La disponibilidad de los servicios de TI es una responsabilidad que recae directamente sobre esta dirección.

- Dirección de Servicios de TI y Soporte a usuarios: Bajo esta dirección e encuentran las áreas encargadas de realizar las pruebas y transición de cambios sobre los sistemas de información de la empresa, estando segregadas bajo coordinaciones independientes que comparten la misma Jefatura. Adicionalmente en esta dirección se mantiene una relación directa con el tercero encargado de prestar el servicio de Mesa de ayuda y Soporte técnico en sitio, velando por el cumplimiento de los niveles de servicio pactados en el contrato.

- Dirección de Desarrollo de Sistemas de Información: En esta dirección se encargan de recibir los requerimientos de las diferentes áreas del negocio y de la Vicepresidencia de Tecnología, para materializarlos ya sea en nuevos aplicativos o en mejoras o correcciones sobre los aplicativos actualmente soportados. Vale la pena resaltar que no todas las aplicaciones y sistemas de información manejadas por el negocio están actualmente soportadas por la Dirección de desarrollo de Sistemas de Información y se encuentran soportadas directamente por proveedores externos administrados por cada área del negocio.

- Dirección de Proyectos estratégicos de TI: Esta dirección se encarga de coordinar los diferentes proyectos diseñados para el crecimiento de la empresa y que contienen un alto componente tecnológico o de sistemas de información. En algunos casos los nuevos sistemas de información son solicitados por medio de esta dirección y no pasan directamente desde el negocio hasta la Dirección de desarrollo de Sistemas de Información.

Como se puede ver en las diferentes áreas que componen la vicepresidencia de tecnología de la empresa, en general las responsabilidades asociadas con desarrollo, pruebas y producción se encuentran razonablemente segregadas de acuerdo a las buenas prácticas.

Como se comentó previamente, la gerencia de activos informáticos se encarga de documentar los procesos de la gerencia de TI, encontrando entre los principales los siguientes:

- Proceso de control de cambios: La empresa ha implementado recientemente este proceso, que se basa en la premisa de que cualquier cambio de alto impacto debe ser validado por el comité de control de cambios antes de pasar a producción. Existen otros cambios, llamados de alta prioridad, que solamente son comunicados al comité de cambios antes de su paso a producción, y existen otros cambios llamados pre-aprobados, que son llevados una única vez al comité y de ahí en adelante pueden ser ejecutados en ciertas condiciones sin pasar por dicho comité.

- Proceso de Gestión de Acceso Lógico: Este proceso lleva un buen tiempo en ejecución y permite concentrar la creación, modificación y eliminación de usuarios en la Jefatura de Seguridad Informática de la empresa. Vale la pena resaltar que a la fecha no todas las aplicaciones y sistemas de información de la empresa están centralizadas en esta área, por lo que se establecen anualmente planes de mejoramiento que incluyen la recepción de la gestión de accesos de nuevos sistemas. El área encargada de gestionar los accesos cuenta actualmente con cinco (5) operadores de acceso lógico y un (1) líder, todos pertenecientes a un tercero que provee este servicio a la empresa.

- Proceso de Gestión de eventos de seguridad informática: Es un proceso reciente que se encuentra en crecimiento y que permite validar con cierta periodicidad las acciones efectuadas sobre las bases de datos en producción, acciones efectuadas por administradores del dominio (Active Directory) y otros eventos como los reportados por la consola de antivirus. El proceso es ejecutado directamente por el Jefe de Seguridad Informática.

- Proceso de atención de incidentes y mesa de ayuda: La empresa cuenta con una mesa de ayuda con atención telefónica o por correo electrónico y se encarga de brindar el primer nivel de soporte, atención a incidentes, problemas o eventos asociados con la infraestructura tecnológica y los sistemas de información. Como se comentó anteriormente, la mesa de ayuda y el área de soporte técnico se encuentran tercerizados, contando con personal en sitio y con la mesa de ayuda a distancia.

2.4. Organización de Seguridad de la información

La seguridad de la información en la empresa es un tema reciente que ha venido cobrando fuerza gracias a las diferentes regulaciones que han venido adoptando los diferentes países en materia de protección de datos de carácter personal. Este tipo de regulaciones ha apalancado el interés de la empresa en desarrollar un SGSI y en fortalecer la seguridad de sus recursos informáticos. Sin embargo la empresa aún se encuentra en un proceso de concientización y crecimiento en torno a estos temas.

En la empresa, a pesar de que los procesos de seguridad de la información se encuentran en desarrollo y aún no cuentan con un nivel de madurez adecuado, ya se cuenta con las siguientes áreas y roles con responsabilidades formalmente establecidos en torno a la seguridad de la información:

- **Oficial de seguridad de la información**: Actualmente es el único integrante de lo que podría llegar a ser el área de Seguridad de la Información, y se encarga entre otras de diseñar, redactar y someter a aprobación las políticas de seguridad de la información, proponer el roadmap de maduración del SGSI, adicional a la identificación de activos críticos y sus riesgos relacionados, liderar la gestión de incidentes de seguridad de la información y coordinar los diferentes proyectos requeridos dentro de la implementación del SGSI.

- **Área de Seguridad Informática**: Cuenta actualmente con siete (7) personas, de las cuales seis (6) pertenecen al proveedor del servicio de acceso lógico y son liderados directamente por el Jefe de Seguridad Informática. Esta área es responsable de todas las labores relacionadas con el diseño, implantación y mantenimiento de controles y procedimientos asociados con seguridad de TI. Adicionalmente se tienen contratos con terceros para la gestión administrada de la consola de antivirus, la administración de la seguridad perimetral (Firewall UTM) y de otras herramientas y procesos como la gestión de seguridad de correo electrónico (Appliances para filtrado de virus y spam de correo) y la gestión de eventos de acceso a bases de datos del ambiente de producción por parte del personal de TI.

- **Gerencia de Prevención de fraudes y pérdidas**: Es el área encargada de diseñar, implementar y mantener los controles para la protección física de los activos e instalaciones de la empresa. Mantiene contratos con terceros para la prestación del servicio de vigilancia en sitio y video vigilancia remota.

- **Comité de Seguridad de la Información**: Se encuentra integrado por los principales involucrados en Seguridad, por la alta gerencia y por el área de riesgo. A grandes rasgos es el ente encargado de tomar las decisiones más relevantes en torno a seguridad de la información de la empresa.

2.5. Recursos tecnológicos

La empresa cuenta con equipos de cómputo, servidores, dispositivos de seguridad, equipos de infraestructura de red, bases de datos, entre otras, distribuidos en cada uno de los almacenes, sedes administrativas de la empresa y en los distintos data centers arrendados tanto a nivel central como regional para alojar los recursos que son considerados de mayor criticidad.

La topología de red que permite la interconexión de las distintas sedes de la empresa puede ser apreciada a grandes rasgos en la figura 2. En ella se observa que existe una sede principal, la cual está ubicada en Costa Rica y varias regionales, ubicadas en otros cuatro países (México, Panamá, Colombia y Brasil), todas ellas interconectadas mediante un proveedor de telecomunicaciones con presencia a nivel de Centro América y Sudamérica (ISP Internacional).

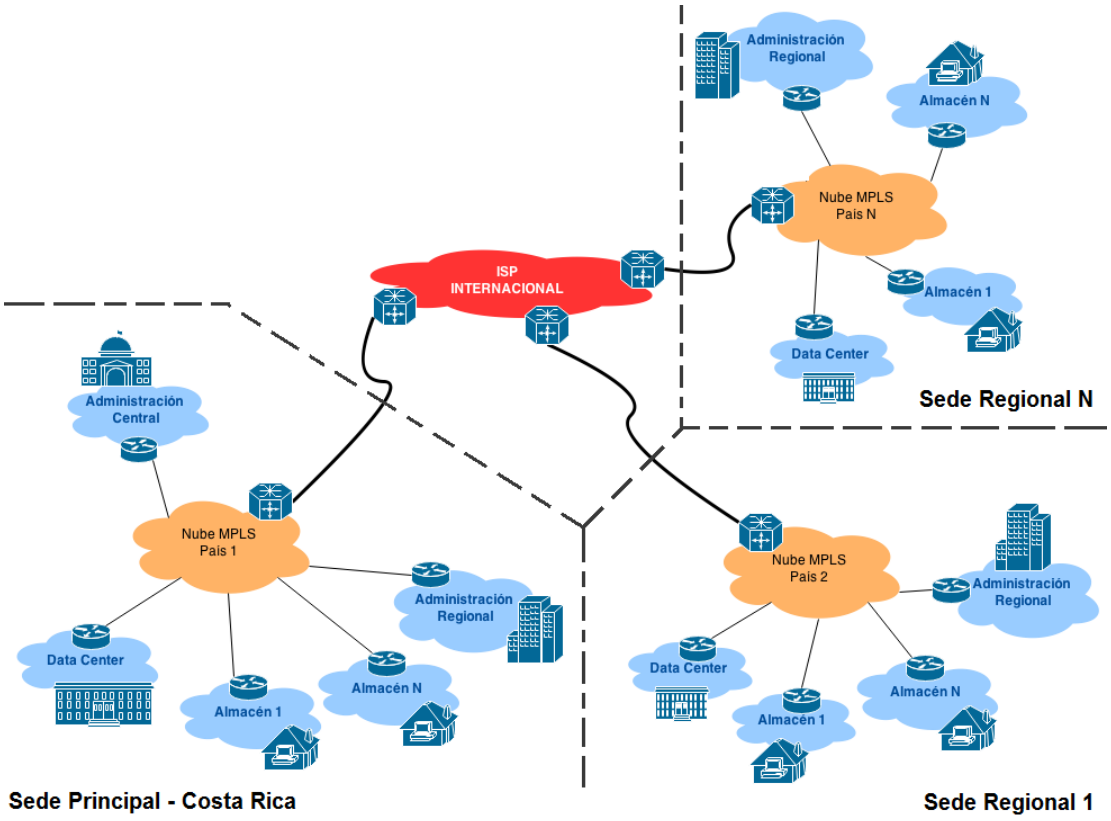


Figura 2. Esquema de interconexión de red de las sedes de la empresa

En cada una de las sedes, tanto la principal como las regionales se tienen contratados servicios de telecomunicaciones para la interconexión de almacenes, bodegas y sedes administrativas mediante canales dedicados conformando lo que se conoce como una nube MPLS. Así mismo, a cada una de dichas nubes se adiciona un enlace de mayor ancho de banda y niveles de disponibilidad, contratado con un proveedor de telecomunicaciones internacional, que permite la interconexión de los distintos países de manera que todos puedan acceder a los recursos administrados desde el nivel central (Costa Rica).

Adicionalmente, vale la pena resaltar que existen servicios de Data Center en cada una de las regionales, ya que algunos de los servicios tecnológicos requeridos para la operación deben ser manejados en cada regional, mientras que los servicios principales se encuentran alojados en el Data Center ubicado en Costa Rica (Data Center principal), incluyendo los recursos tecnológicos relacionados con el canal de Ventas por Internet, el sistema central de nómina, entre otros.

A continuación se muestran de forma muy general, los esquemas de red donde se relacionan los principales recursos informáticos que se encuentran alojados tanto en la sede principal, como en las distintas sedes regionales de la empresa (ver figuras 3 y 4 respectivamente).

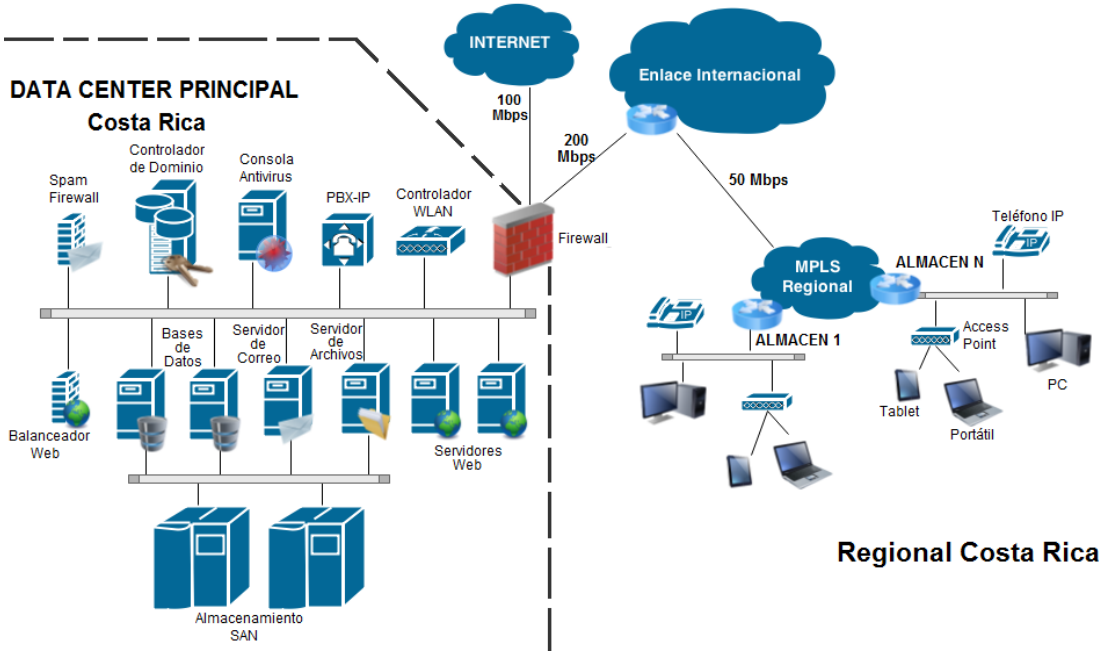


Figura 3. Topología de red y principales recursos tecnológicos – Sede Principal

En la figura 3 se puede apreciar la topología de red diseñada para el alojamiento de los principales servicios de red y sistemas de información en el data center principal contratado por la empresa. Vale la pena recalcar que a diferencia de las sedes regionales, los almacenes y sedes administrativas de Costa Rica no cuentan con un data center regional para acceder a algunos servicios, sino que deben acceder siempre al data center principal. A continuación se relacionan los principales recursos informáticos alojados en el data center de la sede principal:

- Para la seguridad perimetral se cuenta con un servicio administrado de Firewall UTM en alta disponibilidad con el tercero propietario del data center. Este servicio adicionalmente permite controlar las categorías y páginas web a las que los empleados pueden acceder de acuerdo a su rol en la empresa.

- Consola de Antivirus y Antispyware corporativo, que incluye adicionalmente productos para el control de dispositivos USB, control de virus en la navegación web, firewall de host y módulo de prevención de intrusiones de host. Esta consola presta sus servicios para la sede de Costa Rica.

- Dos (2) controladores de dominio, incluyendo servicios de directorio activo, DNS interno y DHCP para Costa Rica.

- Dos (2) Appliance para el filtrado de Virus de correo y SPAM, configurados en alta disponibilidad.

- Herramienta Software para el registro y posterior monitoreo de accesos en bases de datos.

- Dos (2) Appliance en alta disponibilidad para balanceo de servicios web.

- Dos (2) servidores virtualizados en alta disponibilidad para prestar el servicio de correo electrónico corporativo a toda la empresa.

- Un (1) servidor virtualizado que presta el servicio de almacenamiento de archivos para la regional de Costa Rica y adicionalmente para algunos procesos a nivel corporativo (todas las sedes).

- Diez (10) servidores físicos para el alojamiento de los servicios de la empresa. Estos servidores son el soporte físico para generar cada uno de los servidores virtualizados configurados.

- Treinta y dos (32) servidores virtualizados con rol de Web Server para las aplicaciones corporativas.

- Doce (12) servidores virtualizados con el rol de Base de Datos configurados en cluster, con almacenamiento en la SAN. Se manejan tanto bases de datos Oracle como SQL, de acuerdo a la aplicación que las utiliza.

- Dos (2) dispositivos SAN de cinco (5) Terabytes para el almacenamiento centralizado requerido en la empresa. Estas SAN dan soporte para el almacenamiento de las bases de datos, servidor de archivos y servidor de correo electrónico corporativo.

- Controlador inalámbrico para la sede de Costa Rica, que permite controlar y configurar remotamente cada uno de los Access Points ubicados en los almacenes de dicha sede.

- Planta telefónica PBX-IP para Costa rica.

Como se observa en la figura 4, cada sede regional cuenta con algunos servicios de manera local y debe acceder a otros en la sede principal (data center de Costa Rica) mediante el enlace internacional. A continuación se relacionan los principales servicios con los que cuenta una sede regional:

- Consola de Antivirus, configurada e forma independiente pero con los mismos servicios que la consola ubicada en Costa Rica.

- Dos (2) controladores de dominio, incluyendo servicios de directorio activo, DNS interno y DHCP.

- Dos (2) servidores físicos para el alojamiento de los servicios de la regional. Estos servidores son el soporte físico para generar cada uno de los servidores virtualizados configurados.

- Un (1) servidor virtualizado que presta el servicio de almacenamiento de archivos para la regional.

- Cuatro (4) servidores virtualizados con rol de Web Server para las aplicaciones alojadas en cada regional.

- Dos (2) servidores virtualizados con el rol de Base de Datos SQL configurados en cluster, con almacenamiento en la SAN.

- Un (1) dispositivos SAN de un (1) Terabyte para el almacenamiento centralizado requerido en la regional. Esta SAN da soporte para el almacenamiento de las bases de datos y para el servidor de archivos.

- Controlador inalámbrico, que permite controlar y configurar remotamente cada uno de los Access Points ubicados en los almacenes y sede administrativa de dicha regional.

- Planta telefónica PBX-IP para brindar servicio de telefonía a la regional.

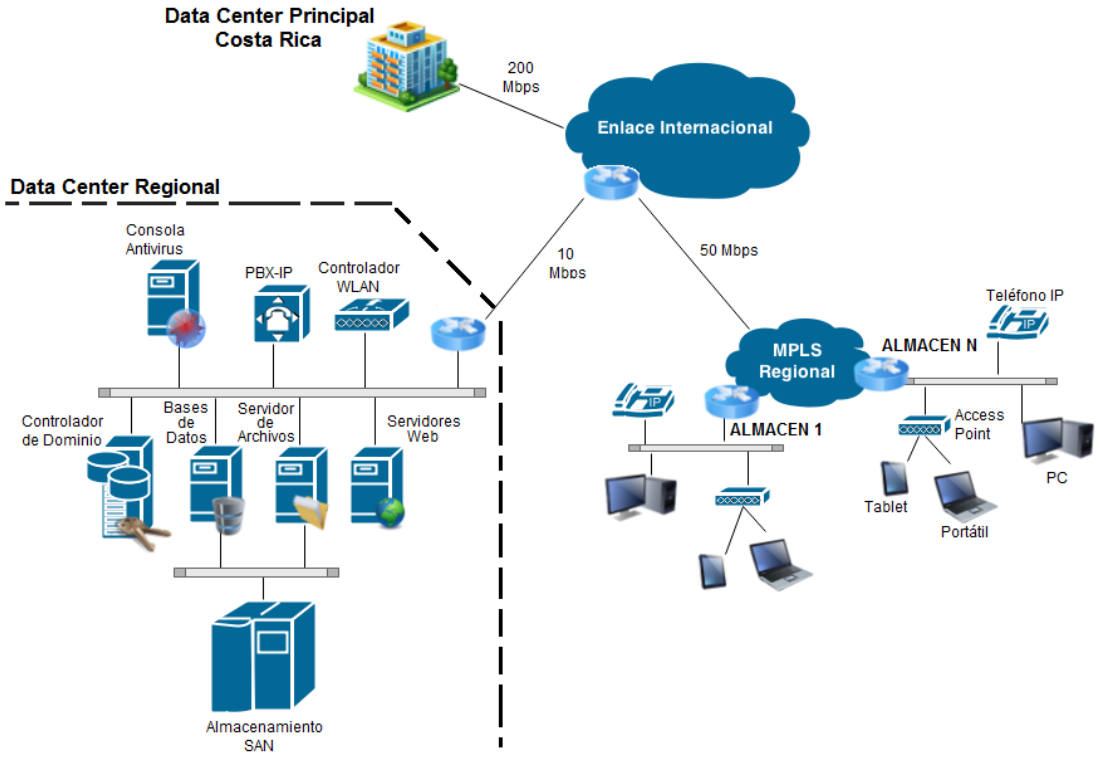


Figura 4. Topología de red y principales recursos tecnológicos – Sede Regional

Adicionalmente, la empresa cuenta con los siguientes recursos tecnológicos para prestar sus servicios tecnológicos en las oficinas principales de cada sede regional y en cada uno de los almacenes:

- Aproximadamente tres mil (3000) equipos de cómputo de escritorio y unos quinientos (500) portátiles, todos ellos adquiridos en modalidad de leasing actualmente con el proveedor IBM.

