

Recomendaciones para la implementación de un SGSI según la norma ISO 27001:2013

TABLA DE CONTENIDO

1	OBJETIVO del documento	3
2	ALCANCE	3
3	NORMAS UTILIZADAS	3
4	SGSI (sistema de gestión de la seguridad de la información)	3
4.1	MODELO PHVA	3
4.2	DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN	4
5	METODOLOGIA RECOMENDADA	5
5.1	CONTEXTO.....	5
5.2	SITUACIÓN ACTUAL.....	6
5.3	DEFINICIÓN DE LAS VARIABLES PARA EL ANÁLISIS	7
6	RECOMENDACIONES PARA LA IMPLEMENTACIÓN	12
6.1	A.5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	12
6.2	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	12
6.3	A.7. SEGURIDAD DEL RECURSO HUMANO	13
6.4	A.8. GESTIÓN DE ACTIVOS	14
6.5	A.9. CONTROL DE ACCESO	15
6.6	A.10. CRIPTOGRAFÍA	16
6.7	A.11. SEGURIDAD FÍSICA Y DEL ENTORNO	16
6.8	A.12. SEGURIDAD EN LAS OPERACIONES	18
6.8.1	<i>PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES</i>	18
6.8.2	<i>REGISTRO Y SEGUIMIENTO</i>	18
6.9	A.13. SEGURIDAD EN LAS COMUNICACIONES	19
6.10	A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19
6.11	A.15. RELACIONES CON LOS PROVEEDORES	21
6.12	A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	21
6.13	A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	22
6.14	A.18. CUMPLIMIENTO	25
7	DEFINICIONES	26

1 OBJETIVO DEL DOCUMENTO

Presentar el modelo recomendado por *Sisteseg Consulting (Colombia)* para implementar la norma ISO 27001:2013 y sus controles de seguridad de la mano de un modelo de Sistema de Gestión de Seguridad de la Información, (SGSI), utilizando el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar). Los diferentes controles de la norma serán priorizados lo que determinará a futuro un plan de acción que ayudará a la implementación de la norma de un modo estratégico. Para este modelo se tienen en cuenta los siguientes aspectos:

1. La integridad
2. La confidencialidad
3. La disponibilidad
4. Controles de acceso
5. Técnicas criptográficas
6. Servicios AAA (authentication, accounting, authorization)
7. Definición de variables

2 ALCANCE

Este modelo considera los controles de la norma NTC/ISO 27001:2013.

3 NORMAS CONSIDERADAS

1. NTC/ISO 27001:2013
2. NTC/ISO 27005:2009
3. GTC/ISO 27002:2015

4 SGSI (SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN)

4.1 MODELO PHVA

El modelo del SGSI ISO 27001:2013 está basado en el ciclo de mejoramiento continuo PHVA, el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI ISO 27001:2013.

A continuación, el detalle del ciclo:

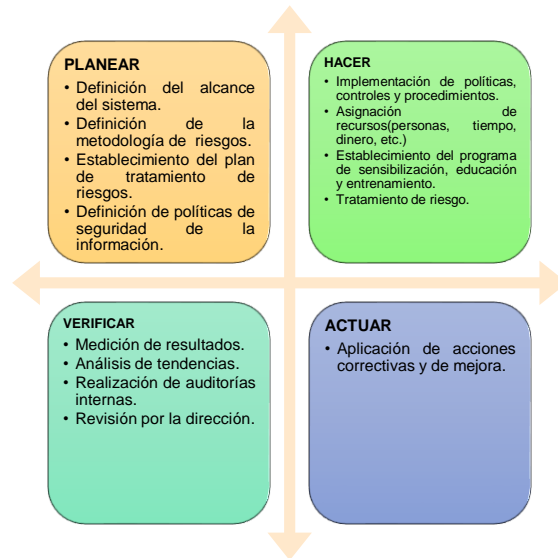


Ilustración 1. Fases del Ciclo PHVA

4.2 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo a su importancia, a continuación se ilustran dichos componentes:

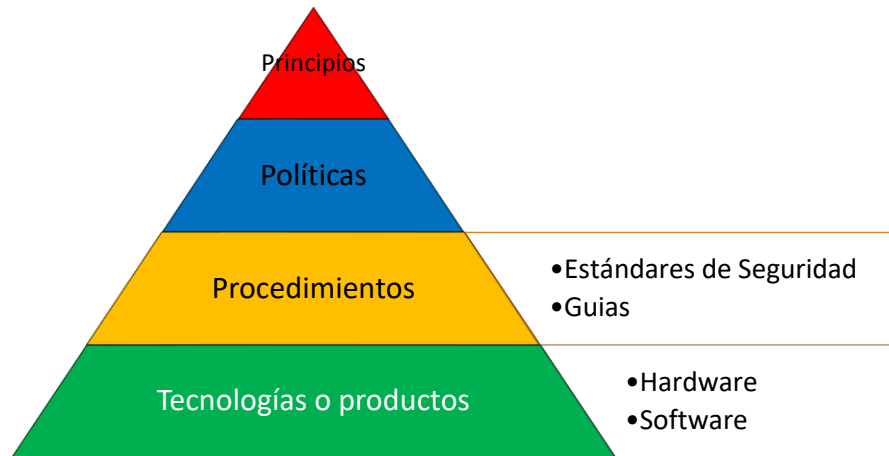


Ilustración 2. Componentes del Modelo de la seguridad de la información

5 METODOLOGIA RECOMENDADA

La metodología recomendada para la implementación del SGSI ISO 27001:2013 se muestra y se explica a continuación:

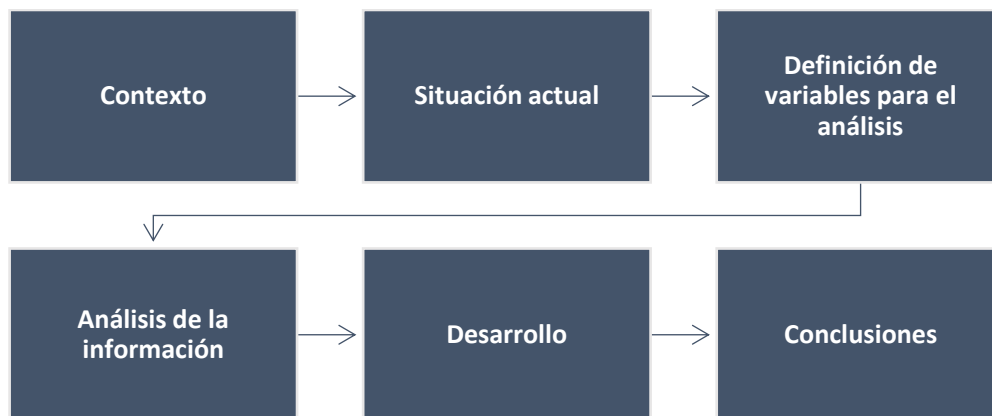


Ilustración 3. Metodología recomendada

5.1 CONTEXTO

En esta fase inicial de la metodología recomendada de implementación del SGSI ISO 27001:2013, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

1. La misión	2. La visión	3. Antecedentes
4. Estructura organizacional	5. Procesos	6. Cultura y valores
7. Legislación pertinente	8. Tecnología existente	

5.2 SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento la organización con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina análisis GAP ISO 27001:2013 o análisis de brecha. Para poder realizar este Plan es indispensable que se tenga en cuenta los niveles de madurez por cada uno de los dominios (ver figura a continuación) con el fin de plantear prioridades sobre su implementación.

Dominio ISO 27001	Objetivo de control
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Ilustración 4. Dominios.

La metodología recomendada para realizar el GAP ISO 27001:2013 se presenta a continuación:

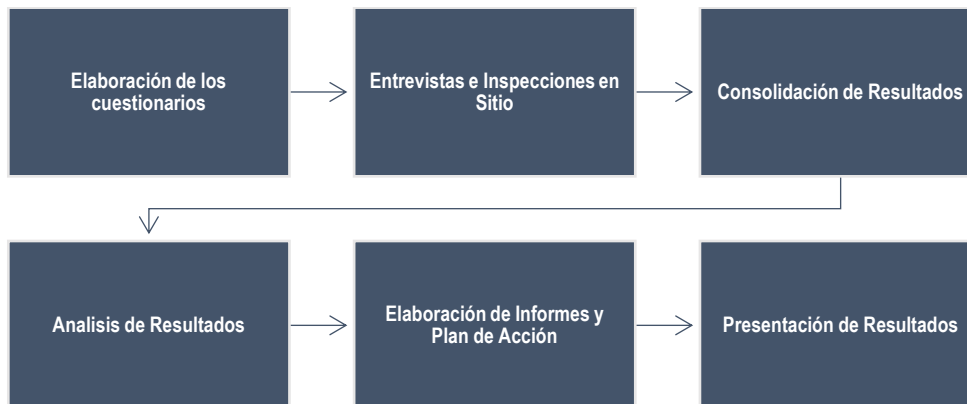


Ilustración 5. Metodología recomendada para el GAP.