- Dos (2) servidores físicos ubicados en cada almacén, con sistema operativo Linux utilizados en configuración de alta disponibilidad activo-pasivo para la aplicación de

terminales de pago (POS). En total se tienen actualmente ciento cuatro (104) servidores en producción para toda la empresa.

- Herramienta para Virtualización de aplicaciones, con la que potencian la empresa a trabajar desde cualquier PC de la empresa con todas las aplicaciones que cada uno requiere de acuerdo a su rol.

- Herramienta de Virtualización de servidores, con la que logran compartir recursos de hardware en diferentes servidores virtuales, mejorando la eficiencia en el consumo de recursos.

- Sesenta (60) Routers para la conectividad de red (MPLS).

- Doscientos (200) Switches de 24 puertos de 1Gbps.

- Ciento veinte (120) Access Point 802.11n.

- Cuatro mil (4000) teléfonos IP.

2.6. Principales aplicaciones y sistemas de información

A continuación se relacionan los principales sistemas de información, con su respectiva ubicación:

Sistema de Información	Ubicación
Aplicación para gestión de inventarios, precios y costos	Sedes regionales
Aplicación de recibo y despacho de mercancía	Sedes regionales
Sistema para gestionar los pedidos a proveedores y a bodegas de almacenamiento central	Sede principal
Sistema para la logística de operaciones	Sede principal
Aplicación para el manejo de fuerza comercial de ventas	Sede principal
Sistema para el control de los puntos de venta (POS – Point of Sale)	Cada uno de los almacenes de la empresa
Sistema de control de nómina	Sede principal

Tabla 1. Relación de los principales sistemas de información de la empresa

2.7. Otros procesos de negocio

La empresa cuenta en general con procesos que se ejecutan de forma coherente y sistemática, sin embargo no todos ellos se encuentran en un buen nivel de madurez y más aun no todos se encuentran completamente documentados.

Algunos de los procesos que la empresa considera misionales (principales para el negocio) son:

- Venta de productos y servicios por Internet: Es un proceso diseñado para brindar a los clientes una mejor relación con la marca, permitiendo adquirir o apartar productos o servicios de la empresa sin salir de su hogar. Comprende el mantenimiento de la página web, incluyendo algunas etapas operativas como la validación de los productos ofrecidos, la toma de fotografías y videos promocionales, el diseño de ofertas especiales, la generación física de tirillas y su posterior envío al cliente, y algunas etapas automatizadas como la validación y ajuste de inventarios en línea, la generación de órdenes de compra para el despacho de mercancías, el pago de productos o servicios por medios electrónicos y la atención telefónica de quejas o reclamos.

- Recibo, alistamiento y despacho de mercancía: Comprende las etapas de recibo de mercancía en bodegas centralizadas desde los proveedores, el envío de mercancía entre las bodegas de almacenamiento y los almacenes, y culmina con el envío de mercancía desde los almacenes hasta el domicilio de los clientes, manteniendo el registro de todos los movimientos en el software de recibo y despacho de mercancía.

- Gestión de inventarios: Control y documentación de inventarios físicos en los almacenes.

- Reabastecimiento de mercancía en almacenes: Comprende la identificación de huecos (mercancía a punto de agotarse), el reporte al sistema central de pedidos.

- Logística de importaciones y exportaciones: incluye todas las etapas que se surten para importar productos hacia los países donde la empresa tiene presencia y la exportación de mercancía entre dichos países.

- Diseño de campañas comerciales: Todo lo relacionado con promociones y campañas comerciales de cara al cliente.

A continuación se relacionan algunos de los procesos que se encuentran fuera del ámbito de TI que se encuentran directamente relacionados con la seguridad de la información en la empresa y son considerados de apoyo a los procesos misionales:

- Proceso de vinculación, promoción y desvinculación de personal (Directo y tercero): Se encuentra directamente relacionado con el proceso de gestión de acceso lógico que se ejecuta en el área de Seguridad Informática.

- Proceso de Investigaciones disciplinarias: Es coordinado al interior de la Vicepresidencia de Gestión Humana y se aplica en aquellos incidentes de seguridad de la información donde se sospeche que hubo alguna conducta indebida o malintencionada de parte de algún colaborador.

- Proceso de Auditoría interna: Una vez al año se elabora el plan de auditoría y se ejecuta en el transcurso del año. Permite entre otras validar la correcta implantación de los procesos de TI y Seguridad de la información.

Otros ejemplos de procesos considerados de apoyo para el negocio son:

- Gestión de experiencia de compra y atención a clientes
- Compensación salarial
- Gestión del clima organizacional

3. ALCANCE Y OBJETIVOS DEL PLAN DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a lo definido con la junta directiva, la implantación del plan director de seguridad de la información en la empresa debe ser realizada de forma gradual, acotada inicialmente a los procesos misionales definidos en el siguiente alcance, incluyendo la tecnología, el personal y los procesos de apoyo asociados:

> El Sistema de Gestión de Seguridad de la Información (SGSI) de *Tu Hogar con Estilo S.A.* tiene como alcance los procesos de ***Venta de Productos y Servicios por Internet*** y ***Recibo, alistamiento y despacho de mercancía***, teniendo en cuenta para este último que su implantación se verá acotada al ***Centro de Distribución Principal*** de Costa Rica, ubicado en Alajuela y al ***Almacén Colonia del Rio***, ubicado en San José de Costa Rica.

A continuación se presentan los principales objetivos del plan maestro de seguridad de la información, considerando que éste nos permitirá obtener la certificación ISO 27001:2005 acotados en el alcance definido.

- Brindar niveles razonables de seguridad a la información que los clientes entregan a la empresa al realizar compra de productos o servicios por Internet, reduciendo la materialización de posibles amenazas que conlleven a la divulgación o modificación no autorizada de dicha información.

- Garantizar el cumplimiento de las diferentes normativas nacionales en materia de Seguridad de la información y protección de datos personales en los diferentes países en los que tiene presencia la empresa.

- Asegurar los procedimientos manuales o automatizados que involucran intercambio de información de clientes con los terceros contratados para la prestación del servicio de atención telefónica de quejas y reclamos (Call Center).

- Aumentar las ventas, el posicionamiento de la marca y la experiencia de compra de los clientes generando seguridad, confianza y sensación de respaldo al solicitar productos o servicios de la empresa por canales no presenciales.

- Ofrecer un canal estable y seguro que permita a los clientes relacionarse con la marca “Tu Hogar con Estilo” a cualquier hora del día, cualquier día del año.

4. ANÁLISIS DIFERENCIAL

Basado en los requerimientos generales de la norma ISO 27001 y en los 11 dominios, 39 objetivos de control y 133 controles relacionados en su anexo A se elaboró un marco general para realizar un análisis de brecha, o análisis diferencial de la seguridad de la información en la empresa respecto a la mencionada norma. Adicionalmente se tuvo en cuenta las recomendaciones de implementación relacionadas en la norma ISO 27002 para estimar el Estado y porcentaje de implementación de cada control en la empresa.

Dicho análisis se realizó teniendo en cuenta el estado de la seguridad de la información en la empresa antes de haber dado inicio a la definición de este proyecto, es por ese motivo que a pesar de ya contar con un alcance definido para el plan director de implantación del SGSI (Ver numeral 3. Alcance y objetivos del plan director de seguridad de la información), en los resultados del análisis diferencial aún se relaciona que la empresa no cuenta con dicho alcance.

El marco utilizado como base para el análisis diferencial se puede apreciar en la tabla 2, y el análisis completo realizado se puede encontrar en el Anexo 1 de este documento. En dicho anexo se incluye la evaluación del cumplimiento de los principales requisitos generales de la norma ISO 27001 y adicionalmente se incluye la evaluación del nivel de implementación de todos los controles y objetivos de control incluidos en el anexo A de dicha norma.

Requerimiento, Control u Objetivo de Control ISO 27001				IMPLEMENTACIÓN		
Tipificación	# Sección	Nombre	Descripción/Objetivo	Estado	%	Observaciones

Tabla 2. Marco utilizado para el análisis diferencial respecto a ISO 27001

En el marco utilizado se incluyeron las siguientes columnas:

- **Tipificación:** Permite identificar y diferenciar los requisitos generales, dominios, objetivos de control o controles.

- **# de Sección:** Se encuentra ligado a los números de sección de la norma ISO 27001:2005.

- **Nombre:** Corresponde al nombre del requisito, dominio, objetivo de control o control evaluado.

- **Descripción/Objetivo:** Se relaciona una breve descripción extraída de la norma ISO 27002.

- **Estado:** Corresponde a “Implementado”, “Parcialmente implementado” o “No implementado” según corresponda. El estado se encuentra directamente relacionado con el porcentaje (%) de implementación mediante una estimación matemática, de

manera que si tenemos un control en el 0% equivale a un control “No implementado”, si se encuentra por encima del 60% se puede considerar “Implementado” y en los demás casos será “Parcialmente implementado”.

- **%:** Corresponde al porcentaje estimado de implementación del control o requisito basado en la realidad actual de la empresa evaluada respecto a la norma ISO 27001 teniendo en cuenta los lineamientos dados por la norma ISO 27002.

- **Observaciones:** Se incluyen a manera explicativa sobre la forma o condición específica en la que se encuentra implementado cada control o requisito en la empresa.

Vale la pena recalcar que en este análisis se han incluido todos los controles del anexo A de la norma ISO 27001, sin tener en cuenta que algunos de esos controles no serán de aplicación en la empresa, pues este asunto será tenido en cuenta posteriormente durante la elaboración del SOA.

Para estimar matemáticamente la calificación del nivel de implementación de los objetivos de control se ha realizado un promedio de las evaluaciones de los controles incluidos en éstos objetivos. Así mismo, la evaluación de los Dominios de la ISO 27001 corresponde al promedio resultante de la evaluación de sus objetivos de control y controles.

De acuerdo a la evaluación realizada del cumplimiento de los requisitos generales de la ISO 27001, se obtuvo que en promedio solo el 19% de éstos se encuentran implementados en la empresa. Lo anterior no quiere decir que la seguridad de la información en la empresa no sea adecuada, sino que actualmente la empresa no cuenta con el nivel de madurez en sus procesos de seguridad de la información de acuerdo a lo establecido en la norma ISO 27001 y por ende no es encuentra lista para afrontar una auditoría de certificación.

Implementación de Requerimientos Generales ISO 27001	**19%**

Tabla 3. Estado de implementación de requisitos generales de la ISO 27001

Respecto a la evaluación de los controles del anexo A de la norma ISO 27001, a continuación se relaciona el consolidado de dicha evaluación agrupado por dominios y en general para todos los controles (Ver tabla 4).

# Sección	Nombre	% implementación
A.5	Política de Seguridad	55%
A.6	Aspectos Organizativos de la Seguridad de la Información	41%
A.7	Gestión de Activos	13%

A.8	Seguridad Ligada a los Recursos Humanos	58%
A.9	Seguridad Física y del Entorno	77%
A.10	Gestión de Comunicaciones y Operaciones	62%
A.11	Control de Acceso	46%
A.12	Adquisición,Desarrollo y Mantenimiento de Sistemas de Información	39%
A.13	Gestión de Incidentes de Seguridad de la Información	36%
A.14	Gestión de la Continuidad del Negocio	8%
A.15	Cumplimiento	60%
TOTAL SGSI		**45%**

Tabla 4. Estado general de implementación ISO 27001 por dominios

En las figuras presentadas a continuación se muestra la relación entre todos los dominios respecto al máximo posible (100%) evidenciando en color rojo aquellos que están por debajo del valor medio posible.

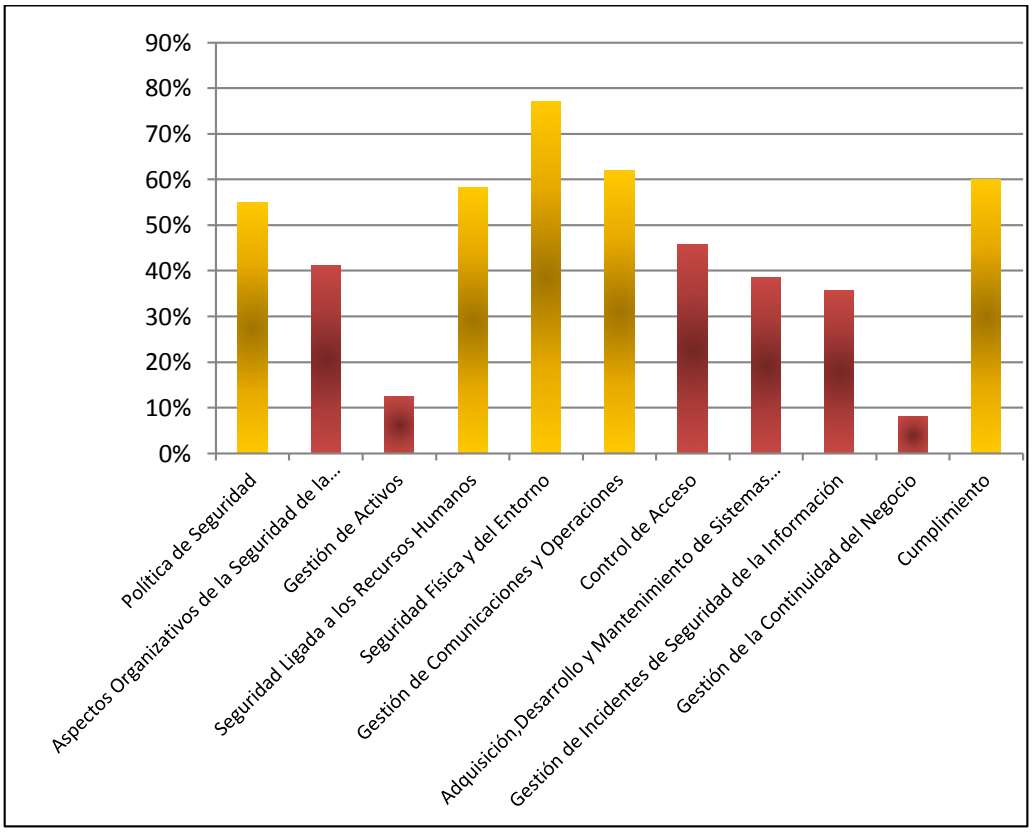


Figura 5. Estado general de implementación de controles del anexo A - ISO 27001

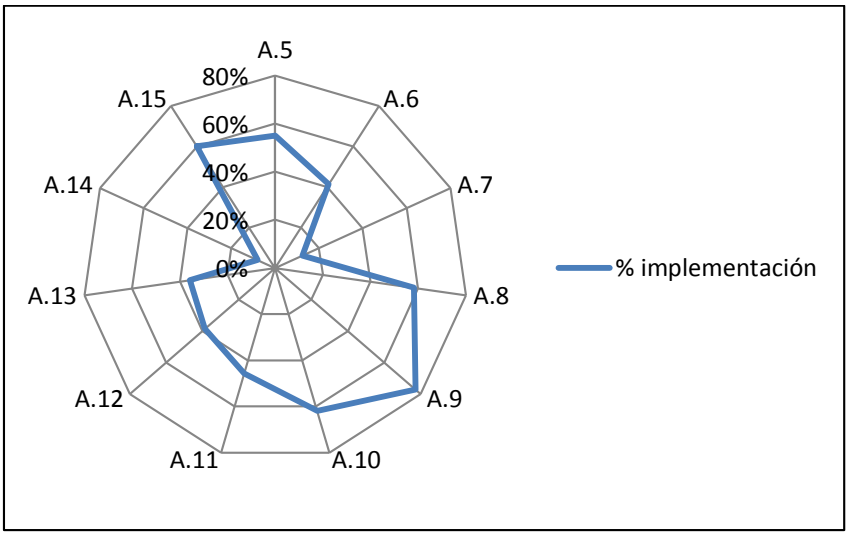


Figura 6. Diagrama de radar implementación controles el Anexo A - ISO 27001

En los datos y gráficos mostrados anteriormente, vale la pena destacar que el dominio que tiene un mayor nivel de madurez en la implementación de controles es el A.9, asociado con la seguridad Física y del entorno. Históricamente para la empresa este dominio había sido su principal preocupación en cuanto a la seguridad, por lo cual había desarrollado procedimientos e implementado mecanismos de control para la protección física de la empresa y sus activos. Adicionalmente con la evaluación de los controles asociados a este dominio se evidencia claramente la ventaja de contratar el servicio de DataCenter con una empresa reconocida, la cual le brinda un nivel de seguridad física considerablemente alto a sus activos informáticos, adicional a un buen nivel de servicio (disponibilidad), de acuerdo a lo exigido en el contrato.

Por otro lado, se evidencia que los dominios A.7 y A.14, asociados a Gestión de Activos y Continuidad del Negocio respectivamente, corresponden a los que menor grado de madurez tienen en la empresa, teniendo un evidente amplio camino por recorrer de frente a una posible certificación en ISO 27001:2005.

5. ESQUEMA DOCUMENTAL DEL SGSI

5.1. Tipos de documentos

El esquema documental del SGSI está compuesto por las políticas, registros, instructivos, diagramas de flujo y formatos asociados con los procesos, procedimientos y controles implementados en Tu Hogar con Estilo S.A. A continuación se describe a groso modo la función de cada uno dentro del SGSI:

- **Política:** Utilizado para definir las bases, lineamientos u obligaciones generales o específicas propias de un proceso o procedimiento.
- **Instructivo:** Permite documentar el paso a paso de cierto procedimiento.
- **Registro:** Permite documentar valores específicos asociados con un control, actividad o indicador, obtenidos como salida de un proceso o procedimiento.
- **Diagrama de Flujo:** Describe el paso a paso de las actividades realizadas en un proceso o procedimiento.
- **Formato:** Utilizado principalmente para documentar solicitudes, que serán el insumo de un proceso o procedimiento.

Cada documento debe cumplir con una estructura definida de acuerdo al tipo de documento. Para el caso de las políticas e instructivos, adicional al contenido propio de cada documento, se debe contar como mínimo con lo siguiente:

- **Portada**: indicando el nombre del documento, descripción general de su contenido, nombre y logo de la empresa, nivel de clasificación de acuerdo a su confidencialidad y fecha de publicación.
- **Caracterización del documento**: Nombre del documento, nivel de clasificación de acuerdo a su confidencialidad, codificación, versión del documento, fecha de última modificación, fecha de creación, cargo o rol del responsable del documento y cargo o rol del responsable de aprobar el documento.
- **Control de versiones**: incluyendo el número de versión, la fecha de publicación, el encargado de la modificación y algunas observaciones asociadas a la motivación del cambio.
- **Tabla de contenido**: Indicando los títulos y su ubicación en el documento.
- **Aprobación del documento**: Se deben incluir los nombres y cargos de las personas que validaron el contenido del documento y aprobaron su publicación.

Para el caso de los registros, diagramas de flujo y formatos se debe contar como mínimo con los siguientes campos propios de la caracterización de documentos:

- Nombre y logo de la empresa
- Nombre del documento
- Versión del documento
- Codificación
- Nivel de clasificación de acuerdo a su confidencialidad

5.2. Control de versiones

Cada documento debe manejar un control de versiones, definido mediante un número entero que indica la versión y un (1) dígito decimal que indica la sub-versión. La primera liberación del documento al público deberá realizarse con la versión 1.0 y se define que cada vez que el documento sufra cambios mayores en su contenido deberá aumentar de versión y cuando sufra cambios de forma o cambios menores en su contenido deberá cambiar de sub-versión. Adicionalmente se establece que cuando se alcancen los diez (10) cambios de sub-versión, se deberá cambiar de versión, pues se considera que ha sufrido cambios mayores desde su versión actual.

5.3. Codificación de documentos

La codificación definida para cada documento tiene el siguiente formato:

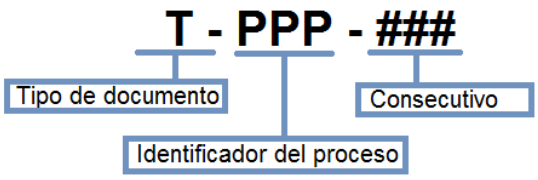


Figura 7. Codificación de documentos para el esquema documental

A continuación se relaciona cada uno de los campos que componen la codificación definida:

1) **Tipo de documento**: Permite identificar políticas (P), registros (R), instructivos (I), diagramas de flujo (D) y formatos (F).

2) **Identificador del proceso**: se asigna un código de tres (3) dígitos a cada proceso creado en la empresa. El código es asignado por el área de procesos corporativos.

3) **Consecutivo**: es un código numérico que va desde 001 hasta 999 y permite enumerar los distintos documentos en cada proceso.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información fue incluida en el documento maestro del SGSI llamado “Modelo de Seguridad de la Información”. Este documento contiene entre otras, los principales lineamientos establecidos por Tu Hogar con Estilo S.A. para ofrecer niveles razonables de protección a su información y sus activos, y la declaración de compromiso de la dirección en apoyo del desarrollo del SGSI.

El documento elaborado, perteneciente al proceso de Gestión de Seguridad de la Información fue codificado como P-GSI-001 (ver anexo 2) y debe ser conocido y aplicado por todos los colaboradores que presten sus servicios a la empresa independiente de su modalidad de contratación.

En el numeral 9 del anexo 2 (documento P-GSI-001 adjunto a este trabajo), se documenta el contenido de la Política General de Seguridad de la Información, separada en diez (10) políticas de primer nivel que agrupan las cincuenta y dos (52) políticas actuales de segundo nivel[6], relacionadas con temas específicos que requieren lineamientos normativos de seguridad de la información.

Adicionalmente, en el numeral 8 del anexo 2 se incluye el compromiso formal de la dirección con la seguridad de la información y su apoyo formal al diseño, implementación, mantenimiento y mejora del SGSI.

[6] El detalle de las políticas de segundo nivel no se incluye en este trabajo

7. ROLES Y RESPONSABILIDADES

En el numeral seis (6) del anexo 2 (documento P-GSI-001 adjunto a este trabajo), se documentan los principales roles, áreas y cargos involucrados con el desarrollo, implementación, mantenimiento y mejora del SGSI con las responsabilidades asociadas a cada uno de ellos.

Los principales roles a destacar son el del Comité de Seguridad de la información, cuya conformación se documenta en el numeral 7.2 del anexo 2; adicionalmente, el rol del Oficial de Seguridad de la Información, encargado de liderar el comité y en general el SGSI, y finalmente el rol de todos los colaboradores de la empresa, encargados de que la seguridad de la información alcance todos los niveles de la organización.

8. PROCEDIMIENTO DE REVISIÓN POR LA DIRECCIÓN

De acuerdo a lo establecido por la Junta Directiva, el Comité de Seguridad de la Información es el órgano encargado de efectuar cada año iniciando el mes de diciembre, una revisión integral de los aspectos más importantes relacionados con el Sistema de Gestión de Seguridad de la Información. En el documento codificado como D-GSI-001 (ver anexo 3) se presenta de una forma muy básica el diagrama de flujo del procedimiento establecido para la revisión del SGSI por la dirección.

Para esta revisión, el comité deberá tener en cuenta los siguientes insumos:

1) Los resultados de la auditoría del SGSI

2) Las actas del Comité de Seguridad de la información del año en curso.

3) Propuestas de nuevas técnicas, productos, controles, procesos o procedimientos o recomendaciones de mejora presentadas por el Oficial de Seguridad de la Información.

4) Informe de fin de año del estado de las acciones correctivas y preventivas efectuadas sobre el SGSI

5) Listado de riesgos, vulnerabilidades o amenazas no gestionadas adecuadamente durante el año en curso

6) Los resultados de las mediciones de efectividad de los controles del SGSI

7) Los planes de acción definidos en la pasada revisión por la dirección.

Al finalizar la revisión, el Comité de Seguridad de la Información debe emitir un informe en el que incluya posibles mejoras y su concepto general sobre como mínimo los siguientes aspectos:

1) Plan estratégico de S.I.

2) Modelo de Seguridad de la Información y políticas asociadas

3) Efectividad del SGSI

4) Plan de tratamiento y evaluación del riesgo

5) Procedimientos y controles asociados con la seguridad de la información

6) Recursos tecnológicos, de personal, de capacitación o consultoría requeridos.

7) Metodología de medición de la efectividad de los controles.

9. AUDITORÍAS INTERNAS DEL SGSI

Una vez la empresa obtenga la certificación ISO 27001:2005 deberá someterse a un proceso de auditorías periódicas que permitirá entre otras, garantizar la continuidad del SGSI a través del tiempo. Para ello la empresa ha definido que realizará auditorías internas 1 vez al año en complemento a las auditorías anuales realizadas por el ente certificador.

9.1. Planificación de las auditorías

Para garantizar que el sistema de gestión de seguridad de la información se encuentra alineado con los requisitos de la ISO 27001 necesarios para su certificación, el área de auditoría interna presentará cada año finalizando el mes de julio un informe consolidado con las conclusiones y hallazgos de la auditoría realizada. Para ello, elaboró y presentó un plan de auditorías con periodicidad de ejecución anual, incluyendo entre otras, el documento codificado como R-AUD-001 (ver anexo 4), perteneciente al proceso de Auditoría Interna, en el que se muestra el cronograma de actividades estimado para la auditoría interna del SGSI, comenzando en la "semana 0" que debería coincidir generalmente con la primera semana de junio de cada año.

Adicionalmente se incluye en el plan de auditoría, el listado de las principales verificaciones que serán realizadas durante la auditoría interna del SGSI, las cuales se presentan en la siguiente tabla.

Objetivo/Control/Requisito auditado	Alcance
Documentación del SGSI	Validar la existencia y suficiencia de una Política de seguridad de la información (incluyendo el compromiso de la dirección), alcance del SGSI, declaración de aplicabilidad (SOA), roles y responsabilidades de SI, procedimientos o metodologías para gestionar riesgos y activos de información y estructura organizacional de la función de seguridad de la información.
Activos de información de la organización	Validar la existencia y estado de actualización de las matrices de activos de información por cada uno de los procesos incluidos en el alcance de la certificación del SGSI. Adicionalmente se validará que los activos de información en dichas matrices cuenten con una clasificación (valor de la información) y que dichas matrices sean efectivamente utilizadas dentro de la gestión de seguridad de la organización.
Análisis de riesgos de los procesos	Validar la existencia y estado de actualización de las matrices de riesgo de seguridad de la información por cada uno de los procesos incluidos en el alcance de la certificación del SGSI. Adicionalmente se validará que dichas matrices sean efectivamente utilizadas dentro de la gestión de seguridad de la organización y que contemplen la criticidad de sus activos de información.
Plan de divulgación, capacitación y concientización de Seguridad de la Información	Se validará la existencia y estado de implementación de un plan continuo de sensibilización sobre seguridad de la información, al igual que su aplicación en el momento de la vinculación de los empleados y de manera periódica a toda la organización. Adicionalmente se realizará un muestreo entre las diferentes áreas para determinar el grado de efectividad de dicho plan entre los empleados.
Verificación de controles y	Validar la efectividad de los procedimientos definidos para otorgar,

procedimientos asociados con acceso lógico en sistemas críticos	modificar y retirar privilegios de acceso a los principales aplicativos de la organización. Se incluye el directorio activo (ldap), los servidores de bases de datos y de aplicaciones críticas de la organización.
Pruebas de vulnerabilidades y penetración sobre la infraestructura tecnológica crítica	Se validará la existencia y suficiencia de pruebas semestrales de vulnerabilidades sobre la infraestructura de red y servicios de la organización al igual que la existencia y suficiencia de pruebas de penetración sobre los servicios críticos de la organización que sean accesibles desde Internet. Para cada una se verificará la existencia de planes de acción asociados con los hallazgos realizados en cada prueba y el cumplimiento de dichos planes de acción.
Verificación de controles y procedimientos asociados con acceso físico a las instalaciones críticas	Validar la efectividad de los controles de acceso físicos a las instalaciones de procesamiento de datos sensibles de la organización, incluyendo el centro de cómputo principal y los archivos de almacenamiento de datos en formato físico (papel, cintas magnéticas, etc).
Plan de continuidad del negocio y recuperación de desastres	Validar la existencia de un plan de continuidad de negocio y recuperación de desastres para los procesos definidos en el alcance de la certificación del SGSI y para la infraestructura de misión crítica de la organización. Adicionalmente se validarán la existencia de informes asociados con pruebas periódicas de la efectividad de los planes de continuidad y recuperación.
Cumplimiento de requisitos legales y de derechos de autor	Validar la existencia de procedimientos para garantizar el cumplimiento de los requisitos legales aplicables en materia de seguridad de la información (incluyendo privacidad) y de cumplimiento de derechos de autor en el software utilizado en las instalaciones. Adicionalmente se realizará un muestreo en diferentes áreas de la organización para validar que no cuenten con software no autorizado en los equipos de cómputo.
Verificación de controles y procedimientos asociados con el ciclo de vida de los sistemas de información	Validar los controles aplicados en el diseño, desarrollo, pruebas e implementación de aplicaciones y sistemas de información de la organización o en la contratación de los mismos con terceros, de acuerdo a lo definido en la declaración de aplicabilidad. En dichas etapas deben estar incluidas consideraciones de seguridad de la información de acuerdo a su clasificación y al nivel de riesgo asociado.
Verificación de controles y procedimientos asociados con seguridad perimetral	Se realizarán intentos de acceso desde redes externas hacia la red interna de servicios y de usuarios (sin pretender reemplazar pruebas extensivas de penetración). Se analizará la configuración de reglas de acceso (locales y remotas) y la topología lógica asociada con la seguridad perimetral de la organización.
Verificación general de controles de acuerdo a la declaración de aplicabilidad (SOA)	Dada la gran cantidad de controles establecidos en la empresa, se realizarán validaciones de cada uno de los controles de forma incremental hasta alcanzar la totalidad de ellos, teniendo como base la declaración de aplicabilidad. La planeación de dicha verificación es realizada de tal forma que en el transcurso de 3 años se habrán verificado por lo menos 1 vez cada uno de los controles definidos de acuerdo a lo estipulado en el documento SOA, teniendo como base una primera verificación completa previa a la obtención de la certificación. El cronograma detallado de la verificación incremental de los controles se encuentra separado del cronograma general de auditoría, pues incluye actividades que son realizadas en el transcurso de 3 años.

Tabla 5. Objetivos, controles y requisitos auditados

9.2. Metodología de revisión de los controles y requerimientos

De acuerdo a lo estipulado en conjunto con el área de auditoría Interna, la auditoría será realizada in situ, verificando la existencia y el cumplimiento de políticas, metodologías, procedimientos, la implantación de los controles de seguridad y la eficacia del sistema en su conjunto.

Las auditorías internas anualmente darán inicio con una reunión de apertura en la que el área de auditoría interna presentará al comité de seguridad de la información los objetivos y alcance de la auditoría, incluyendo los procesos, las áreas y las instalaciones del negocio que serán incluidas y los recursos necesarios de parte de la empresa en el transcurso de la auditoría. La auditoría tomará como base la declaración de aplicabilidad (SOA), los informes y hallazgos de auditorías pasadas, el estado de implantación de políticas, procedimientos y controles, reportado por el oficial de seguridad de la información, entre otras que se definan en común acuerdo con la empresa durante la reunión de inicio.

Previo a iniciar con la revisión de los controles se realiza una validación de cada una de las observaciones y exclusiones documentadas en la declaración de aplicabilidad (documento SOA). Tal como se mencionó en la planeación de la auditoría, se tiene contemplado realizar una validación inicial de todos los controles y a partir de allí, se realizará una verificación incremental de cada uno de ellos, hasta abarcar la totalidad en un lapso de 3 años (Tiempo que dura la certificación), iniciando por aquellos controles que a juicio del auditor sean de mayor criticidad para los procesos del negocio incluidos en el alcance de la certificación. Lo anterior incluye controles que solo serán validados una (1) vez cada 3 años y adicionalmente otros que por su criticidad, serán verificados cada año.

Adicionalmente, la auditoría aportará a la empresa una evaluación del nivel de madurez en seguridad de la información tomando como base el Modelo de Madurez de la Capacidad (CMM), dando una estimación del nivel de madurez de cada uno de los controles implantados en la empresa, para con ello obtener una estimación de la madurez de los objetivos de control[7] y dominios[8] planteados en la norma ISO 27002.

De acuerdo al modelo planteado, existen cinco (5) posibles niveles de madurez y un nivel adicional para los controles que se consideran inexistentes (nivel cero). A medida que se avanza en los niveles se considera que el control es más efectivo para la organización, por ello se mide adicionalmente el porcentaje de efectividad para cada control.

En la tabla 6 se puede observar cada uno de los niveles de madurez, relacionado con su respectivo porcentaje de efectividad (en rango) y con una breve descripción del cada nivel de madurez.

[7] Cálculo obtenido como el promedio matemático del nivel de madurez de los controles contenidos en cada objetivo de control

[8] Cálculo obtenido como el promedio matemático del nivel de madurez de los objetivos de control incluidos en cada dominio

Efectividad (%)	Nivel de Madurez (CMM)		Descripción
0%	L0	Inexistente	-Carencia completa de cualquier proceso. -La empresa no ha reconocido que existe un problema a resolver.
Entre 0% y 10%	L1	Inicial / Ad-hoc	-El éxito de las actividades de los procesos se basa la mayoría de las veces en esfuerzos individuales. -No existen plantillas definidas a nivel corporativo.
Entre 10% y 50%	L2	Reproducible, pero intuitivo	-Los procesos similares se ejecutan en forma similar por diferentes personas con la misma tarea. -Se normalizan las buenas prácticas en base a la experiencia y al método. -No hay comunicación o entrenamiento formal -Las responsabilidades quedan a cargo de cada individuo. -Se depende del grado de conocimiento de cada individuo.
Entre 50% y 90%	L3	Proceso definido	-La organización entera participa en el proceso. -Los procesos están implantados, documentados y comunicados formalmente.
Entre 90% y 95%	L4	Gestionado y medible	-Se cuenta con indicadores y métricas que permiten cuantificar la evolución de los procesos.
Mayor a 95%	L5	Optimizado	-Los procesos están bajo constante mejora. -En base a los indicadores y métricas se determinan las desviaciones más comunes y se optimizan los procesos.

Tabla 6. Escala de medición de madurez de seguridad

La auditoría finalizará con una reunión de cierre en la que presentará un informe gerencial de auditoría y entregará el informe final que incluye los detalles completos del proceso realizado y sus hallazgos. Dichos hallazgos resultantes de la revisión de los controles y requerimientos de la norma serán priorizados y presentados de forma ordenada de acuerdo a la siguiente escala de impactos establecida en común acuerdo entre el área de auditoría interna y el comité de seguridad de la información:

Clasificación	Tipo de Hallazgo	
Impacto Alto	No Conformidad Mayor	Se debe brindar atención inmediata, estableciendo planes de acción a corto plazo. Por su severidad implican la no obtención de la certificación ISO 27001.
Impacto Medio	No Conformidad Menor	Se deben establecer planes de acción a corto y mediano plazo. Implican un aplazamiento en la obtención de la certificación ISO 27001.
Impacto Bajo	Oportunidad de Mejora	Se recomienda establecer planes de acción a mediano y largo plazo. Corresponden a las recomendaciones del auditor sobre algunos aspectos que el auditor encuentra conforme a la norma pero que podrían ser mejoradas para elevar el nivel de madurez de seguridad de la empresa y reducir los riesgos asociados.
Informativo	Fortalezas identificadas	Corresponde a aquellos puntos identificados como muy positivos por la auditoría y sobre los cuales la empresa debería enfocarse en mantener a través del tiempo.

Tabla 7. Clasificación de impacto para los hallazgos de auditoría Interna del SGSI

9.3. Informe de auditoría

La etapa final del plan de auditoría consiste en la elaboración y presentación del informe final, que permitirá dar a conocer los hallazgos y conclusiones de la auditoría. La estructura utilizada para dichos informes es la siguiente:

- **Introducción:** incluyendo los objetivos y el alcance definidos.
- **Metodología empleada:** Se explica las técnicas, metodologías y buenas prácticas empleadas durante el proceso.
- **Resultados de la evaluación del nivel de madurez de seguridad de la información:** Se relaciona cada uno de los controles implantados (de acuerdo al documento SOA), con el nivel de madurez estimado y las posibles recomendaciones u oportunidades de mejora que realice la auditoría. Adicionalmente se consolidan los resultados, estimando el nivel de madurez de cada dominio de la norma ISO 27002.
- **Listado detallado de los hallazgos:** Se presenta el listado completo de las no conformidades mayores, menores, oportunidades de mejora y fortalezas identificadas en la auditoría.
- **Conclusiones y recomendaciones:** Para cada hallazgo o set de hallazgos se presentan unas recomendaciones de mejora, adicional a las conclusiones y recomendaciones generales de la auditoría.
- **Anexos:** Incluye la posible documentación que permita soportar los hallazgos identificados y aquella requerida para ampliar el detalle del informe presentado.