5.3 DEFINICIÓN DE LAS VARIABLES PARA EL ANÁLISIS

Para la implementación priorizada del SGSI ISO 27001:2013 es necesario definir una serie de variables que ayuden a la priorización de los diferentes dominios de la NTC/ISO 27001:2013. Los 14 dominios de la norma están conformados por 114 controles. Este Plan propone una estrategia para la implementación basada en una serie de variables que permiten inferir el orden de implementación de cada uno de los dominios teniendo en cuenta algunos aspectos asociados a cada uno de los controles. En la siguiente figura se presentan la matriz de valoración para cada una de las combinaciones posibles.

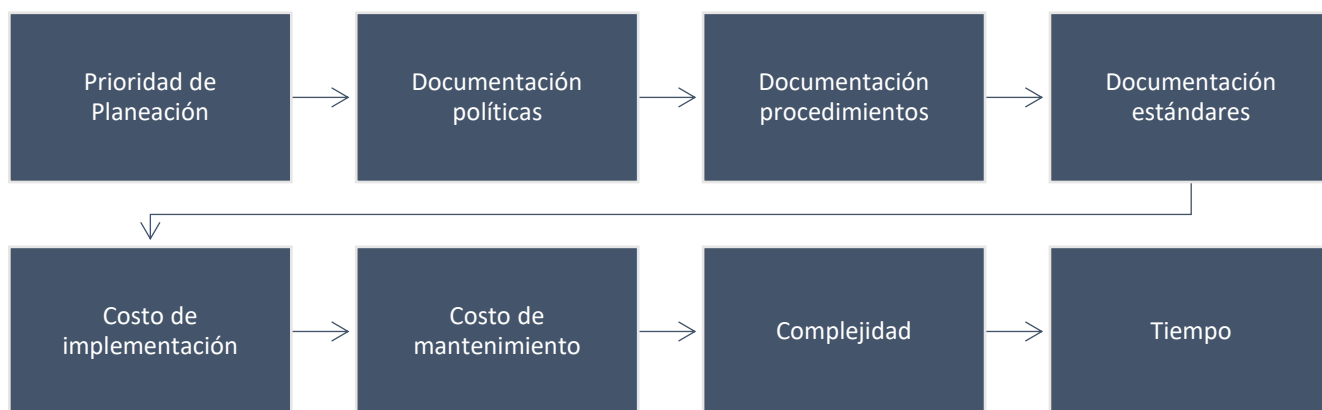


Ilustración 6. Variables analizadas.

Prioridad de Planeación: Esta variable considera los aspectos relacionados con el dominio desde el punto de vista de las categorías del tipo de control o dominio: administrativo (3), tecnológico (2) y físico (1) y los aspectos referentes a los niveles de planeación: estratégico (3), táctico (2) y operativo (1). Dependiendo de la conjunción de estos dos criterios (nivel de planeación y categorías del tipo del control o dominio) se asigna un valor que ayudará a definir la prioridad de implementación teniendo en cuenta la magnitud de este valor tal como se muestra en la siguiente figura (los valores de mayor a menor son: 9, 6, 4, 3, 2,1).

Categorías	Estratégico (3)	3	6	9
	Táctico (2)	2	4	6
	Operativo (1)	1	2	3
		Físico (1)	Tecnológico (2)	Administrativo (3)
Niveles de planeación				

Ilustración 7. Prioridad.

Documentación política: El esfuerzo asociado con la documentación de políticas por cada uno de los dominios se mide en esta variable. La cantidad de políticas y normas que hay que desarrollar por dominio es un estimativo que ayuda a determinar su prioridad de implementación.

Los rangos utilizados para calificar esta variable se muestran a continuación:

DOCUMENTACION DE POLITICAS ISO 27001:2013		
VALOR	NIVEL	Rango Número de Políticas
5	MUY ALTO	Entre 13 y 16
4	ALTO	Entre 9 y 12
3	MEDIO	Entre 6 y 8
2	BAJO	Entre 4 y 5
1	MUY BAJO	Entre 1 y 3

Tabla 1. Documentación de políticas.

Documentación procedimientos: El esfuerzo requerido por cada dominio en el número de procedimientos requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los diferentes dominios. Los valores estimados de criticidad relacionados con el número de procedimientos estimado requerido se presenta a continuación:

DOCUMENTACION DE PROCEDIMIENTOS ISO 27001:2013		
VALOR	NIVEL	Rango Número de proc.
5	MUY ALTO	Entre 13 y 16
4	ALTO	Entre 9 y 12
3	MEDIO	Entre 6 y 8
2	BAJO	Entre 4 y 5
1	MUY BAJO	Entre 1 y 3

Tabla 2. Documentación de procedimientos.

Documentación estándares: El esfuerzo requerido por cada dominio en el número de estándares requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los dominios.