9.4. Requisitos para conformar el equipo de auditoría Interna

A nivel general, se proponen los siguientes roles requeridos para gestionar el programa de auditoría del SGSI en la empresa:

- **Rol de auditor jefe o auditor líder**: Esta persona debe ser un líder por naturaleza, capacidad de comunicación verbal y escrita, y adicionalmente debe estar en capacidad de gestionar los recursos requeridos y resolver los conflictos que se presenten. Adicionalmente debe contar con las mismas habilidades y destrezas que las requeridas para el rol de auditor. La persona que ejerza este rol debe ser Ingeniero de Sistemas, telemático o similar, contar con una experiencia profesional previa de mínimo cinco (5) años como auditor jefe o un cargo similar, contar como mínimo con las certificaciones CISA y auditor líder en SGSI ISO 27001.
- **Rol de auditor:** Debe tener capacidad de comunicación verbal y escrita, buena presentación personal y habilidades para la elaboración de informes escritos y exposiciones presenciales. Adicionalmente es importante que las personas que ejerzan este rol sean sinceros, honestos, discretos, estén dispuestos a escuchar diferentes opiniones, ser observador, constante, respetuoso y con gran capacidad de adaptarse a

diferentes situaciones. La persona que ejerza este rol debe ser Ingeniero de Sistemas, telemático o similar, contar con una experiencia profesional previa de mínimo tres (3) años como auditor interno de SGSI, contar como mínimo con la certificación CISA y cursos de auditor interno ISO 27001 o similares

- **Rol de experto técnico:** Las personas que ejerzan este rol deben ser Ingenieros de Sistemas, Telemáticos, Electrónicos o similares, contar con un posgrado relacionado con Seguridad Informática y como mínimo la certificación CISSP. Debe demostrar amplios conocimientos y experiencia en las áreas y procesos del negocio que la empresa requiere auditar. Adicionalmente debe contar con una experiencia mínima de 5 años en cargos relacionados con seguridad de las tecnologías de información y comunicaciones. La empresa considera que el rol de experto técnico no requiere conocimientos ni experiencia previa en auditoria y sería incluido en un proceso de formación y capacitación por parte de la empresa para convertirse en auditor de la misma. En otras palabras serían considerados auditores en formación, para que con el tiempo, los auditores de la empresa sean a su vez expertos técnicos.

Con estos roles definidos se requieren inicialmente tres (3) personas con dedicación de tiempo completo que serían asignadas a diferentes auditorías relacionadas con tecnologías de la información y tendrían la función de acompañar al auditor externo en las auditorías de certificación. La planta de personal debería ser ampliada a medida que se requiera ampliar el alcance de los controles validados, las pruebas realizadas o los procesos o áreas dentro del alcance.

10. METODOLOGÍA DE ANÁLISIS DE RIESGOS

El comité de seguridad de la información ha decidido aplicar al interior de la empresa un método propio basado en la metodología de análisis y gestión de riesgos conocido como MAGERIT[9], elaborada por el Consejo Superior de Administración Electrónica y orientado a las administraciones públicas de España. A pesar de que dicha metodología se enfoca en la información en medios digitales, almacenada o procesada mediante sistemas de información, el comité consideró dicho método adecuado y para una siguiente fase de madurez se analizará la viabilidad de incluir en la metodología los activos en medios físicos (documentos en papel).

Tal como se muestra en la figura 8, el método a groso modo implica que se realizará una identificación y valoración de riesgos y amenazas sobre los activos de información de la organización, para luego determinar las medidas de control actuales y futuras necesarias para realizar un tratamiento adecuado a dicho riesgo.

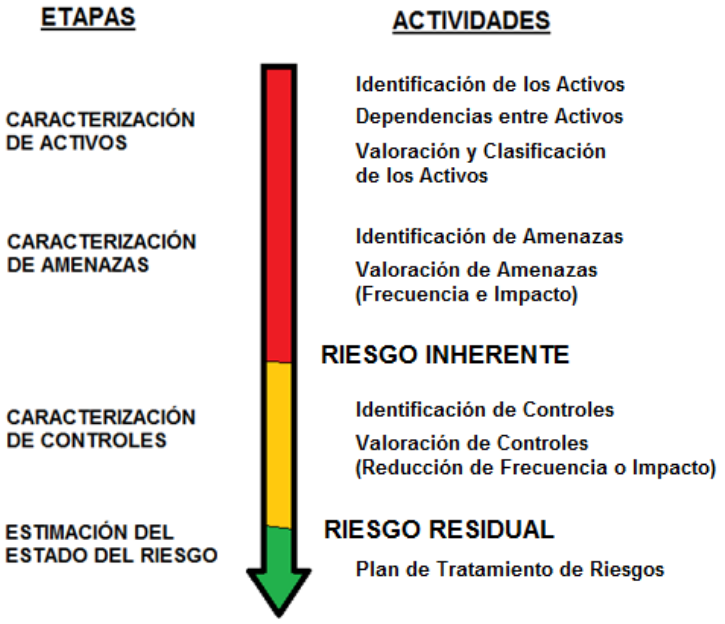


Figura 8. Etapas y actividades del método de análisis de riesgos

Para tratar de garantizar que para cada proceso del negocio se surtan adecuadamente cada una de las etapas y actividades de este método, se publicó una lista de chequeo, codificada como F-GSI-001 (ver anexo 5 de este documento), en la que se relacionan cada una de las etapas y actividades en el orden en que deben ser realizadas. A continuación se presenta cada una de las etapas que componen el método de análisis y gestión de riesgos y en el anexo 10 del presente documento se relaciona la lista de chequeo (F-GSI-001) elaborada para los procesos dentro del alcance del SGSI previo a la primera auditoría de cumplimiento ISO 27001:2005.

[9] El método original se encuentra en su versión 3 y consta de tres (3) documentos que pueden ser consultados y descargados a través del portal http://administracionelectronica.gob.es

Adicionalmente, en el anexo 12 se encuentra un ejemplo paso a paso del desarrollo del método definido para un (1) activo dentro de un (1) proceso de la empresa.

10.1. Cómo identificar activos de información

A partir del método de análisis de riesgos surge la definición de lo que en la empresa se conoce como activos de información, los cuales son la base para la metodología en sí, siendo aquello que debe ser protegido. La definición acuñada en la empresa fue extraída de la definición dada al término "Activo" en la norma UNE 71504:2008 y en el mismo método MAGERIT. Veamos:

> **Activo de información:**
> *"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos."* [UNE 71504:2008]

A continuación se relacionan los diferentes tipos o categorías de activos de información identificables en las actividades propias del día a día de los colaboradores de la empresa y en general en los procesos del negocio:

- Información o datos que la materializan
- Servicio que presta un sistema de información o servicios auxiliares necesarios por el sistema
- Aplicaciones informáticas que permiten manejar datos
- Equipos informáticos que permiten almacenar datos o información, o que permiten prestar el servicio o soportar la aplicación.
- Dispositivos de almacenamiento de datos o información
- Equipamento y suministros necesarios para garantizar el funcionamiento de los dispositivos y equipos informáticos. Ej: Suministro eléctrico, climático
- Las redes y equipos de telecomunicaciones que permiten transmitir información o datos
- Instalaciones donde se encuentran los equipos informáticos o de telecomunicaciones
- Personas involucradas con los elementos anteriormente mencionados

En general se precisa que se deben identificar todos los activos de información que tengan un valor para la empresa y que por tanto, requieran ser protegidos, teniendo en cuenta que entre más valioso es el activo, mayor nivel de protección deberá disponerse sobre éste.

Para realizar la identificación de los activos de información en cada proceso, se recomienda analizar cada una de las actividades y etapas que lo componen, identificando los posibles activos asociados (información, servicios, personal, etc) y se debe diligenciar la llamada Matriz de Activos de Información, que no es otra cosa que el registro donde se documentan los activos de información y sus características. Dicha matriz fue codificada como R-GSI-001 (ver anexo 7) y a groso modo contiene los siguientes campos:

Nombre del campo	Descripción
Fecha de Actualización	Fecha en la que se realizó la última actualización del activo de información. Se debe escribir en el formato dd/mm/aaaa.
Proceso	Nombre del proceso del negocio en el cual se identifica el activo de información.
Consecutivo Propio	Número consecutivo único asignado a cada activo de información.
Depende del consecutivo	Se relaciona uno (1) o más consecutivos de los activos superiores del activo documentado. Con base en estos consecutivos se calculará el valor del activo, como la suma de los valores de cada activo relacionado en esta columna. Para los activos que no tengan un activo superior se debe calcular su valor propio.
Categoría del activo de información	Se debe seleccionar la categoría a la que pertenece el activo de información: - Información o datos - Servicio - Aplicación - Equipo Informático - Dispositivo de Almacenamiento - Suministro - Equipo de red o telecomunicaciones - Instalación física - Personal
Nombre del activo de información	Nombre corto del activo de información identificado. Debe personalizarse lo mejor posible en cada proceso para evitar nombres duplicados en activos de información distintos entre los diferentes procesos del negocio.
Descripción del activo de información	Descripción del activo de información que especifique a grandes rasgos la información que contiene, de manera que se pueda establecer fácilmente la importancia que tiene el activo de información para el negocio y así determinar su valor y clasificación.
Responsable del activo de información	Encargado de establecer el valor o criticidad de un activo de información y tomar decisiones relevantes sobre el mismo.

Tabla 8. Campos que componen la matriz de activos de información

Adicional a los campos anteriores, en el documento R-GSI-001 se encuentran los campos que permiten documentar el valor del activo y su clasificación. Para ello se deben seguir las instrucciones dadas en los numerales siguientes.

A manera de ejemplo sobre la identificación de activos en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.2. Cómo valorar activos de información

Para efectuar la valoración de los activos de información, inicialmente se debe tener presente que de forma natural existe una dependencia entre activos, definida como la medida en que un activo se puede ver afectado por un incidente de seguridad materializado en otro activo. De allí surgen los conceptos de activos superiores y activos inferiores, siendo superior aquel que transmite sus necesidades de protección a los demás activos, llamados inferiores, pues la materialización de una amenaza en el activo inferior perjudica al activo superior. De acuerdo a las dependencias mencionadas anteriormente se presenta la siguiente relación:

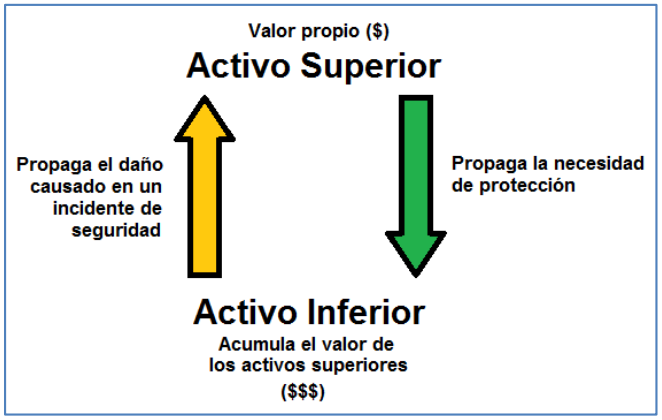


Figura 9. Dependencia entre activos superiores e inferiores

En general, el valor de los activos superiores, como la información o los servicios que presta un sistema, es propio del activo y debe ser definido con base en la pérdida que puede causar al negocio una afectación a la seguridad en alguna de sus dimensiones, sea confidencialidad, integridad o disponibilidad. Por otro lado, el valor de los activos inferiores no será calculado de forma propia, sino que será calculado como el correspondiente valor acumulado de los activos superiores que dependen o se apoyan en éste.

La valoración de los activos, sea propia o acumulada por dependencias, puede ser presentada de forma cualitativa o cuantitativa, existiendo un rango de valores cuantitativos que generan determinado valor cualitativo. Adicionalmente se contempla un valor promedio cuantitativo para cada valor cualitativo. En la tabla siguiente se documenta la relación entre la valoración cualitativa del activo y su estimado valor cuantitativo (En dólares americanos).

VALOR CUALITATIVO	VALOR CUANTITATIVO	
	Rango de valores ($ USD)	Valor promedio ($ USD)
Extremo	valor > 300.000	500.000
Muy alto	100.000 < valor > 300.000	200.000
Alto	50.000 < valor > 100.000	75.000
Medio	5.000 < valor > 50.000	25.000
Bajo	100 < valor > 5.000	2.500
Despreciable	valor < 100	100

Tabla 9. Relación entre valores Cualitativos y Cuantitativos de activos

La valoración de los activos debe ser realizada de forma independiente por cada una de sus tres dimensiones de seguridad, identificando el impacto o daño que causaría a la empresa un incidente de seguridad asociado con cada una de dichas dimensiones de seguridad.

Con el fin de agregar cierto nivel de objetividad al proceso de determinación del valor propio de los activos superiores, que por naturaleza es subjetivo, y con el fin de disminuir el riesgo de sesgo en dicho procedimiento, se dispone del instructivo codificado como I-GSI-001 (ver anexo 6), donde se presenta un listado de impactos posibles para el negocio, comparados entre sí, y en referencia a una escala de valoración que va desde 0 (activo con valor despreciable) hasta 5 (activo con valor extremo). En dicho instructivo, básicamente se pretende establecer una relación directa entre posibles impactos para el negocio y un valor cuantitativo (económico), junto con su correspondiente valor cualitativo.

Para determinar los niveles de impacto del negocio asociados con cada activo en cada dimensión de seguridad se deben hacer las siguientes preguntas:

- **Confidencialidad**: ¿Qué impacto causaría a la empresa que el activo de información fuera publicado o que fuera conocido por quien no debe?

- **Integridad**: ¿Qué impacto causaría a la empresa que el activo de información, estuviera dañado, corrupto o que fuera alterado sin autorización?

- **Disponibilidad**: ¿Qué impacto causaría a la empresa no tener el activo de información o no poder utilizarlo cuando se requiere y donde se requiere?

Por cada activo superior identificado se debe evaluar cada una de las dimensiones de seguridad, utilizando el documento I-GSI-001 como base para la determinación del valor de los activos propios y se debe registrar en la matriz de activos de información (documento R-GSI-001), marcando con una “X” todos los impactos para el negocio que apliquen en el nivel estimado que aplique para cada impacto.

Se debe tener en cuenta que los niveles de cada impacto son excluyentes entre sí, definiendo que para la valoración de cada activo en cada dimensión siempre primará el mayor valor posible de impacto para el negocio. Por ejemplo, si para un activo se determina que aplica el nivel “Extremo” del impacto “Afectación a Clientes o al público”, no se debe continuar evaluando los niveles menores del mismo impacto y se debe pasar a evaluar el impacto “Incumplimiento de leyes o regulaciones” y posteriormente los demás impactos que apliquen.

Adicionalmente, vale la pena resaltar que si un activo puede ser indiscriminadamente desechado sin causar un impacto previsible a la empresa en ninguna de las tres (3) dimensiones de seguridad evaluadas, en general no se debe considerar como un activo de información pues no tiene valor alguno para la empresa y no requiere ser protegido (El activo es de valor despreciable).

Una vez se valore cada una de las dimensiones de seguridad por separado para cada activo superior (con valor propio) respecto al listado de impactos, se debe documentar en el R-GSI-001 el valor cualitativo del activo y su correspondiente valor cuantitativo en $ USD de acuerdo con el documento I-GSI-001. Por otro lado, la determinación del valor cuantitativo de los

activos inferiores se debe realizar sumando los correspondientes valores de sus activos superiores y con base en el valor resultante se debe determinar el valor cualitativo de dicho activo de acuerdo a los rangos estipulados en la tabla 8. Así mismo, la selección de impactos de cada activo inferior será la acumulación de los impactos más altos que apliquen a sus activos superiores. Lo anterior debe ser registrado en el documento R-GSI-001.
En este punto, la matriz de activos de información solo debería tener pendiente diligenciar los campos asociados con la clasificación del activo, para lo que debemos seguir las instrucciones dadas en el siguiente numeral.

A manera de ejemplo sobre la actividad de valoración de activos en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.3. Cómo clasificar activos de información

Posteriormente a la etapa de valoración se debe asociar un nivel de clasificación a cada uno de los activos de información en cada una de las dimensiones de seguridad establecidas en la empresa. Esta clasificación permite entre otras, conocer las necesidades de protección de los activos y permitirá priorizar la implementación de medidas de control de acuerdo con dichas necesidades. En la tabla siguiente se aprecia la relación que existe entre el valor del activo y su clasificación en cuanto a Confidencialidad, Integridad y Disponibilidad.

<table>
<tr><th rowspan="2">VALOR CUALITATIVO</th><th colspan="3">CLASIFICACIÓN</th></tr>
<tr><th>CONFIDENCIALIDAD</th><th>INTEGRIDAD</th><th>DISPONIBILIDAD</th></tr>
<tr><td>Extremo</td><td rowspan="2">CONFIDENCIAL</td><td rowspan="2">ALTA</td><td rowspan="2">MISIÓN CRÍTICA</td></tr>
<tr><td>Muy Alto</td></tr>
<tr><td>Alto</td><td rowspan="3">USO INTERNO</td><td rowspan="2">MEDIA</td><td rowspan="2">CRÍTICA</td></tr>
<tr><td>Medio</td></tr>
<tr><td>Bajo</td><td rowspan="2">BAJA</td><td rowspan="2">NO CRÍTICA</td></tr>
<tr><td>Despreciable</td><td>PÚBLICO</td></tr>
</table>

Tabla 10. Relación entre el valor del activo y su clasificación

En General, cuando el valor del activo es Extremo o Muy Alto, la clasificación será la más alta posible en cada dimensión, así mismo si el valor del activo en cada dimensión es Alto o Medio, la clasificación será intermedia, y cuando el valor del activo sea Bajo o Despreciable la clasificación será la menor posible, excepto para la dimensión de Confidencialidad (Ver nota inferior). Esto debe ser analizado por cada una de las dimensiones de forma independiente pues es posible que un mismo activo tenga valores diferentes por cada una de sus dimensiones, y por ende tenga requisitos de protección (clasificación) diferentes por cada dimensión.

Nota: La clasificación menor posible en la dimensión de confidencialidad (Público) implica que el activo puede ser conocido por el público en general, y para ello se requiere que no exista un impacto previsible al momento de una divulgación no autorizada. Lo anterior implica que el único valor del activo que haría viable una divulgación general del activo es “Despreciable”, y el valor “Bajo” se asocia al nivel de confidencialidad “Uso Interno” dado que aún genera impactos para la empresa ante una posible divulgación del activo.

Finalmente, es necesario diligenciar el respectivo valor de los campos de clasificación para las dimensiones de confidencialidad, integridad y disponibilidad de la matriz de activos de información (documento R-GSI-001) de acuerdo al valor cualitativo seleccionado para cada activo en cada dimensión y basado en la relación dada en la tabla 9.

A manera de ejemplo sobre la actividad de clasificación de activos en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.4. Identificación de Amenazas

El siguiente paso del método de análisis de riesgos consiste en identificar las posibles amenazas que puedan llegar a afectar a cada uno de los activos de información identificados. La definición acuñada en la empresa fue extraída de la definición dada al término "Amenaza" en la norma UNE 71504:2008 y en el mismo método MAGERIT. Veamos:

> **Amenaza:**
> *"Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización"*
> [UNE 71504:2008]

Así mismo se han acuñado al interior de la empresa el catálogo de amenazas incluido en el libro 2, numeral 5 de MAGERIT V3[10]. Dichas amenazas pueden ser categorizadas de la siguiente manera:

- **De origen natural:** Accidentes naturales (terremotos, inundaciones, etc.).
- **Del entorno:** Desastres industriales (contaminación, fallos eléctricos, etc.)
- **Defectos de las aplicaciones:** Corresponden a las llamadas vulnerabilidades técnicas propias del diseño o implementación del sistema.
- **Causadas por las personas de forma accidental:** Causadas típicamente por errores u omisiones no intencionales.
- **Causadas por las personas de forma deliberada:** Incluyendo ataques deliberados; ya sea con el ánimo de beneficiarse a sí mismo, beneficiar a otros, o para causar daños y perjuicios a la empresa.

Vale la pena resaltar que las amenazas afectan a los activos dependiendo de su tipificación, al igual que lo hace dependiendo de cada dimensión de seguridad. Las amenazas que apliquen a la organización (extraídas de MAGERIT) deben ser relacionadas una a una en la primera columna de la parte 2 del documento R-GSI-001, denominada "Riesgo inherente".

Posteriormente, en el mismo documento se deberá registrar la forma en la que cada amenaza puede llegar a afectar cada uno de los activos de la organización.

[10] El listado de amenazas puede ser consultado o descargado en el libro II de MAGERIT "Catálogo de elementos" a través del portal http://administracionelectronica.gob.es en el área de descargas.

A manera de ejemplo sobre la actividad de identificación de amenazas en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.5. Valoración de Amenazas (Frecuencia e Impacto)

Es necesario valorar inicialmente la frecuencia de ocurrencia de una amenaza para cada activo por cada dimensión de seguridad sin tener en cuenta la aplicación de controles (actuales o futuros), para ello se debe establecer una escala de valores de frecuencia de ocurrencia de la amenaza por año, teniendo en cuenta 6 posibles valores frecuencias (cantidad de veces que podría materializarse la amenaza en el transcurso del año).

Frecuencia		
Descripción	**Valor**	**Valor anual**
Muy frecuente	1 vez al mes	12
Frecuente	1 vez al trimestre	4
Normal	1 vez al año	1
Poco Frecuente	1 vez cada 4 años	0,25
Muy poco frecuente	1 vez cada 10 años	0,1

Tabla 11. Criterios para calificar la frecuencia de ocurrencia de una amenaza

El valor de la probabilidad se debe registrar por cada amenaza respecto a cada activo en el documento R-GSI-001 en su parte 2, en cada una de las celdas donde aparece la frase “Frecuencia (Anual)”.

Adicionalmente es necesario determinar el impacto que generará a la empresa la eventual materialización de cada amenaza sobre cada activo. Dicho impacto será calculado con base en la degradación del activo, es decir, el porcentaje (%) del valor del activo que se pierde por la materialización de una amenaza. Esta labor debe realizarse por cada amenaza en cada una de las dimensiones de seguridad y para cada activo, y debe registrarse en el documento R-GSI-001 en su parte 2, en cada una de las celdas donde aparece la frase “Degradación (%)”.

En la siguiente tabla se muestra una escala cualitativa y cuantitativa con los diferentes índices de degradación asumidos para la metodología de la empresa.

Degradación del activo		
Descripción	**Rango de valores**	**Valor**
Muy Alta	80% - 100 %	100 %
Alta	50 % - 80%	80 %
Media	25 % - 50 %	50 %
Baja	10% - 25 %	25 %
Muy Baja	< 10 %	10 %

Tabla 12. Criterios para la evaluación de la degradación del activo

Una vez se ha estimado el valor de la degradación para cada posible amenaza sobre un determinado activo, es necesario estimar el valor del impacto, es decir, la pérdida en la que incurriría la organización ante una eventual materialización de determinada amenaza. Dicho impacto se puede valorar de forma cualitativa o cuantitativa, siendo esta última la multiplicación numérica del valor del activo en $USD y el porcentaje de degradación del activo. Este cálculo se debe registrar por cada activo respecto a cada amenaza en el documento R-GSI-001 en su parte 2, en cada una de las celdas donde aparece la palabra “IMPACTO”.

Por otro lado, si se desea conocer de forma cualitativa el impacto, se puede utilizar la siguiente tabla que relaciona el valor del activo y su posible degradación.

IMPACTO	**Degradación del activo**				
Valor del Activo	**Muy Baja 10%**	**Baja 25%**	**Media 50%**	**Alta 80%**	**Muy Alta 100%**
Extremo US $ 500.000	Medio $50.000	Alto $125.000	Muy Alto $250.000	Muy Alto $400.000	Muy Alto $500.000
Muy alto US $ 200.000	Bajo $20.000	Medio $50.000	Alto $100.000	Alto $160.000	Muy Alto $200.000
Alto US $ 75.000	Bajo $7.500	Bajo $18.750	Medio $37.500	Medio $60.000	Alto $75.000
Medio US $ 25.000	Bajo $2.500	Bajo $6.250	Bajo $12.500	Bajo $20.000	Medio $25.000
Bajo US $ 2.500	Muy Bajo $250	Muy Bajo $625	Muy Bajo $1.250	Muy Bajo $2.000	Bajo $2.500
Despreciable US $ 100	Muy Bajo $10	Muy Bajo $25	Muy Bajo $50	Muy Bajo $80	Muy Bajo $100

Tabla 13. Determinación cualitativa del impacto

En general se observa que existen cinco (5) posibles niveles de impacto: Muy Alto, Alto, Medio, Bajo y Muy Bajo.

A manera de ejemplo sobre la actividad de valoración de amenazas en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.6. Determinación del Riesgo Inherente

Finalmente, para determinar el impacto que tiene sobre la empresa la materialización de una amenaza, teniendo en cuenta la frecuencia con la que esto podría ocurrir en un (1) año y sin considerar los posibles controles implementados para mitigarlo, es decir, para determinar la medida del riesgo inherente, es necesario establecer una relación para cada activo entre la probabilidad de ocurrencia y el impacto que podría causar la materialización de cada amenaza en cada una de las dimensiones de seguridad analizadas para el activo.

La empresa ha determinado que realizará estimaciones cualitativas y cuantitativas del riesgo inherente, siendo esta última la multiplicación numérica entre la probabilidad y el valor en $USD calculado previamente del Impacto de cada amenaza en cada activo. Este cálculo se

debe registrar por cada activo respecto a cada amenaza en el documento R-GSI-001 en su parte 2, en cada una de las celdas donde aparece la palabra “RIESGO INHERENTE # - #”.

Nota: La notación “# - #” se utiliza para identificar cada riesgo respecto a cada activo y cada amenaza. Por ejemplo, el RIESGO INHERENTE 2-4 corresponde al riesgo del activo 2 dada la posible materialización de la amenaza 4.

Por otro lado, si se desea obtener de forma cualitativa el nivel de riesgo, se debe utilizar como referencia la siguiente tabla, donde se relacionan los valores cualitativos de probabilidad e impacto.

RIESGO	PROBABILIDAD				
IMPACTO	**Muy Poco Frecuente**	**Poco Frecuente**	**Normal**	**Frecuente**	**Muy Frecuente**
Muy Alto	Apreciable	Importante	Crítico	Crítico	Crítico
Alto	Bajo	Apreciable	Importante	Crítico	Crítico
Medio	Bajo	Bajo	Apreciable	Importante	Crítico
Bajo	Despreciable	Bajo	Bajo	Apreciable	Importante
Muy Bajo	Despreciable	Despreciable	Despreciable	Bajo	Apreciable

Tabla 14. Estimación cualitativa del riesgo

Visto de otra manera, es posible obtener la medida cualitativa del riesgo a partir de su valor cuantitativo, para ello se debe tomar como referencia la siguiente tabla.

RIESGO	Valor ($ USD)
Crítico	Mayor o igual a $500.000
Importante	Entre $125.000 y $499.999
Apreciable	Entre $30.000 y $124.999
Bajo	Entre $6.250 y $29.999
Despreciable	Menor a $6.250

Tabla 15. Estimación cuantitativa del riesgo

Para determinar el cálculo total del riesgo inherente anual, es necesario primero totalizar (sumar) cada uno de los riesgos inherentes causados por cada amenaza (Documentar en la columna llamada “TOTAL AÑO” del documento R-GSI-001 parte 2) y finalmente sumar dichos valores (Documentar en la celda denominada “GRAN TOTAL RIESGO INHERENTE” del documento R-GSI-001).

A manera de ejemplo sobre la actividad de valoración del riesgo inherente en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.7. Determinación del Riesgo Residual

Para determinar el riesgo residual, es decir, el valor del riesgo al que la empresa se verá sometido teniendo en cuenta los posibles controles aplicables actualmente (sin tener en cuenta planes de acción futuros), es necesario determinar primero el valor de la efectividad de los controles de seguridad, es decir, el porcentaje (%) en el que se podría reducir el riesgo, ya sea reduciendo la frecuencia de ocurrencia o el impacto (degradación), al aplicar medidas de control. Se debe tener en cuenta que el riesgo nunca va a llegar a cero (0), por lo que la disminución del impacto o frecuencia nunca será del 100%.

Disminución del nivel de degradación o la frecuencia		
Descripción	**Rango de valores**	**Valor**
Alta	60 % - 99 %	90 %
Media	40 % - 60 %	60 %
Baja	20 % - 40 %	40 %
Despreciable	< 20 %	20 %

Tabla 16. Criterios para determinar efectividad de los controles

El valor del riesgo residual debe calcularse teniendo en cuenta la posible reducción de probabilidad o impacto causada por todos los controles aplicables, realizando una multiplicación numérica entre el valor de probabilidad resultante y el valor en $USD del impacto reducido por controles. El cálculo de la reducción de probabilidad o impacto se debe registrar por cada riesgo inherente respecto a cada control en el documento R-GSI-001 en su parte 3, en cada una de las celdas donde aparecen las frases “Reducción de impacto (%) y Reducción de Frecuencia (%)”.

Para determinar el cálculo total del riesgo residual anual, es necesario primero totalizar (sumar) cada uno de los riesgos residuales producto de la aplicación de controles (Documentar en la fila llamada “TOTAL AÑO” del documento R-GSI-001 parte 3) y finalmente sumar dichos valores (Documentar en la celda denominada “GRAN TOTAL RIESGO RESIDUAL”).

A manera de ejemplo sobre la actividad de valoración del riesgo residual en un proceso se pueden tener en cuenta los anexos 10 (Lista de chequeo) y 11 (Documento R-GSI-001 diligenciado).

10.8. Aceptación del Riesgo

El comité de seguridad de la información de la empresa ha definido que todos los riesgos cuya evaluación cualitativa sea superior o igual a “Importante” deben ser tratados de forma inmediata. Así mismo determina que los riesgos cuya evaluación resulte como “Apreciable” deben contar por lo menos con un plan de tratamiento de riesgo a mediano plazo y los riesgos definidos como de impacto igual o inferior a “Bajo” deberían contar con mediciones periódicas para garantizar que se mantengan en dichos niveles y podrán ser aceptados por la empresa sin definir acciones a corto o mediano plazo para su remediación.

11. DECLARACIÓN DE APLICABILIDAD

La empresa ha determinado aquellos controles que serán de aplicación para la protección de sus activos y los ha documentado en la declaración de aplicabilidad (SOA[11]).

El marco utilizado como base para la declaración de aplicabilidad se puede apreciar en la tabla 17, y el documento completo fue codificado como R-GSI-002 (Ver anexo 8). Este documento incluye un campo que indica si el control es de aplicación en la empresa, la justificación con la que se determinó si el control es de aplicación en ésta y algunas referencias adicionales como por ejemplo la documentación asociada a cada control.

Controles ISO 27001				APLICABILIDAD			
Tipificación	# Sección	Nombre	Descripción/Objetivo	Aplica (SI/NO)	Justificación	Descripción del control en la empresa	Referencias

Tabla 17. Marco utilizado para la declaración de aplicabilidad (SOA)

[11] Del inglés Statement Of Applicability

12. GESTIÓN DE INDICADORES

De acuerdo al nivel de madurez actual en seguridad de la información de la empresa, el comité de seguridad de la información revisó y aprobó veintidós (22) indicadores asociados a los controles y requisitos generales de las normas ISO 27001 e ISO 27002.

Los indicadores definidos se encuentran consolidados en un documento codificado como R-GSI-003 (Ver anexo 9), los cuales están asociados a los controles y requisitos de la ISO 27001. Para cada indicador se incluye la siguiente información:

- Nombre del indicador: Nombre breve alusivo al indicador o métrica definida
- Descripción /Objetivo: Descripción breve del propósito u objetivo del indicador
- Fórmula de medida: Indica la forma en la que se calcula el indicador con base en los datos recolectados
- Unidades de medida: Unidades en las que se presenta el indicador. v.gr. Porcentaje, # de eventos, etc.
- Frecuencia de medición: Frecuencia con la que se calculan los indicadores por el responsable de cada medición
- Frecuencia de Reporte: Frecuencia con la que se presentan los indicadores al comité de seguridad de la información
- Responsable de la medida: Se indica el cargo del responsable
- Valor objetivo: Es el valor que la empresa considera adecuado
- Valor Umbral: Es el valor por debajo del que la empresa debe tomar acciones correctivas inmediatas

Los indicadores son medidos por diversas personas y en diversos puntos de la organización dependiendo del tipo de control que se deba medir o del tipo de indicador que se pretenda obtener. Dichos indicadores deben ser presentados en la periodicidad definida al comité de seguridad de la información, quien está en la responsabilidad de establecer los planes de acción que considere adecuados y tomar las decisiones requeridas para cumplir los objetivos trazados.

13. PLAN DE TRATAMIENTO DE RIESGOS

Parte esencial del Sistema de Gestión de Seguridad de la Información es el plan que se debe elaborar para aumentar la efectividad de los controles y la inclusión de nuevos controles que permitan mitigar los riesgos previamente identificados y valorados, llevándolos a niveles razonables (Aceptables o transferibles a terceros).

Dicho plan incluye la implementación de proyectos de seguridad de la información enfocados principalmente en la mitigación de riesgos, agregando nuevos controles o mejorando los actuales, y a su vez, permitirán aumentar el nivel de madurez de Seguridad de la información en la empresa.

Inicialmente se han definido diez y siete (17) proyectos, que podrán desarrollarse en un plazo corto, medio o largo dependiendo de los recursos requeridos y de su complejidad, los cuales se encuentran relacionados en el documento R-GSI-005 parte 1, icluyendo el título asignado, una breve descripción que incluye el alcance de cada proyecto, el responsable de su implementación, el área funcional encargada entre otras del levantamiento de requerimientos y de las condiciones de satisfacción, el presupuesto de inversión requerido (en dólares), el plazo para su implementación y el número de recursos de personal requeridos de tiempo completo y de dedicación parcial. A continuación se relacionan los títulos de los proyectos categorizados por su tiempo de implementación:

- **Proyectos a corto plazo**: Implementación menor a 3 meses.

    1. Borrado seguro
    2. Cifrado de discos
    3. Rediseño del Modelo de Capacitación y Concientización de SI
    4. Intercambio seguro de información con terceros
    5. Optimización, Corrección y Ampliación del monitoreo de Bases de Datos
    6. Gestión de llaves, criptogramas, contraseñas y monitoreo de cuentas de superusuarios
    7. Políticas de Seguridad de la Información

    Ver cronograma detallado en el Anexo 13 Fase 1. Cronograma de proyectos de implementación a corto plazo.

- **Proyectos a mediano plazo**: Implementación menor a 1 año.

    1. Segregación de redes
    2. Seguridad perimetral en profundidad
    3. Análisis interno de vulnerabilidades
    4. Herramientas avanzadas de Seguridad de EndPoint

    Ver cronograma detallado en el Anexo 13 Fase 2. Cronograma de proyectos de implementación a mediano plazo.

- **Proyectos a largo plazo**: Implementación entre 1 y 3 años.

  1. Gestión de dispositivos móviles
  2. IDM (Identity Management)
  3. DLP (Data loss Prevention)
  4. NAC (Network Access Control)
  5. Correlacionador de eventos
  6. PCN y DRP

  Ver cronograma detallado en el Anexo 13 Fase 3. Cronograma de proyectos de implementación a largo plazo.

Dado que uno de los principales objetivos de los proyectos es la mitigación de riesgos, generando mejoras en los controles, en el documento R-GSI-005 parte 2 se ha elaborado una relación entre los controles del anexo A de la ISO 27001 y los proyectos planteados, destacando una mejora sustancial en el nivel de implementación de sesenta y dos (62) controles y nueve (9) requerimientos generales de la ISO 27001.

El aumento en el nivel de implementación de los controles implica una mejora general de cada uno de los dominios de la ISO 27001. Dicha mejora puede ser comparada contra el nivel de implementación realizado en el análisis diferencial inicial (Tablas 3 y 4, figuras 5 y 6 del numeral 4 del presente trabajo), sin embargo, dicho análisis fue realizado antes de dar inicio al plan de implementación del SGSI y por ende no incluye algunos aspectos que han mejorado en el transcurso de dicho plan. Dado lo anterior, y para determinar con mayor veracidad la mejora causada exclusivamente por los proyectos, fue necesario realizar una actualización al análisis diferencial, la cual se encuentra en el anexo 1 – Segundo análisis diferencial.

Una vez realizado el segundo análisis diferencial, se procedió a documentar cada una de las mejoras en el grado de implementación de los requerimientos generales de ISO 27001 y los controles de ISO 27002, obteniendo los siguientes resultados (Ver documento R-GSI-005 parte 4 – Resumen).

- En cuanto a la evaluación realizada del cumplimiento de los requisitos generales de la ISO 27001, en el segundo análisis diferencial se obtuvo que en promedio el 66% de éstos se encuentran implementados en la empresa. Al culminar la implementación de los proyectos, se espera que lleguen a un 84% (Ver tabla 18).

Implementación de Requisitos Generales ISO 27001	% de Implementación	
	Antes de Proyectos	Después de Proyectos
	66%	84%

Tabla 18. Mejora en la implementación de requisitos generales de la ISO 27001 por los proyectos

- El porcentaje de implementación de cada uno de los dominios de la norma ISO 27002 (Anexo A ISO 27001) en general aumentará para todos los dominios una vez se culminen los proyectos planteados. A continuación se muestra el estado de los dominios obtenido en el segundo análisis diferencial y la mejora esperada al implementar los proyectos planteados (ver tabla 18).

# Sección	Nombre	% de Implementación	
		Antes de Proyectos	Después de Proyectos
A.5	Política de Seguridad	65%	100%
A.6	Aspectos Organizativos de la Seguridad de la Información	46%	71%
A.7	Gestión de Activos	62%	88%
A.8	Seguridad Ligada a los Recursos Humanos	76%	89%
A.9	Seguridad Física y del Entorno	77%	92%
A.10	Gestión de Comunicaciones y Operaciones	64%	89%
A.11	Control de Acceso	46%	70%
A.12	Adquisición,Desarrollo y Mantenimiento de Sistemas de Información	43%	63%
A.13	Gestión de Incidentes de Seguridad de la Información	38%	69%
A.14	Gestión de la Continuidad del Negocio	8%	100%
A.15	Cumplimiento	60%	72%
TOTAL SGSI		53%	82%

Tabla 19. Mejora en la implementación de dominios ISO 27001 por los proyectos

La relación mostrada anteriormente en la tabla 18 puede ser representada ya sea en un diagrama de barras (ver figura 10) o mediante un diagrama de radar (ver figura 11). En ambos casos se puede visualizar de forma simple la mejora que traerá en cada dominio la implementación del plan de tratamiento de riesgos (proyectos de seguridad).