Los valores estimados de criticidad relacionados con el número de estándares estimado requerido se presenta a continuación:

DOCUMENTACION DE ESTANDARES ISO 27001:2013		
VALOR	NIVEL	CRITERIOS (CANTIDAD)
5	MUY ALTO	3
4	ALTO	2
3	MEDIO	1
2	BAJO	0
1	MUY BAJO	0

Tabla 3. Documentación de estándares.

Costo de implementación: Cada uno de los dominios de la norma dependiendo de la cantidad de herramientas, software, servicios, infraestructura, horas hombre, entre otros aspectos, requerirá de unos esfuerzos financieros diferentes. De tal manera que se puede recomendar como parte de este Plan, que aquellos dominios con menor costo sean implementados en el menor tiempo posible con el fin de obtener lo que se conoce como ganancias tempranas lo que a larga beneficiará la aceptación de todo lo concerniente a la seguridad de la información por parte de la entidad y mantendrá la motivación en niveles altos durante

la fase de implementación del SGSI ISO 27001:2013. La tabla utilizada para estimar de manera cualitativa el costo asociado a un dominio es la siguiente:

COSTO DE IMPLEMENTACION ISO 27001:2013		
VALOR	NIVEL	CRITERIOS
5	MUY ALTO	Mayor a 100.000\$
4	ALTO	Entre 99.999\$ y 60.000\$
3	MEDIO	Entre 59.999\$ y 20.000\$
2	BAJO	Entre 19.999\$ y 5.000\$
1	MUY BAJO	Menor a 5000\$

Tabla 4. Costos de implementación.

Gasto de mantenimiento: Todo control asociado a un dominio tiene por su misma naturaleza unos gastos asociados en mantener su efectividad en el transcurso del tiempo. Estos gastos normalmente tienden a ser reiterativos y en algunos casos se requiere de un tercero para que cumpla con la función del mantenimiento.

La tabla utilizada para estimar de manera cualitativa los gastos asociados a un dominio es la siguiente:

GASTOS DE MANTENIMIENTO ISO 27001:2013		
VALOR	NIVEL	CRITERIOS
5	MUY ALTO	Mayor a 100.000\$
4	ALTO	Entre 99.999\$ y 60.000\$
3	MEDIO	Entre 59.999\$ y 20.000\$
2	BAJO	Entre 19.999\$ y 5.000\$
1	MUY BAJO	Menor a 5000\$

Tabla 5. Gastos de mantenimiento.

Complejidad: La variable complejidad considera las calificaciones requeridas en el recurso humano con el fin de acometer la implementación del dominio o control en cuestión, para ello se consideran los siguientes aspectos:

Especialista	Ingeniero
Técnico	Estudiante técnico o profesional
Personal no calificado	

La tabla utilizada para estimar de manera cualitativa la complejidad asociada a un dominio es la siguiente:

COMPLEJIDAD		
VALOR	NIVEL	CRITERIOS
5	MUY ALTO	Especialista
4	ALTO	Ingeniero
3	MEDIO	Técnico
2	BAJO	Estudiante técnico o profesional
1	MUY BAJO	Personal no calificado

Tabla 6. Complejidad.

Tiempo: La variable tiempo le imprime al dominio unas restricciones importantes en lo referente al tema de cuándo se debe abordar su implementación. Se considera que si un control o dominio toma mucho tiempo para su implementación es recomendable abordarlo posteriormente para que de esta manera podamos implementar muchos más controles que sean de corta duración en su implementación y se aumenta rápidamente el porcentaje de cumplimiento de la norma de seguridad.

La tabla utilizada para estimar de manera cualitativa el tiempo asociado a la implementación de un dominio determinado es la siguiente:

TIEMPO		
VALOR	NIVEL	CRITERIOS
5	MUY ALTO	Más de 1 mes
4	ALTO	entre 30 días y 15 días
3	MEDIO	Menos de una semana
2	BAJO	Menos de un día
1	MUY BAJO	Menos de 24 horas

Tabla 7. Tiempo.

6 RECOMENDACIONES PARA LA IMPLEMENTACIÓN

6.1 A.5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La política determina los objetivos de seguridad, lo que se quiere hacer en temas de seguridad, se basa en los análisis de riesgos y en los resultados de la gestión de incidentes de seguridad. Las políticas siempre responden a la pregunta ¿Qué voy a hacer? y en ese sentido hay que redactar la política. La política define los objetivos a alcanzar y no cómo se va a implementar, es un error incluir en una política temas de tipo operativo.

Proyectos ISO 27001:2013	Avance del proyecto
Consultoría para el SGSI	
Sistema de Gestión Documental	
Auditoría Externa del modelo de Seguridad	
Adquisición de plantillas para las políticas	

Tabla 8. Proyectos Políticas de Seguridad.

6.2 A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información realmente es una cultura, en la cual se deben involucrar todos los colaboradores, tanto servidores públicos, clientes y contratistas para que contribuyan a crear un clima de seguridad tanto al interior como al exterior de la entidad. La organización de seguridad debe estar distribuida por toda la entidad en diferentes funciones con responsabilidades relacionadas con la seguridad de la información.

Se deben utilizar roles para la realización de las actividades que los colaboradores realizan en cada procedimiento, y posteriormente asociar a los cargos, los roles previamente definidos, que contienen las actividades y las funciones de cada rol.

A la hora de realizar esta asignación de roles a cargos se debe:

1. Realizar una matriz RACI¹ para cada procedimiento, de tal forma que puedan ser controladas las actividades por diferentes personas.

¹ Matriz de asignación de responsabilidades

2. Realizar una matriz de segregación de funciones entre los roles con el fin de asegurarse que para un cargo no se presenten conflictos de intereses en temas de seguridad de la información.

Dentro del modelo de seguridad, la organización de seguridad debe tener al menos:

- Un **comité de seguridad de la información** en el cual se debe integrar la alta gerencia. Este comité es el órgano máximo del modelo de seguridad. Sus funciones principales, entre otras, podrían ser:
 - Definir los lineamientos y estrategias de Seguridad de la información en función de los objetivos del negocio.
 - Aprobar el modelo de seguridad de la entidad (políticas, normas, procedimientos, etc.).
- **Líder de seguridad de la Información de la Entidad.** Es el encargado de coordinar todo el modelo de seguridad. Debería estar dedicado tiempo completo a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad.
- **Analista de seguridad de la información.** Son funcionarios dedicados tiempo completo a temas de seguridad de la información y que realizan labores operativas del modelo de seguridad. Son dirigidos por el líder de seguridad de la información.

Proyectos ISO 27001:2013	Avance del proyecto
Consultoría para el SGSI	
Contratación personal de seguridad	
Auditoría Externa del Modelo de Seguridad	
Implementación de DMZ y VPN'S en Teletrabajo	
Sistema de control de acceso dispositivos móviles	

Tabla 9.Proyectos Organización de la Seguridad.

6.3 A.7. SEGURIDAD DEL RECURSO HUMANO

Con relación a la seguridad de los recursos humanos se debe tener en cuenta el ciclo de vida del recurso humano, esto es, antes, durante y después de su contratación. En este sentido se darán recomendaciones en estas tres etapas.

Antes de la contratación:

Contar con un procedimiento de selección de personal que, de acuerdo con las leyes y reglamentos de ética pertinentes, incluya:

- Verificación de referencias
- Verificación de la hoja de vida completa
- Verificar en términos generales que sea una persona confiable.

Durante el periodo de contratación:

- Todos los colaboradores y contratistas que accedan a información reservada o sensible deben firmar un acuerdo de confidencialidad y no divulgación ANTES de tener acceso a dicha información por cualquier medio.
- Todos los colaboradores deben firmar una cesión de derechos de propiedad intelectual a favor de la entidad sobre los desarrollos que se realicen fruto de su trabajo en la entidad.

Se debe crear un programa de capacitaciones continuas en seguridad que deberán cubrir como mínimo los siguientes aspectos

- Concientización sobre riesgos de seguridad.
- Conocimiento del modelo de seguridad.
- Puntos de contacto para información de problemas de seguridad.

Proyectos ISO 27001:2013	Avance del proyecto
Consultoría para el SGSI ISO 27001:2013	
Sistema de Gestión Documental	
Educación formal en seguridad de la información	

Tabla 10.Proyectos recursos humanos.

6.4 A.8. GESTIÓN DE ACTIVOS

Este dominio pretende identificar los activos de información de la entidad, clasificarlos, asignarles responsables a estos activos y brindarles un tratamiento apropiado de acuerdo a su clasificación.

Las recomendaciones en este punto son:

- Realizar un inventario de todos los activos de información, para este fin normalmente se realiza una búsqueda de los activos de información en los procesos y procedimientos, buscando el flujo de información en los mismos.
- Incluir en el inventario, el tipo de activo (físico o digital), ubicación, activos de soporte, redes, medios, servidores o servicios en las que se encuentra, proceso al que pertenece, entre otros.
- La disposición final para los medios removibles debe realizarse en forma segura, por ejemplo incineración o borrado seguro.