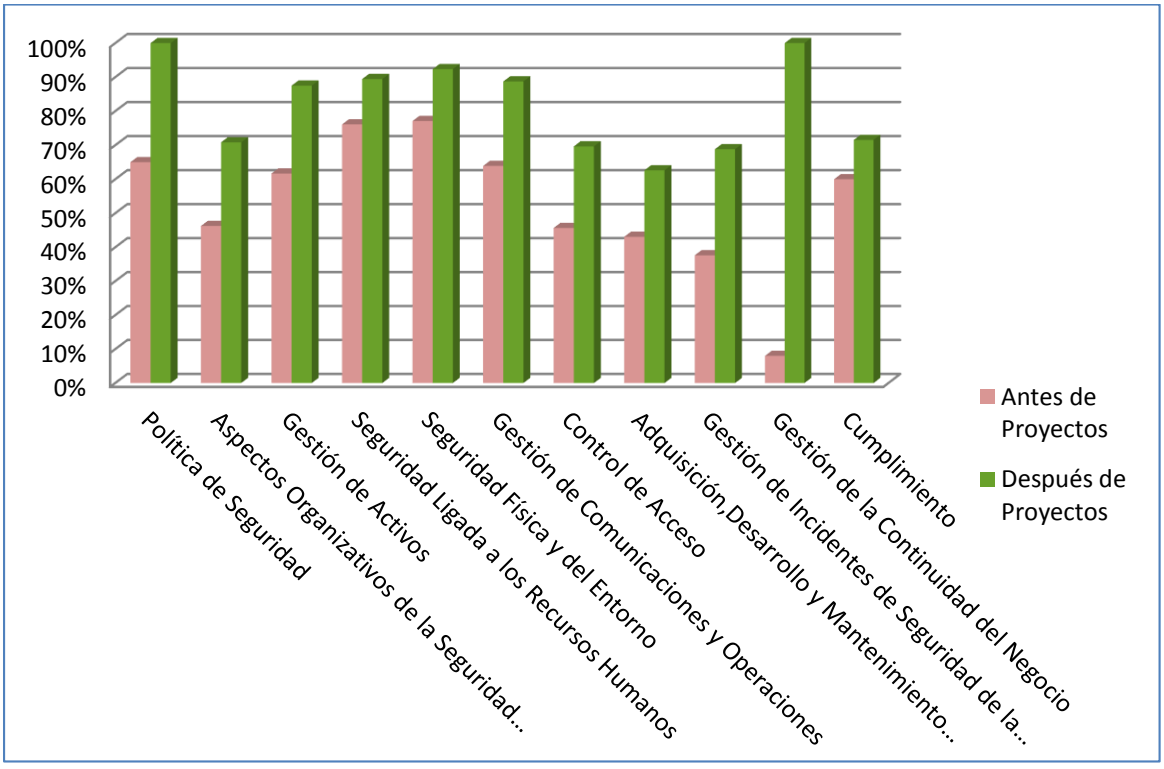


Figura 10. Diagrama de barras de la mejora causada en dominios ISO 27002 por proyectos de SI

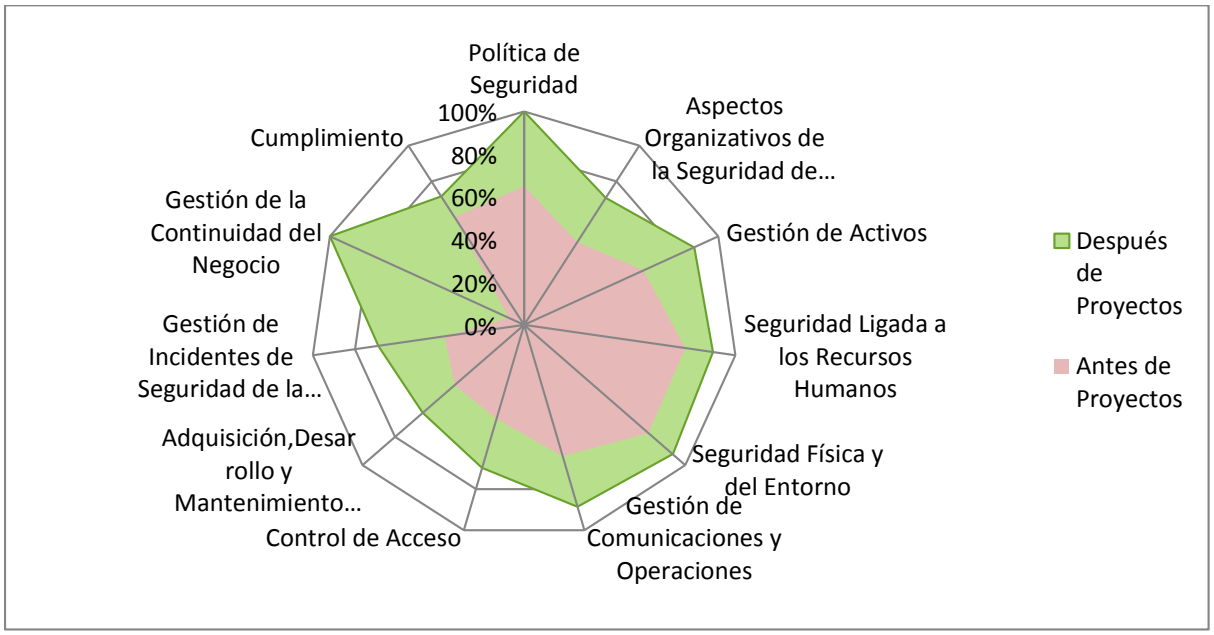


Figura 11. Diagrama de radar de la mejora causada por proyectos en la implementación de dominios ISO 27002

Adicional a lo anterior, es necesario validar que los proyectos planteados conllevarán a una mejora en los riesgos residuales identificados. Para ello, en el documento R-GSI-005 parte 3 se plantean una actualización al análisis de riesgos realizado anteriormente, mostrando principalmente la variación del riesgo residual asociada a los cambios en los controles de seguridad, resultado de la implementación de los proyectos planteados en el plan de tratamiento de riesgos.

En general se observa que al implementar los proyectos, la eficacia de los controles en la mitigación del riesgo se incrementa, lo que conlleva a una posible reducción de la frecuencia de ocurrencia de una amenaza o a un aumento en la reducción el impacto de la amenaza. A continuación se relacionan algunos controles que reportan una mejora en su eficacia para mitigar riesgos:

- **A.10.6.1. Controles de red:** Aumenta su efectividad en la reducción de la frecuencia de ocurrencia del 20% al 90% para amenazas como el “Acceso no autorizado” y la “Difusión de software dañino”.

- **A.11.6.1. Restricción del acceso a la información:** Aumenta su efectividad en la reducción de la frecuencia de ocurrencia y el impacto de amenazas como el “Abuso de privilegios de acceso” y la “Difusión de software dañino” de un 40% a un 60%. Así mismo aumenta de un 40% a un 90% la reducción de la frecuencia de ocurrencia del “Acceso no autorizado”.

- **A.8.2.2. Concienciación, formación y capacitación en seguridad de la información:** Aumenta su efectividad en la reducción de la frecuencia de ocurrencia de todas las amenazas documentadas de un 20% a un 60%.

Adicional a lo anterior, se observa que en el análisis de riesgos aparecen controles adicionales que permitirán aportar cierto nivel de mitigación a los riesgos detectados. Entre ellos se destacan:

- **A.14.1.3. Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información**: Este nuevo control permitirá reducir el impacto de amenazas como "Abuso de privilegios de acceso", "Difusión de software dañino", "Fuego", "Daños por agua" y "Desastres industriales".

- **A.11.4.6. Control de la conexión a la red:** Este nuevo control permitirá reducir la probabilidad de ocurrencia de amenazas como "Acceso no autorizado" y "Difusión de software dañino".

Finalmente, se destaca una amplia reducción del riesgo en la organización, el cual pasaría de un gran total de **$10.463.590 (USD)** a tan solo **$928.954 (USD)** anuales.

Con los valores anteriores es posible obtener importantes datos asociados con el retorno de la inversión de los proyectos de seguridad propuestos. Al valor de pérdidas posibles por materialización de riesgos en un año se le conoce como ALE (Annual Loss Expectancy) y el retorno de inversión para la empresa causado por las inversiones de seguridad se denomina ROSI (Return Of Security Investment). A continuación se muestra el cálculo del ROSI y adicionalmente se estimará la cantidad de años que tardará la empresa en recuperar dicha inversión:

ALE = $10.463.590 (USD)
ALE incluyendo proyectos (ALE_{nuevo}) = $928.954 (USD)
Costo Total Proyectos = $1.320.000 (USD)
Ahorro anual por riesgos no materializados = ALE - ALE_{nuevo} = $9.534.636 (USD)

Con los datos anteriores es posible determinar la cantidad de años que le tomaría a la empresa recuperar la inversión realizada en el plan de tratamiento de riesgos (Proyectos de seguridad):

Años de retorno de inversión = (Costo Total Proyectos) / (Ahorro anual por riesgos no materializados)
Años de retorno de inversión = $1.320.000 / $9.534.636 = 0,14 años

Lo anterior significa que en menos de 1 año (0,14 años) la empresa vería claramente el retorno de la inversión de los proyectos de seguridad planteados[12]. Por otro lado, para calcular la tasa de retorno de la inversión (ROSI) se utilizará la siguiente fórmula:

ROSI = (ALE – ALE_{nuevo} – Costo Total Proyectos) / Costo Total Proyectos
ROSI = ($9.534.636 - $1.320.000) / $1.320.000
ROSI = 6,223

El ROSI obtenido es del 6,223, es decir que la tasa de retorno de inversión es del 622,3%, lo que indica que los proyectos son altamente rentables a través del tiempo.

[12] Asumiendo que todos los proyectos fueran implementados en el mismo año

14. INFORME DE AUDITORÍA INTERNA DE CUMPLIMIENTO

14.1. Introducción

En el presente informe se plasman los resultados de la auditoría efectuada sobre los procesos incluidos en el alcance del SGSI, como preparación para la obtención de la certificación ISO 27001:2005. Adicionalmente se presenta de forma estructurada y ordenada los resultados de la evaluación del nivel de madurez de seguridad de la información realizado para los controles de seguridad de acuerdo a la norma ISO 27002. En el anexo 14 del presente trabajo se incluye el detalle de dicho análisis.

Los hallazgos realizados fueron priorizados y son presentados de forma ordenada de acuerdo a la siguiente escala de impactos establecida en común acuerdo con la empresa durante la reunión de inicio:

Clasificación	Tipo de Hallazgo		Cantidad de Hallazgos
Informativo	Fortalezas identificadas	Corresponde a aquellos puntos identificados como muy positivos por la auditoría y sobre los cuales la empresa debería enfocarse en mantener a través del tiempo.	6
Impacto Alto	No Conformidad Mayor	Se debe brindar atención inmediata, estableciendo planes de acción a corto plazo. Por su severidad implican la no obtención de la certificación ISO 27001.	2
Impacto Medio	No Conformidad Menor	Se deben establecer planes de acción a corto y mediano plazo. Implican un aplazamiento en la obtención de la certificación ISO 27001.	11
Impacto Bajo	Oportunidad de Mejora	Se recomienda establecer planes de acción a mediano y largo plazo. Corresponden a las recomendaciones del auditor sobre algunos aspectos que el auditor encuentra conforme a la norma pero que podrían ser mejoradas para elevar el nivel de madurez de seguridad de la empresa y reducir los riesgos asociados.	4

Tabla 20. Clasificación de hallazgos de auditoría

Los objetivos y el alcance de la presente auditoría fueron:

- Identificar el grado de cumplimiento del Sistema de Gestión de Seguridad de la Información respecto a la norma ISO 27001:2005 para los procesos “Venta de Productos y Servicios por Internet” y “Recibo, Alistamiento y Despacho de Mercancía”, incluyendo sus procesos de apoyo.

- Verificar en sitio la correcta implementación de los controles definidos en la declaración de aplicabilidad de acuerdo con el alcance del SGSI.

- Realizar una evaluación del nivel de madurez de los controles de seguridad de la información, tomando como base la norma ISO 27002 y la declaración de aplicabilidad de la empresa.

14.2. Metodología empleada

Los hallazgos presentados fueron identificados con base en la revisión de los requisitos de la norma ISO 27001:2005 y con base en la verificación de la implementación de los controles declarados en el documento SOA realizada en sitio. Adicionalmente se efectuó una revisión a alto nivel de la madurez en seguridad de la información de la empresa, respecto a los dominios de la norma ISO 27002 y teniendo como referencia el esquema de valoración de madurez CMM.

En esta primera auditoría de cumplimiento previa a una posible obtención del a certificación ISO 27001:2005 se realizó una validación completa de los controles de acuerdo a la declaración de aplicabilidad, y se espera que para auditorías internas posteriores se realicen validaciones parciales, separando la totalidad de los controles en un plazo de tres (3) años.

A continuación se presentan las fases abarcadas en la presente auditoría:

Fase 1. Recolección de información

El principal objetivo de esta fase fue obtener la mayor cantidad de información asociada con el Sistema de Gestión de Seguridad de la Información de “Tu Hogar con Estilo S.A.”, recolectar la documentación asociada y efectuar la asignación de recursos para cada fase de la auditoría.

Fase 2. Checklist de documentación del SGSI

Se verificó al detalle cada uno de los documentos enmarcados dentro de los requisitos de la certificación ISO 27001, incluyendo la política de seguridad de la información, el compromiso de la dirección, la declaración de aplicabilidad, el plan de tratamiento de riesgos, entre otros.

Fase 3. Ejecución de auditoría in situ a procesos dentro del alcance

Se validó la existencia, el estado de implementación y de concientización de los procedimientos y procesos asociados con el Sistema de Gestión de Seguridad de la Información en los siguientes procesos de negocio, incluidos dentro del alcance:

- Venta de Productos y Servicios por Internet
- Recibo, alistamiento y despacho de mercancía
- Gestión de Seguridad de la Información
- Seguridad de los recursos informáticos
- Gestión de estrategia de negocio
- Selección, contratación y novedades de personal
- Seguridad de las instalaciones

Fase 4. Verificación de eficacia de controles

Se validó la implementación de los controles estipulados en el documento SOA (declaración de aplicabilidad) para los procesos y en las instalaciones físicas incluidas en el alcance del SGSI.

Fase 5. Análisis de información recopilada

Se analizaron los documentos recibidos y las evidencias recolectadas para determinar el estado general de seguridad de la información (Nivel de madurez) y se documentaron y clasificaron los hallazgos.

Fase 6. Elaboración, presentación y entrega del informe de auditoría

Fase estimada para la elaboración del informe de auditoría y su respectiva concertación con las áreas de seguridad previa formalización y presentación a la dirección.

14.3. Resultados de la evaluación del nivel de madurez de seguridad de la información en la empresa

La valoración del nivel de madurez fue realizada para cada control de la declaración de aplicabilidad, la cual se encuentra basada en ISO 27002, teniendo en cuenta las entrevistas realizadas a los responsables de los procesos junto con las visitas in situ realizadas por los auditores y expertos técnicos que apoyaron la labor de auditoría. El resultado acumulado mostrado en la tabla 21 corresponde al promedio matemático de cada uno de los objetivos de control que lo componen, que a su vez se calculó con el promedio de los valores de efectividad (madurez porcentual) de cada uno de los controles que lo componen.

# Sección	Nombre	Efectividad (%)	Nivel de Madurez	Nivel de Madurez (CMM)
A.5	Política de Seguridad	91%	4	Gestionado y medible
A.6	Aspectos Organizativos de la Seguridad de la Información	58%	3	Proceso definido
A.7	Gestión de Activos	63%	3	Proceso definido
A.8	Seguridad Ligada a los Recursos Humanos	78%	3	Proceso definido
A.9	Seguridad Física y del Entorno	73%	3	Proceso definido
A.10	Gestión de Comunicaciones y Operaciones	68%	3	Proceso definido
A.11	Control de Acceso	56%	3	Proceso definido
A.12	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	48%	2	Reproducible, pero intuitivo
A.13	Gestión de Incidentes de Seguridad de la Información	44%	2	Reproducible, pero intuitivo
A.14	Gestión de la Continuidad del Negocio	8%	1	Inicial / Ad-hoc
A.15	Cumplimiento	57%	3	Proceso definido
TOTAL SGSI		**59%**	**3**	**Proceso definido**

Tabla 21. Resultado de la evaluación del nivel de madurez por dominios ISO 27002

En la tabla anterior se puede observar que en la mayoría de los dominios la empresa se encuentra por encima del nivel tres (3) de madurez, es decir que cuenta con la mayoría de los procesos requeridos con un nivel como mínimo "Definido", prueba de ello es que el promedio de madurez del SGSI en su conjunto es equivalente a dicho nivel de madurez. Sin embargo se encontraron serias debilidades en los dominios de "Adquisición, Desarrollo y Mantenimiento de Sistemas de Información" y "Gestión de Incidentes de Seguridad de la Información" y una ausencia casi completa de procesos y controles en el dominio de "Gestión de la Continuidad del Negocio".

A pesar de que la empresa se encuentra actualmente con unos planes de acción definidos, los cuales se plasmaron en el plan de tratamiento de riesgos, la auditoría recomienda que dichos planes sean priorizados para ajustar la empresa en el menor tiempo posible al cumplimiento requerido por la certificación ISO 27001.

El mismo análisis anterior puede ser visto en las siguientes figuras, que corresponden a la representación en un diagrama de radar y en un diagrama de barras, donde se observa la brecha existente entre los niveles actuales de madurez de seguridad de la empresa y los niveles a los que la empresa desea llegar a estar.

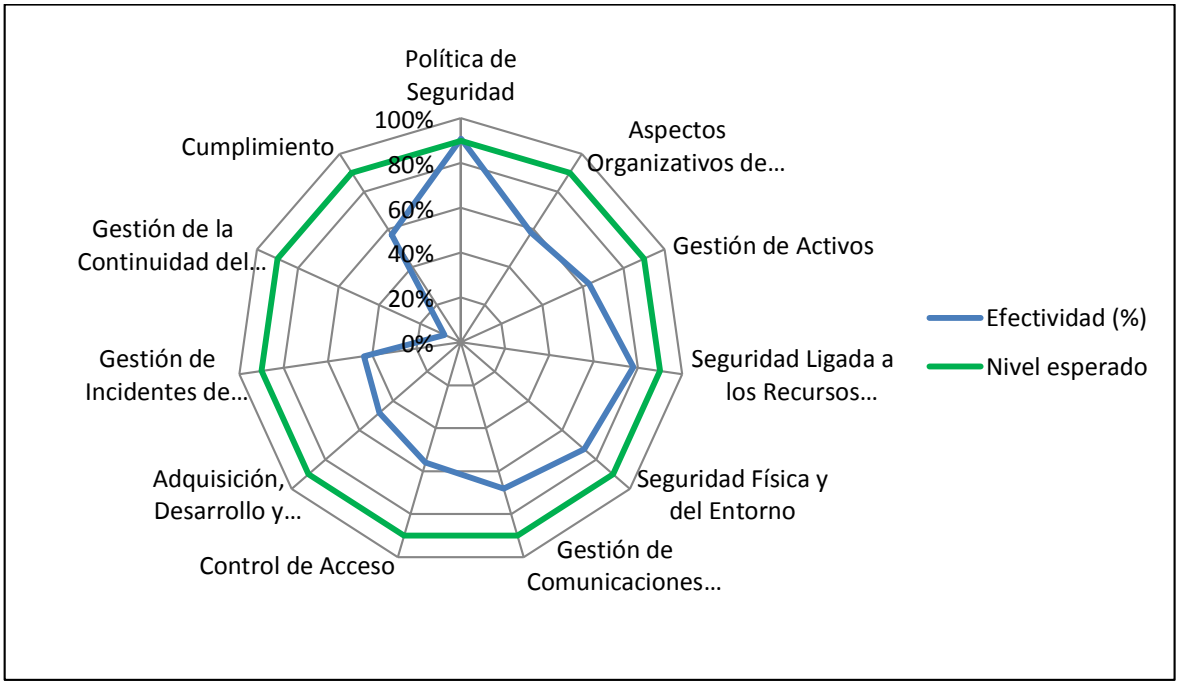


Figura 12. Diagrama de radar del nivel de madurez actual respecto al esperado (en porcentaje %)

En el diagrama de barras presentado en la figura 13 se puede observar de forma más intuitiva la diferencia entre el nivel de madurez actual de cada dominio, representado en escala CMM (0 a 5), donde vemos que la mayoría de los dominios se encuentran en nivel tres (3), sobresaliendo el dominio de política de seguridad con nivel cuatro (4) y resaltando nuevamente algunos dominios que apenas alcanzan los niveles dos (2) y uno (1).