Proyecto ISO 27001:2013	Avance del proyecto
Consultoría para el SGSI	
Sistema de Gestión Documental	
Herramienta de control de información	
Software para borrado seguro	
Herramienta para la destrucción de medios	

Tabla 11.Proyectos gestión de activos.

6.5 A.9. CONTROL DE ACCESO

El objetivo del dominio de control de acceso consiste en limitar el acceso a la información y a las instalaciones con el fin de salvaguardar los activos de información.

- Se debe realizar unas políticas de control de acceso, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones para esta política son:
 - Tener en cuenta para este fin la clasificación de la información, la legislación pertinente de acuerdo con las leyes de protección de datos.
 - Implementar un procedimiento de gestión de derechos de acceso a los diferentes tipos de activos de información en los que se involucre a los dueños de los activos de información.

Proyectos ISO 27001:2013	Avance del proyecto
Consultoría para el SGSI	
Sistema de Gestión Documental	
Sistema de Single-Sign-On	
Sistemas de detección de intrusos	

Tabla 12. Proyectos de control de acceso.

6.6 A.10. CRIPTOGRAFÍA

El objetivo de este dominio es asegurar la confidencialidad mediante el uso de métodos apropiados de criptografía. Los sistemas centralizados de gestión de llaves garantizan la seguridad de las diferentes llaves utilizadas por los sistemas de cifrado.

Los proyectos recomendados para este dominio son:

Proyectos ISO 27001:2013	Avance del proyecto
Uso de sistemas centralizados para gestión de llaves (HSM por ejemplos)	
Sistemas de doble autenticación	
Tecnologías de cifrado fuerte	

Tabla 13. Criptografía

6.7 A.11. SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad no es una tecnología, ni un producto, es un proceso que se apoya en la tecnología para lograr sus objetivos a lo largo de toda la entidad. La seguridad debe ser un enfoque sistémico realizado por profesionales en la materia, que propongan una serie de actividades, procesos y productos para que todos funcionando de manera sincronizada ejerzan un control, factores disuasivos, e información; que en su conjunto garanticen que la entidad pueda lograr sus objetivos de manera oportuna y productiva.

La seguridad física en Colombia es y ha sido un aspecto muy importante de la forma como las empresas protegen sus activos económicos. Se requiere contar con una metodología que permite evaluar qué tan efectivos son los controles existentes en la infraestructura de la Entidad con el fin de actuar como factor

disuasivo y control, contra eventos que pongan en peligro la disponibilidad, confidencialidad e integridad de la información.

1. Centros de Procesamiento normales o de emergencia
2. Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación
3. Áreas donde se encuentren concentrados dispositivos de información

Normas que se deben aplicar

- NFPA 70 National Electrical Code (NEC), 2005
- ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard.
- NFPA 75 Standard for the Protection of Electronic Computer/Data Processing Equipment, 2.003 Edition.
- IEEE 1100-2005, Recommended Practice for Powering and Grounding Sensitive Electronic Equipment.
- TIA/EIA 568 B2.1 Commercial Building Telecommunications Wiring Standards.
- TIA/EIA 569A Commercial Building Standard for Telecommunications Pathways and Spaces.
- Thermal Guide for Data Processing Environments. ASHRAE (American Society of Heating, Refrigerating and Air Conditioning Engineers, Inc)
- Recomendaciones de fabricantes de equipos de cómputo para instalación de sus equipos (site prep).

Proyectos ISO 27001:2013	Avance del proyecto
Diseño de nuevo Centro de Datos	
Sistemas automáticos de apagado de incendios	
Centro de datos alternativo	
CCTV	
Sistemas de detección de intrusos	

Tabla 14. Seguridad física.

6.8 A.12. SEGURIDAD EN LAS OPERACIONES

El objetivo de este dominio consiste en asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Para ello, lo divide en siete grandes subdominios que se tratarán individualmente:

6.8.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Para este subdominio se debe:

- Tener procedimientos documentados de cada uno de los elementos de procesamiento de información, como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debería incluir como mínimo:
 - Instalación y configuración de los sistemas
 - Procedimientos de encendido y apagado
 - Procedimientos de respaldo tanto de los datos como de la configuración

- Contar con un procedimiento de gestión de la capacidad. El principio fundamental consiste en monitorear todos los recursos de procesamiento y comunicación, tales como ancho de banda de los canales, memoria, capacidad de almacenamiento, capacidad de cálculo, entre otros, y alertar cuándo lleguen a valores críticos con el fin de gestionar la capacidad de cómputo, bien sea optimizando o adquiriendo más capacidad.