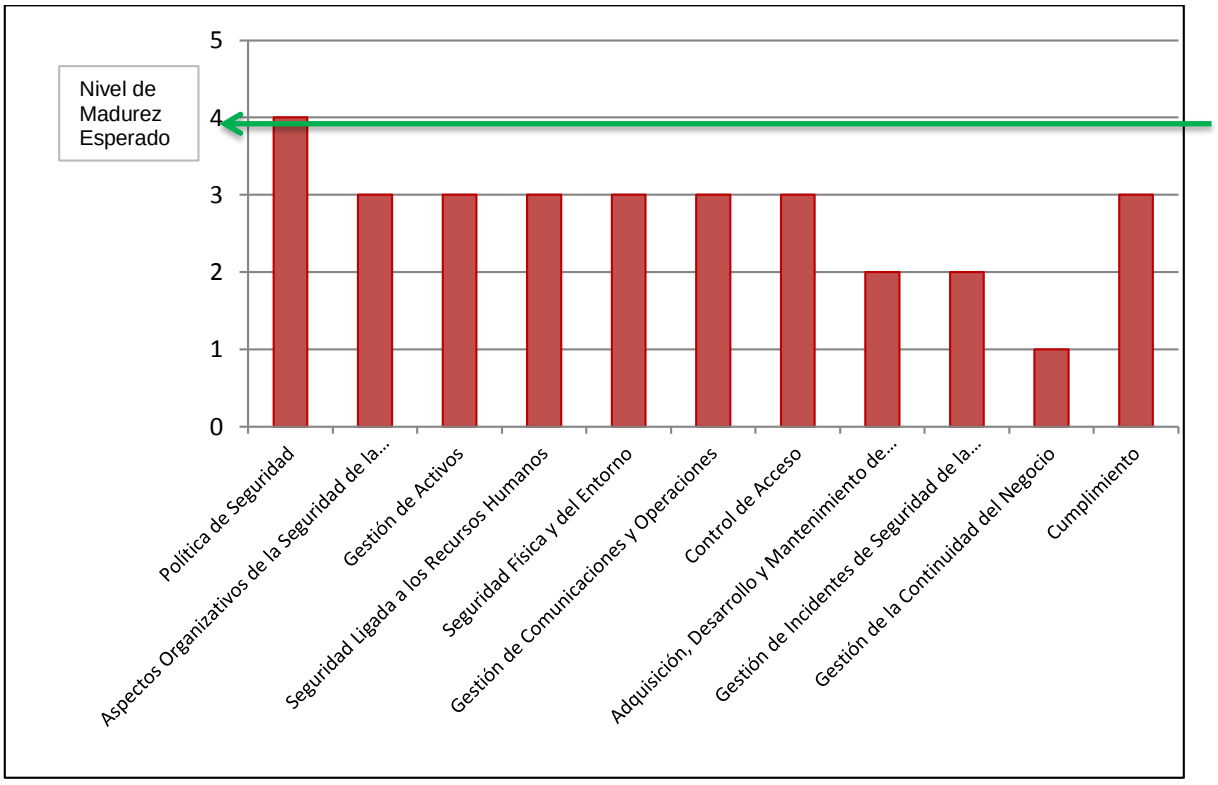


Figura 13. Nivel de madurez actual respecto al esperado (en escala CMM)

14.4. Listado detallado de los hallazgos

A continuación se relacionan los principales puntos fuertes identificados, junto con los hallazgos y oportunidades de mejora clasificados de acuerdo a su severidad:

14.4.1. Puntos fuertes: Se resaltan de forma positiva los siguientes aspectos del SGSI:

- POLÍTICA GENERAL DE SEGURIDAD: Se cuenta con la política general de SI, incluyendo los objetivos de SI y la intención de apoyo de la dirección en torno al SGSI. La política incluye la mayoría de aspectos requeridos por el SGSI y se encuentra redactada en términos comprensibles por lectores de índole no técnico.

- APOYO DE LA DIRECCIÓN: Ya se cuenta con un documento claro y aprobado por la Presidencia General que indica el apoyo de la Dirección en torno al diseño e implementación del SGSI. Se evidencia su veracidad y efectividad por las partidas presupuestales asignadas a dichos fines.

- COORDINACIÓN DE SEGURIDAD: Se cuenta con áreas formalmente establecidas con responsabilidades claras en torno a la seguridad de la información. Adicionalmente se destaca el diseño del Comité de Seguridad de la Información, integrado por los principales involucrados en Seguridad, por la alta gerencia y por el área de riesgo.

- ACCESO CONTROLADO A LA RED: Se evidencian procedimientos y controles para limitar el acceso a la red mediante el registro de la dirección MAC del PC, incluyendo red cableada e inalámbrica. Esto permite reducir de forma exitosa la mayoría de accesos no autorizados, salvo por aquellos realizados con herramientas especializadas.

- GESTIÓN DE USUARIOS Y PRIVILEGIOS: Los procesos y procedimientos asociados con la gestión de usuarios y privilegios de acceso a la información se encuentran en un estado de madurez cercano al deseado, con procesos documentados, formalizados y medidos.

- GESTIÓN DE ACTIVOS DE INFORMACIÓN: Se evidencia la existencia de un método adecuado para la gestión de activos de información y los riesgos de seguridad de la información asociados. El método destaca por su objetividad en la valoración de activos y riesgos.

14.4.2. No conformidades mayores: Se encontraron los siguientes hallazgos calificados como de impacto alto:

- PLAN DE CONTINUIDAD DEL NEGOCIO (PCN): A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se evidenció que la empresa no dispone de un plan de continuidad de negocio para sus procesos definidos en el alcance. Adicionalmente dicho proyecto se estipula para largo plazo, lo que retrasaría la certificación hasta que se implementen y validen todos los procesos, procedimientos y controles asociados. Se recomienda aumentar la prioridad de este proyecto para implementarlo en un menor plazo.

- DIVULGACIÓN, CAPACITACIÓN Y CONCIENTIZACIÓN DE SEGURIDAD: Se evidenció que la organización no tiene definida una planeación para realizar campañas masivas y periódicas de concientización a los usuarios. Adicionalmente no se encontraron registros asociados con capacitaciones ni divulgaciones asociadas al SGSI. Este es uno de los puntos clave para que el SGSI se comporte de la forma en que es planeado, dado que los usuarios son siempre los puntos más débiles de la seguridad.

14.4.3. No conformidades menores: Se encontraron los siguientes hallazgos calificados como de impacto medio:

- REVISIÓN DE LA POLÍTICA POR LA DIRECCIÓN: Se tiene definido que la revisión de la política por la dirección se hará anualmente, sin embargo aún no ha pasado el primer año desde la creación de dicha política para poder tener evidencias de la revisión realizada. Se debe hacer una primera revisión tan pronto como sea posible, para contar sus resultados al comienzo del proceso de auditoría de certificación del SGSI.

- ETIQUETADO Y MANEJO DE INFORMACIÓN: Se evidenció la ausencia de procedimientos para etiquetar y manejar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

- CONTROLES PARA PROTECCIÓN DE EQUIPOS FUERA DE LAS INSTALACIONES: Actualmente la empresa no dispone de mecanismos de control efectivos para mitigar los diferentes riesgos que conlleva trabajar fuera de las instalaciones de la organización.

- BORRADO SEGURO DE INFORMACIÓN: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo verificar que la empresa no dispone de mecanismos de borrado seguro en los procedimientos de entrega de equipos de cómputo y dispositivos de almacenamiento a terceros ya sea para su mantenimiento, reparación o disposición final.

- INTERCAMBIO DE INFORMACIÓN CON TERCEROS: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo verificar que la empresa no dispone de procedimientos y herramientas estandarizadas para efectuar intercambio de información sensible con terceros.

- CONTROL DE ENRUTAMIENTO EN LA RED: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo evidenciar que la empresa no dispone de mecanismos efectivos para controlar el enrutamiento entre las distintas redes y subredes definidas, lo que podría llevar a la materialización de riesgos asociados con acceso no autorizados y conllevar a fuga de información o modificaciones no autorizadas.

- SEGURIDAD EN DISPOSITIVOS MÓVILES: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo evidenciar que la empresa no dispone de mecanismos de control para proteger la información sensible que se encuentra en dispositivos móviles.

- SEGURIDAD EN PROYECTOS: Actualmente la empresa no cuenta con un procedimiento formalizado para aplicar controles y principios de seguridad en los proyectos y sistemas de información desde su concepción.

- GESTIÓN DE LLAVES Y CRIPTOGRAMAS: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo verificar que la empresa no dispone de mecanismos ni procedimientos para efectuar una gestión adecuada de llaves criptográficas ni contraseñas de administrador de los sistemas sensibles.

- SEGURIDAD EN LA GENERACIÓN DE DATOS DE PRUEBA: No se dispone de procedimientos ni herramientas para generar datos de prueba a partir de datos de producción, lo que ha conllevado a que en muchos sistemas de prueba se manejen datos de producción.

- ANÁLISIS DE VULNERABILIDADES: A pesar de que ya se encuentra un proyecto de implementación en curso, en el momento de la auditoría se pudo evidenciar que la

empresa no dispone de mecanismos ni procedimientos para efectuar verificaciones sobre las aplicaciones y la infraestructura crítica que permitan detectar de forma oportuna posibles vulnerabilidades de seguridad.

14.4.4. Oportunidades de mejora: Se encontraron las siguientes recomendaciones y oportunidades de mejora para el SGSI:

- CURSO VIRTUAL DE SEGURIDAD DE LA INFORMACIÓN: Se verificó la existencia de un curso virtual de seguridad de la información, sin embargo se recomienda planear una actualización, dado que la terminología empleada en dicho curso no es fácilmente entendible por personal ajeno a las áreas de seguridad y podría no ser comprensible por los usuarios.

- RESPONSABILIDADES DE SEGURIDAD: Se evidenció que la empresa cuenta con las principales responsabilidades de los involucrados en la coordinación de Seguridad de la Información, de las demás áreas involucradas, y de la comunidad en general, sin embargo se recomienda ajustar su redacción, especialmente las de los colaboradores para que sean comprensibles por la comunidad en general.

- ACUERDO DE CONFIDENCIALIDAD: Se evidenció que existen procedimientos documentados y que son aplicados de forma consistente para que todos los colaboradores contratados ya sea directamente o mediante la modalidad de Outsourcing, firmen un acuerdo de confidencialidad en el momento de la contratación. Sin embargo actualmente no se tiene claridad sobre los contratos anteriores a la implantación del SGSI, se recomienda que se efectúe una jornada masiva de aceptación para garantizar que todos cuenten con dicho acuerdo.

- USUARIO ADMINISTRADOR LOCAL: Se evidenció que en los equipos de cómputo utilizados en los procesos incluidos dentro del alcance de la certificación no cuentan con privilegios de administrador. Sin embargo se evidenció que esto no aplica de forma consistente en toda la organización, lo que podría facilitar la materialización de riesgos contra la información de la empresa, se recomienda continuar con la implementación de este control para que no solo abarque aquello que está dentro del alcance del SGSI sino que aplique para toda la organización.

14.5. Conclusiones y recomendaciones de la auditoria interna

En general se evidenció una cantidad considerable de no conformidades menores, la mayoría de ellas debidas a deficiencias en la implementación de controles puntuales del SGSI, sin embargo se evidencia que la mayoría de controles, procesos y procedimientos se encuentran implementados de forma consistente en la organización.

Se considera que todos los hallazgos identificados podrían ser solventados en un lapso de tiempo razonablemente corto, de manera que la empresa pueda optar por la certificación ISO 27001. A pesar de que se evidenció que la empresa no cuenta con un plan de continuidad del negocio implementado, ya se cuenta con un proyecto definido y cuyo presupuesto ya fue

aprobado para implementar el plan de continuidad de negocio, se recomienda asignar los recursos de personal de manera que se pueda dar prioridad y celeridad a dicho proyecto.

Por otro lado, se considera que el resultado de la evaluación del nivel de madurez de seguridad de la información en la empresa es muy satisfactorio en cuanto a que la mayoría de procesos y controles se encuentran adecuadamente "Definidos" y están a un paso de convertirse en "Gestionados y Medibles". Lo anterior permite evidenciar que los grandes esfuerzos que ha realizado la organización en la definición e implementación del SGSI han dado los resultados que la organización esperaba y que la empresa se encuentra adecuadamente encaminada para la obtención de la certificación ISO 27001:2005.

14.6. Anexos del informe de auditoria interna

El análisis detallado del nivel de madurez de seguridad de la información realizado sobre cada uno de los controles del documento SOA (Basado en ISO 27002) se encuentra codificado como R-GSI-007 y se encuentra anexo a este informe.

CONCLUSIONES

Durante el desarrollo del presente trabajo se logró obtener un avance significativo en el cumplimiento de los requisitos de la norma ISO 27001 y en el cubrimiento de los objetivos de control y dominios de la norma ISO 27002. Lo anterior se evidencia en los resultados del análisis diferencial realizado después de surtir la etapa de valoración de activos, amenazas y riesgos, donde se obtuvo un cumplimiento del 66% respecto al realizado a manera de diagnóstico inicial de la seguridad de la empresa donde el cumplimiento de requisitos era de tan solo el 19%. Por otro lado, al evaluar la seguridad de la empresa en las mismas etapas, la implementación de controles logró avanzar del 45% a un 53%.

Al culminar el plan de tratamiento de riesgos, que incluye proyectos a corto, mediano y largo plazo, se espera que la empresa alcance un cumplimiento de requisitos de la norma ISO 27001 del 84% y un cubrimiento de objetivos de control y dominios de la norma ISO 27002 del 82%. Esto evidencia la efectividad que tendrá la implementación de los proyectos de seguridad definidos en el plan de tratamiento de riesgos y permite de alguna manera sustentar la inversión realizada. Adicional a esto, se espera que la implementación de dichos proyectos permitirá reducir significativamente los riesgos y la materialización de amenazas sobre los principales activos de la empresa, estimando que de una pérdida inicial estimada de USD $10.463.590 llegaría a tan solo USD $928.954 al año.

El proceso de auditoría interna realizado permitió identificar una serie de hallazgos entre los que se pueden resaltar de forma positiva varias fortalezas y entre las que se presentan algunas oportunidades para mejorar los procesos existentes, sin embargo se debe recalcar el hallazgo de dos (2) no conformidades mayores que deben ser tratadas de forma inmediata y once (11) no conformidades menores que deberían ser mitigadas en un plazo razonable para que la empresa pueda optar por la certificación ISO 27001:2005.

Se destaca como resultado de la auditoría la recomendación orientada a dar una mayor prioridad al proyecto de implementación del plan de continuidad de negocio (PCN), que inicialmente fue concebido a un plazo de 3 años y que debería estar listo para poder obtener la certificación deseada. Con base en esta recomendación, la empresa deberá reevaluar sus prioridades y ajustar sus recursos para lograr establecer el PCN en un lapso de tiempo razonable.

BIBLIOGRAFÍA

Adicional a los conocimientos y experiencia previamente adquiridos, y al material proporcionado por el instructor de la materia, fueron requeridas las siguientes fuentes de consulta:

- Portal de información (Wiki) asociada con la ISO 27000. http://www.iso27000.es

- Norma ISO/IEC 27001, British Standards Institution. Octubre de 2005.

- Norma UNE - ISO/IEC 27002, Aenor. Diciembre de 2009.

- Modelo de Seguridad de la Información para la estrategia de gobierno en línea. Ministerio de Tecnologías de la Información y las Comunicaciones. Bogotá, diciembre de 2011. http://programa.gobiernoenlinea.gov.co/apc-aa-files/da4567033d075590cd3050598756222c/Modelo_Seguridad_Informacion_2_0.pdf

- La importancia de la Declaración de aplicabilidad para la norma ISO 27001. Dejan Kosutic, 2 de Junio de 2011. http://cxo-community.com/articulos/blogs/blogs-metodologia-legislacion/3924-la-importancia-de-la-declaracion-de-aplicabilidad-para-la-norma-iso-27001.pdf

- Métricas e indicadores de gestión. Blog de “El Asesor”, mayo de 2010. http://planeameinto-estrategico.blogspot.com/2010/05/metricas-e-indicadores-gestion.html

- Introduction to Return on Security Investment. ENISA (European Network and Information Security Agency), 2012. https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport

ANEXO 1. ANÁLISIS DIFERENCIAL RESPECTO A ISO 27001:2005

- Primer análisis diferencial: Realizado antes de iniciar el TFM
  (Ver documento adjunto “R-GSI-004. Análisis diferencial ISO 27001.xlsx”)

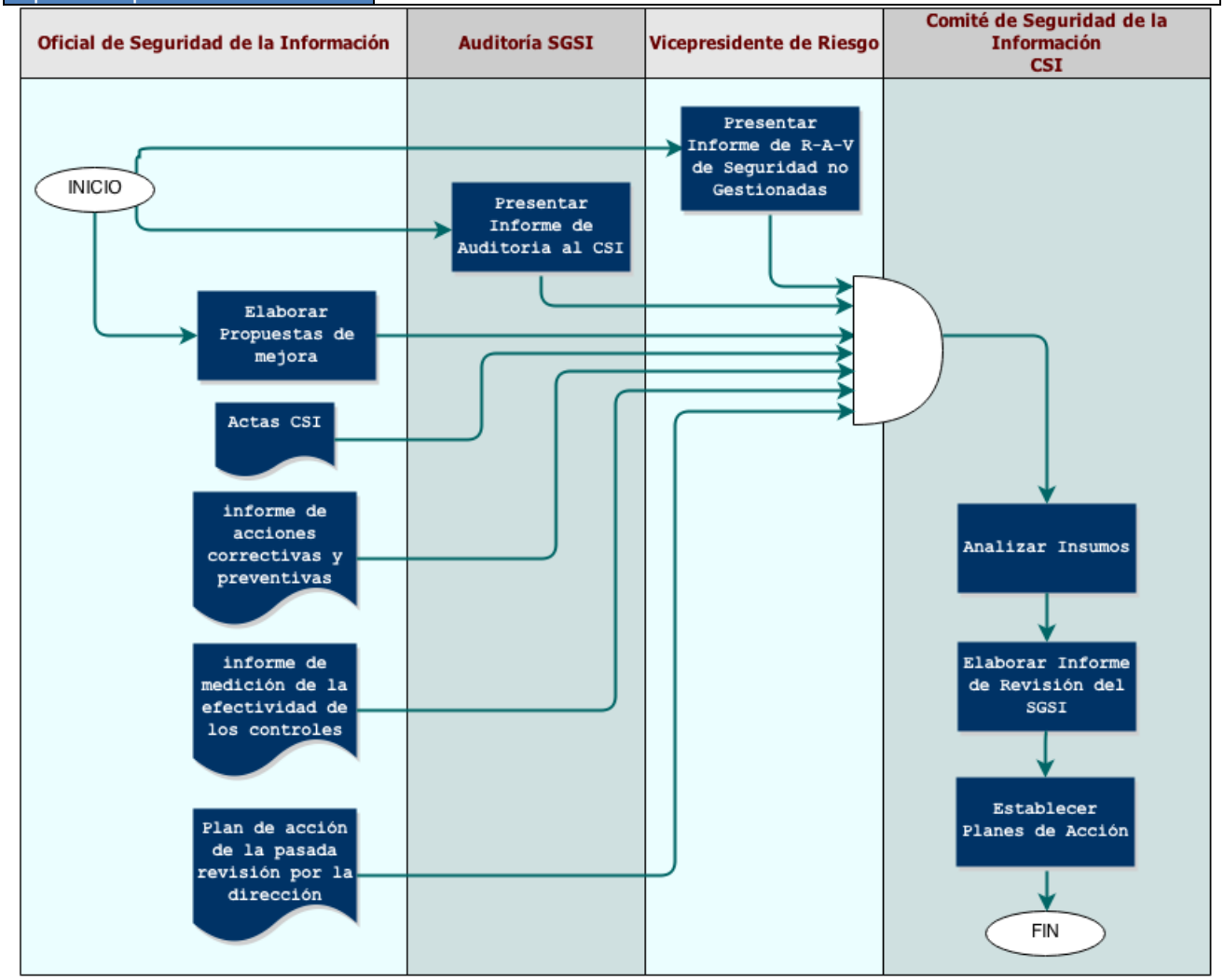
- Segundo análisis diferencial: Realizado después del análisis de activos, amenazas y riesgos pero antes de iniciar el plan de tratamiento de riesgos
  (Ver documento adjunto “R-GSI-004. Análisis diferencial ISO 27001 - v2.xlsx”)