6.8.2 REGISTRO Y SEGUIMIENTO

El objetivo de este subdominio es dejar rastro de los eventos y evidencia de todas las operaciones relevantes con el fin de que sirvan de apoyo en una investigación de seguridad en un momento dado. Se debe tener en cuenta para estos registros que contengan entre otros la siguiente información:

- Identificación de usuarios;
- Actividades del sistema;
- Fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;
- Registros de intentos de acceso al sistema exitosos y rechazados;
- Registros de datos exitosos y rechazados y otros intentos de acceso a recursos;

Proyecto ISO 27001:2013	Avance del proyecto
Software para la gestión de la capacidad y disponibilidad	
Centralizador de logs	
Software o servicios de análisis de vulnerabilidades	
Proyecto de separación de ambientes (físicos y lógicos)	

Tabla 15. Proyectos operaciones.

6.9 A.13. SEGURIDAD EN LAS COMUNICACIONES

La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación.

Proyecto ISO 27001:2013	Avance del proyecto
Switches de nivel 4 con QOS	
Sistemas de protección UTM con QOS	
Balancedores de carga	
Analizadores de tráfico en tiempo real	

Tabla 16. Proyectos comunicaciones.

6.10 A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La seguridad en los procesos de desarrollo de software debe estar a lo largo de cada parte del ciclo de desarrollo de software, las recomendaciones por cada parte son:

Análisis de Requerimientos

- Definir claramente con el usuario final el alcance de los requerimientos.
- Determinar la confidencialidad de la información que se maneja
- Definir el control de autenticación requerido
- Definir los roles y los privilegios de cada rol

Diseño

- Acceso a componentes y administración del sistema
- Logs para auditoría

- Manejo apropiado de errores
- Segregación de funciones
- Defina adecuadamente la administración de identidades
 - Exija el uso de contraseñas seguras
 - En el caso de que se produzca un error en la autenticación, devuelva la mínima información posible
- Compruebe siempre la validez de los datos de entrada
 - Suponga que todos los datos especificados por los usuarios tienen mala intención
 - Compruebe la validez del tipo, longitud e intervalo de los datos
- Administración de la configuración y las sesiones
- Datos confidenciales y criptografía
- Auditoría y registro, siempre dejar registro de las actividades sensibles del aplicativo, (log-in y log-out, Tiempo de sesión, accesos a la base de datos)

Codificación

- Aseguramiento de los ambientes de desarrollo
- Mantener documentación técnica
- Seguridad en las interfaces de comunicación
- Buenas prácticas de codificación:
 - Validación de entradas
 - Codificación de las salidas
 - Estilo de programación limpio
 - Código autodocumentado

Pruebas

- Controles de calidad en controles de seguridad
- Inspección de código por fases
- Comprobación de gestión de configuraciones
- Realizar pruebas de caja blanca y caja negra (owasp top 10)

Instalación, actualización y parches

- Tener en cuenta control de cambios

Proyecto ISO 27001:2013	Avance del proyecto
Implementar aplicativos de control de código fuente	
Implementar software para gestión de pruebas	
Software de revisión de código malicioso	
Simulador de pruebas de estrés	

Tabla 17. Proyectos desarrollo.

6.11 A.15. RELACIONES CON LOS PROVEEDORES

Los proveedores por su naturaleza son una de las fuentes externas de riesgos, pero a su vez son importantes para el cumplimiento de la misión y la visión de la entidad, por esta razón se deben implementar controles para: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con proveedores.

Las auditorías nos ayudan a determinar el nivel de cumplimiento de los proveedores con respecto a la seguridad de la información:

Proyectos ISO 27001:2013	Avance del proyecto
Software para gestión de auditorías externas	
Realización de auditorías a proveedores	

Tabla 18. Proyectos proveedores.

6.12 A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Construir un proceso consistente para gestionar los incidentes de seguridad de la información, el cual debe contener como mínimo:

- Reporte de incidente de seguridad de la información
- Investigación de incidente de seguridad de la información
- Adecuado control de cadena de custodia para gestión de evidencias.

La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Proyecto ISO 27001:2013	Avance del proyecto
Analizador y comparador automático de logs	
Herramientas de análisis forense	
Capacitaciones en Investigaciones de seguridad	
Software para la gestión de incidentes	

Tabla 19. Proyectos Incidentes de Seguridad.

6.13 A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

La continuidad del negocio en lo relacionado a la información es un componente fundamental en la implementación del SGSI. La Gestión de la Continuidad del Negocio (BCM, por sus siglas en inglés Business Continuity Management) debe ser un proceso establecido en nuestra sociedad moderna, globalizada, interconectada, con tecnologías novedosas, más complejas y, además, con una alta presencia de riesgos de tipo operativo que en cualquier momento podrían llegar a materializarse.