ANEXO 2. MODELO DE SEGURIDAD DE LA INFORMACIÓN

(Ver documento adjunto “P-GSI-001. Modelo de Seguridad de la Información.docx”)

ANEXO 3. DIAGRAMA DE FLUJO DEL PROCEDIMIENTO DE REVISIÓN DEL SGSI POR LA DIRECCIÓN

Nombre del Documento:	Procedimiento de Revisión del SGSI por la dirección		
Nivel de Confidencialidad:	**Uso Interno:** Puede ser distribuido libremente entre los colaboradores de la empresa y no debe ser conocido por personal ajeno a ésta.		
Codificación:	D-GSI-001	Versión:	1.0
Fecha de última modificación:	23-03-2014	Fecha de Creación:	23-03-2014
Responsable del documento:	Oficial de Seguridad de la Información		
Aprobado por:	Junta Directiva		



ANEXO 4. CRONOGRAMA DE ACTIVIDADES DE AUDITORÍA INTERNA DEL SGSI

(Ver documento adjunto “R-AUD-001. Cronograma de actividades de auditoría Interna del SGSI.xlsx”)

ANEXO 5. LISTA DE VERIFICACIÓN DE ACTIVIDADES DEL ANÁLISIS DE RIESGOS DE UN PROCESO

(Ver documento adjunto “F-GSI-001. Lista de verificación de actividades del análisis de riesgo del proceso.xlsx”)

ANEXO 6. CRITERIOS DE VALORACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

(Ver documento adjunto “I-GSI-001. Criterios de Valoración y Clasificación de activos de información.xlsx”)

ANEXO 7. MATRIZ DE ACTIVOS DE INFORMACIÓN

(Ver documento adjunto “R-GSI-001. Matriz de Activos de Información.xlsx”)

ANEXO 8. DECLARACIÓN DE APLICABILIDAD (SOA)

(Ver documento adjunto “R-GSI-002. Declaración de Aplicabilidad.xlsx”)

ANEXO 9. MÉTRICAS E INDICADORES DEL SGSI

(Ver documento adjunto “R-GSI-003. Métricas e Indicadores del SGSI.xlsx”)

ANEXO 10. DOCUMENTO F-GSI-001 DILIGENCIADO PARA EL ANÁLISIS DE RIESGOS REALIZADO EN EL PRIMER SEMESTRE DE 2014

(Ver documento adjunto "Anexo 10. Documento Diligenciado F-GSI-001.xlsx")

ANEXO 11. DOCUMENTO R-GSI-001 DILIGENCIADO PARA LOS PROCESOS DENTRO DEL ALCANCE DEL SGSI EN EL PRIMER SEMESTRE DE 2014

(Ver documento adjunto "Anexo 11. Documento Diligenciado R-GSI-001.xlsx")

ANEXO 12. EJEMPLO DE APLICACIÓN DE MÉTODO DE ANÁLISIS DE RIESGOS

Para comprender mejor el método definido, y en especial para utilizar adecuadamente los formatos e instructivos asociados, a continuación se muestra un ejemplo donde se indican todas las actividades que se deben ejecutar. Para limitar el alcance de este ejemplo, se asume que solo disponemos de un (1) proceso, un (1) activo, una (1) amenaza y un (1) control.

Actividad 1. Se diligencia el encabezado del documento F-GSI-001, identificando el "Nombre del Proceso(s)" que será analizado, junto con el "Responsable del Proceso(s)" y la "Fecha de diligenciamiento".

Nombre del Proceso(s):	Venta de Productos y Servicios por Internet
Responsable del Proceso(s):	Vicepresidente de Operaciones
Fecha de diligenciamiento:	28 de Abril de 2014

Adicionalmente se identifican los procesos de soporte que serán incluidos en el análisis de riesgos junto con el proceso principal. Para este ejemplo: Gestión de Seguridad de TI. El resultado de esta actividad se documenta en el campo de observaciones asignado a la "Actividad 1" del F-GSI-001.

Actividad	Estado (✓) (✗)	Observaciones
ETAPA 1. ACTIVOS DE INFORMACIÓN	✓	
Actividad 1. Selección de procesos dentro del alcance	✓	Se seleccionaron los siguientes procesos de negocio extraidos del alcance del SGSI: - Venta de productos y servicios por Internet Adicionalmente se relacionan los siguientes procesos de apoyo: - Gestión de Seguridad de TI

Actividad 2. Se identificó un (1) activo superior, documentando su nombre en el campo "Nombre del Activo de Información" de la parte 1 del documento R-GSI-001. Adicionalmente se documentaron los campos "Fecha de Actualización", "Nombre del Proceso", "Consecutivo Propio", "Depende del Consecutivo" y la "Categoría del activo de información", como se muestra a continuación.

Fecha de Actualización (dd/mm/aaaa)	Nombre el Proceso	Consecutivo Propio	Depende del Consecutivo	Categoría del activo de información	Nombre del activo de información
25/04/2014	- Venta de productos y servicios por Internet	1	No Aplica	Información o datos	Base de datos de inventarios, precios y costos

El resultado de esta actividad se documentó adicionalmente en el campo de observaciones asignado a la "Actividad 2" del F-GSI-001.

Actividad	Estado (✓) (✗)	Observaciones
Actividad 2. Identificación de activos superiores – Información y Servicios	✓	Se identificó 1 activo superior, que corresponde a Información.

Actividad 3. Se identificó un (1) activo inferior, documentando su nombre en el campo "Nombre del Activo de Información" de la parte 1 del documento R-GSI-001. Adicionalmente se documentaron los campos "Fecha de Actualización", "Nombre del Proceso", "Consecutivo Propio" y la "Categoría del activo de información", como se muestra a continuación.

Fecha de Actualización (dd/mm/aaaa)	Nombre el Proceso	Consecutivo Propio	Depende del Consecutivo	Categoría del activo de información	Nombre del activo de información
25/04/2014	Gestión de Infraestructura de TI	2		Equipo Informático	Servidor físico llamado "W12DATP12"

Luego se procedió a documentar el resultado de esta actividad en el campo de observaciones asignado a la "Actividad 3" en el F-GSI-001.

Actividad	Estado (✓) (✗)	Observaciones
Actividad 3. Identificación de activos inferiores	✓	Se identificó un (1) activo considerado inferior, categorizado como Equipo Informático

Actividad 4. Se identificó la relación entre activos inferiores y superiores, documentando el campo "Depende del Consecutivo" de la parte 1 del documento R-GSI-001. Posteriormente se documentó el campo de observaciones asignado a la "Actividad 4" en el F-GSI-001.

Consecutivo Propio	Depende del Consecutivo
2	1

Actividad 5. Se documentó la descripción de cada activo y se asignó un responsable. Lo anterior quedó consignado en el R-GSI-001 parte 1, como se muestra a continuación.

Descripción del activo de información	Responsable del activo de información
Contiene los números de inventario (SKU) de todos los productos que vende la empresa, junto con su precio de venta y costo de adquisición.	Director comercial de precios, costos y márgenes
Servidor windows 2012 ubicado en el datacenter Principal (DATP) cuyo consecutivo asignado es el 12. Diseñado con el rol de base de datos.	Vicepresidente de Tecnología

Las observaciones asociadas a la actividad 5 quedaron consignadas en el F-GSI-001.

Actividad 6. Se utilizó el documento I-GSI-001 como base para identificar impactos para el negocio asociados a la posible vulneración de las dimensiones de seguridad del activo de nivel superior.

Iniciamos con la dimensión de Confidencialidad, luego se analiza la Integridad y finalmente la Disponibilidad:

Confidencialidad - Posibles impactos					
Afectación a Clientes o al Público	**Incumplimiento de Leyes o Regulaciones**	**Intereses Comerciales o Pérdidas Económicas**	**Interrupción de las ventas**	**Interrupción del reabastecimiento de mercancía**	**Pérdida de confianza (reputación)**
Despreciable (US $100)	Extremo (US $500.000)	Alto (US $75.000)	Despreciable (US $100)	Despreciable (US $100)	Extremo (US $500.000)

Integridad - Posibles impactos					
Afectación a Clientes o al Público	**Incumplimiento de Leyes o Regulaciones**	**Intereses Comerciales o Pérdidas Económicas**	**Interrupción de las ventas**	**Interrupción del reabastecimiento de mercancía**	**Pérdida de confianza (reputación)**
Extremo (US $500.000)	Despreciable (US $100)	Muy Alto (US $200.000)	Despreciable (US $100)	Despreciable (US $100)	Extremo (US $500.000)

Disponibilidad - Posibles impactos					
Afectación a Clientes o al Público	**Incumplimiento de Leyes o Regulaciones**	**Intereses Comerciales o Pérdidas Económicas**	**Interrupción de las ventas**	**Interrupción del reabastecimiento de mercancía**	**Pérdida de confianza (reputación)**
Extremo (US $500.000)	Despreciable (US $100)	Alto (US $75.000)	Extremo (US $500.000)	Extremo (US $500.000)	Alto (US $75.000)

Seguidamente, se escogieron los impactos para el activo de nivel inferior, que en este caso son los mismos del activo de nivel superior del cual depende.

Actividad 7. Se diligenciaron las columnas asociadas con el valor cuantitativo y cualitativo de cada activo, escogiendo el máximo valor de los impactos en cada dimensión, cuyo resultado se muestra a continuación.

Confidencialidad Valor Cualitativo del Activo	Confidencialidad Valor Cuantitativo del Activo ($ USD)	Integridad Valor Cualitativo del Activo	Integridad Valor Cuantitativo del Activo ($ USD)	Disponibilidad Valor Cualitativo del Activo	Disponibilidad Valor Cuantitativo del Activo ($ USD)
Extremo	$500.000	Extremo	$500.000	Extremo	$500.000
Extremo	$500.000	Extremo	$500.000	Extremo	$500.000

Actividad 8. Nuevamente con base en el documento I-GSI-001, se valida uno a uno el valor de cada activo en cada dimensión de seguridad y se documenta en el R-GSI-001 la clasificación asignada a cada activo en cada dimensión.

Confidencialidad Clasificación	Integridad Clasificación	Disponibilidad Clasificación
Confidencial	Alta	Misión Crítica
Confidencial	Alta	Misión Crítica

Actividad 9. Se prioriza el análisis de riesgos solo para los activos críticos, por lo que en nuestro caso solamente utilizaremos el activo de información "Base de Datos de Inventarios, Precios y Costos". Se documentó esta consideración en el campo de observaciones de la actividad 9 del F-GSI-001.

Actividad 10. Se escogió para este ejemplo una amenaza representativa. Seguidamente se documentó el activo y la amenaza en el R-GSI-001 parte 2 como se muestra a continuación.

PARTE 2. IDENTIFICACIÓN DE AMENAZAS Y VALORACIÓN DEL RIESGO INHERENTE	Activos	1 Base de datos de inventarios, precios y costos					
	Pricipio de Seguridad	Confidencialidad		Integridad		Disponibilidad	
Amenazas	Valor Activo	$500.000		$500.000		$500.000	
[A.11] Acceso no autorizado El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.							

Actividad 11. Se identificó la frecuencia de ocurrencia en 12 veces al año y la degradación como del 100% tanto para Confidencialidad como para Integridad, dejando en blanco la Disponibilidad pues se consideró que esta amenaza no afecta esta dimensión del activo. Lo anterior se documentó en el R-GSI-001 parte 2 como se muestra a continuación.

PARTE 2. IDENTIFICACIÓN DE AMENAZAS Y VALORACIÓN DEL RIESGO INHERENTE	Activos	1 Base de datos de inventarios, precios y costos					
	Pricipio de Seguridad	Confidencialidad		Integridad		Disponibilidad	
Amenazas	Valor Activo	$500.000		$500.000		$500.000	
[A.11] Acceso no autorizado El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.		12	100%	12	100%		

Así mismo, se documentó el resultado de esta actividad en el respectivo campo de observaciones del F-GSI-001.

Actividad 12. Se realizó el cálculo del impacto (Valor del activo x Degradación) y el Riesgo Inherente (Probabilidad de Ocurrencia x Impacto). Lo anterior se documentó en el R-GSI-001 parte 2 como se muestra a continuación.

PARTE 2. IDENTIFICACIÓN DE AMENAZAS Y VALORACIÓN DEL RIESGO INHERENTE	Activos	1 Base de datos de inventarios, precios y costos					
	Pricipio de Seguridad	Confidencialidad		Integridad		Disponibilidad	
Amenazas	Valor Activo	$500.000		$500.000		$500.000	
[A.11] Acceso no autorizado		12	100%	12	100%		
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.		$500.000		$500.000		$0	
		$6.000.000		$6.000.000		$0	

Adicionalmente se calcularon los valores acumulados de riesgo para cada dimensión de seguridad y el total (suma de los riesgos de las dimensiones), diligenciando los resultados en

el mismo documento.

Total RIESGO x CONFIDENCIALIDAD ACTIVO 1	Total RIESGO x INTEGRIDAD ACTIVO 1	Total RIESGO x DISPONIBILIDAD ACTIVO 1
$6.000.000	$6.000.000	$0
Total RIESGO ACTIVO 1		
$12.000.000		

En este caso, solo tenemos 1 activo y 1 amenaza, por lo que los totales anteriores serían los totales de la organización. Riesgo Total = $ 12.000.000

Actividad 13. Se identificaron dos (2) riesgos críticos, asociados a la confidencialidad e integridad del activo 1 respecto a la amenaza A.11. Se escogieron debido a que superan el umbral de los $500.000 USD. Lo anterior se documentó en el R-GSI-001 parte 3 como se muestra a continuación.

PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL	Riesgo: Amenaza vs Activo		Riesgo 1 - [A.11] Acceso no autorizado sobre la Base de datos de Inventarios, precios y costos			
	Principio de Seguridad		Confidencialidad		Integridad	
Controles Actuales	Frecuencia Inherente (Anual)	Impacto Inherente	12	$500.000	12	$500.000
	Riesgo Inherente		$6.000.000		$6.000.000	
			Reducción de Frecuencia	Reducción de Impacto	Reducción de Frecuencia	Reducción de Impacto

Actividad 14. Del listado de controles aplicables en la empresa (Documento SOA) se identificó el control llamado “A.11.6.1. Restricciones de acceso a la información” que incide directamente sobre las amenazas asociadas, reduciendo los riesgos identificados. Lo anterior se documentó en el R-GSI-001 parte 3 como se muestra a continuación.

PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL	Riesgo: Amenaza vs Activo		Riesgo 1 - [A.11] Acceso no autorizado sobre la Base de datos de Inventarios, precios y costos			
	Principio de Seguridad		Confidencialidad		Integridad	
Controles Actuales	Frecuencia Inherente (Anual)	Impacto Inherente	12	$500.000	12	$500.000
	Riesgo Inherente		$6.000.000		$6.000.000	
A.11.6.1. Restricción del acceso a la información (Reductor de frecuencia de ocurrencia e impacto)			Reducción de Frecuencia	Reducción de Impacto	Reducción de Frecuencia	Reducción de Impacto

Actividad 15. Se calificó como de un 40% tanto la reducción de frecuencia como la reducción de Impacto tanto para Confidencialidad como para Integridad. Lo anterior se documentó en el R-GSI-001 parte 3 como se muestra a continuación.

PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL		Riesgo: Amenaza vs Activo		Riesgo 1 - [A.11] Acceso no autorizado sobre la Base de datos de Inventarios, precios y costos			
		Principio de Seguridad		Confidencialidad		Integridad	
Controles Actuales		Frecuencia Inherente (Anual)	Impacto Inherente	12	$500.000	12	$500.000
		Riesgo Inherente		$6.000.000		$6.000.000	
A.11.6.1. Restricción del acceso a la información (Reductor de frecuencia de ocurrencia e impacto)				Reducción de Frecuencia 40%	Reducción de Impacto 40%	Reducción de Frecuencia 40%	Reducción de Impacto 40%

Actividad 16. Se calcularon los valores de Frecuencia e impacto residuales multiplicando los valores inherentes por la reducción de frecuencia e Impacto. Lo anterior se documentó en el R-GSI-001 parte 3 como se muestra a continuación.

PARTE 3. IDENTIFICACIÓN DE CONTROLES Y VALORACIÓN DEL RIESGO RESIDUAL		Riesgo: Amenaza vs Activo		Riesgo 1 - [A.11] Acceso no autorizado sobre la Base de datos de Inventarios, precios y costos			
		Principio de Seguridad		Confidencialidad		Integridad	
Controles Actuales		Frecuencia Inherente (Anual)	Impacto Inherente	12	$500.000	12	$500.000
		Riesgo Inherente		$6.000.000		$6.000.000	
A.11.6.1. Restricción del acceso a la información (Reductor de frecuencia de ocurrencia e impacto)				Reducción de Frecuencia 40%	Reducción de Impacto 40%	Reducción de 40%	Reducción de Impacto 40%
		Frecuencia Residual (Anual)	Impacto Residual	7,2	$300.000	7,2	$300.000
		TOTAL RIESGO RESIDUAL AÑO		$2.160.000		$2.160.000	

Finalmente se calcula el riesgo total residual como la suma de los riesgos residuales de cada activo en cada dimensión de seguridad, dando como resultado $4,320.000 USD.

ANEXO 13. CRONOGRAMA DETALLADO DE IMPLEMENTACIÓN DE PROYECTOS DE SEGURIDAD

(Ver documento adjunto “R-GSI-006. Cronograma de implementación de proyectos de SI.xlsx”)

ANEXO 14. ANÁLISIS DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN RESPECTO A ISO 27002

(Ver documento adjunto “R-GSI-007. Evaluación de Madurez ISO 27002.xlsx”)