Finalmente, el BCP ha sido estandarizado en el año 2012 bajo la norma internacional ISO 22301; norma certificable que ha servido de consulta permanente e indispensable para la realización de este documento y del proceso en general.

Estos factores, junto con una legislación cada vez más exigente en lo relacionado a la confiabilidad y a la seguridad en la prestación de estos productos y servicios, hacen necesario, en la actualidad, que se cuente con un BCP/DRP con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, con la disponibilidad de los procesos del negocio, con la protección de la información (ISO 27001:2013), con fortalecimiento y preservación del conocimiento, con la tecnología propicia y segura, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las

pandemias, la pérdida de empleados claves, las amenazas naturales y el CIBERTERRORISMO², entre otros, han mostrado la necesidad de incorporar nuevas amenazas en el BCP con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información, por dos años consecutivos, han permanecido en el primer lugar, como causa de activación de los BCP, de acuerdo al 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%.

Proyectos de Planes anexos al BCP

- **Plan de comunicación de crisis:** busca describir los procedimientos y comunicados que las organizaciones deben preparar para responder ante un incidente de manera correcta. Este plan debe estar coordinado con los otros planes de la organización para asegurar que sólo comunicados revisados y aprobados sean divulgados y que solamente el personal autorizado, previamente designado, sea el responsable de responder a las diferentes inquietudes y de diseminar los reportes de estado durante la contingencia a los empleados y al público en general.
- **Planes de evacuación por edificio:** estos planes contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o a la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica, entre otros. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.
- **Plan de respuesta a CIBERINCIDENTES:** este plan establece los procedimientos para responder a los ataques en el ciberespacio contra los sistemas de información de una organización. Son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados al hardware y al software, entre otros. Ejemplos de elementos que pueden generar estos incidentes de

² El BCI Horizon Scan, evaluó 760 organizaciones a nivel mundial y comprobó que el (82%) de los líderes de continuidad temen por un ciberataque inminente. Estos ataques pueden generar unas pérdidas de alrededor de \$7.6 millones de dólares por empresa y con un crecimiento anual de 10.4% en el número de estos ataques.

seguridad pueden ser: la lógica maliciosa, los virus, los gusanos, los troyanos, por mencionar algunos. Estos planes normalmente pueden pertenecer o estar integrados al Sistema de Gestión de la Seguridad de la Información (SGSI), normalmente estipulados y estandarizados bajo la norma ISO 27001:2013.

- **Plan de recuperación de desastres:** este plan es conocido como DRP (Disaster Recovery Plan), y está orientado a responder a incidentes, usualmente catastróficos, que puedan afectar la prestación de los servicios de información. Frecuentemente, el DRP se refiere a un plan enfocado en TI, diseñado para restaurar la operatividad de los sistemas, aplicaciones y bases de datos. Por otra parte, como parte del DRP, se cuenta generalmente con un sitio alternativo en donde se realizarán las operaciones, definidas por el BIA, que fueron interrumpidas por el incidente o desastre en el sitio principal. El alcance de un DRP puede confundirse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieran reubicación.

- **Planes de contingencia:** Según el NIST (National Institute of Standards and Technologies), los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y a recuperar los servicios críticos de TI, después de una interrupción, en el menor tiempo posible. Es factible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective: Tiempo Objetivo de Recuperación), muy cercano a cero. Los planes de contingencia son típicos en los canales de comunicaciones y servidores, de tal manera que, ante la falla de uno de estos canales o servidor, otro, entrará en operación muy rápidamente y, en muchos casos, de manera automatizada

Proyecto ISO 27001:2013	Avance del proyecto
Planes de Continuidad del Negocio	
Planes de recuperación ante desastres	
Planes de contingencia	
Planes para CIBERINCIDENTES	

Tabla 20. Proyectos Continuidad del Negocio.

6.14 A.18. CUMPLIMIENTO

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.

Definir procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados, en el marco de la Ley 719 de 2001.

Establecer una política de privacidad y protección de la información de datos personales, en el marco de la Ley 1581 de 2012 y mantener una capacitación continua sobre estas leyes con expertos en el tema.

Adicionalmente, como parte del ciclo de mejoramiento continuo del SGSI, la entidad debe garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales.

Proyecto ISO 27001:2013	Avance del proyecto
Capacitación continua sobre nuevas legislaciones ej. Habeas Data y Ley de Protección de Datos	
Auditorías externas de seguridad de la información	

Tabla 21. Proyectos de Cumplimiento.

7 DEFINICIONES

- **Activo:** En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Guía:** documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada:** (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros
- **Procedimiento:** Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).