INSTITUCIÓN UNIVERSITARIA DE ENVIGADO Ciencia , educación y desarrollo	**INFORME FINAL DE PRACTICA**	**Código: F-PI-38** **Versión: 02** **Pagina: 1**

FACULTAD DE INGENIERIAS

COORDINACIÓN DE PRÁCTICAS

ASPECTOS GENERALES DE LA PRÁCTICA.

Nombre del estudiante	**Julián Andrés Guisao Osorio**
Programa académico	**Ingeniería Electrónica**
Nombre de la Agencia o Centro de Práctica	**CADENA S.A**
NIT.	**890.930.534-0**
Dirección	**Carrera 50 No. 97A Sur - 150**
Teléfono	**57(4) 378 6666**
Dependencia o Área	**Seguridad de la Información**
Nombre Completo del Jefe del estudiante **Cargo**	**Daniel Pérez Martínez** **Coordinador de Seguridad de la Información**
Labor que desempeña el estudiante	**Apoyo para la implementación de la Norma ISO 27001**
Nombre del asesor de práctica	**Jimmy Collazos Franco**
Fecha de inicio de la práctica	**26/Julio/2017**
Fecha de finalización de la práctica	**26/Diciembre/2017**

ASPECTOS GENERALES DE LA PRÁCTICA.

1.1 Centro de práctica.

CADENA S.A,

Es una empresa que lleva en el mercado 35 años con el propósito de apoyar a las organizaciones a ser mejores y transformarse de la mano con nuestros clientes buscando innovar con productos y servicios para encontrar soluciones únicas a sus procesos críticos.

Esta Ofrece servicios de terceriza-ción de procesos de tecnología e información a través de 6 Unidades de Negocio:

- **Cadena - Relacionamiento:** Se lidera y apoyamos procesos de facturación y recaudo, medios directos, y comunicaciones inteligentes con nuestro modelo CCM. Cada mes imprimimos más de 60 millones de documentos y los distribuimos a más de 8 millones de hogares en todo el territorio nacional.
- **Cadena - Protección contra el fraude:** Se Cuenta con la más alta tecnología para impresión de juegos promocionales, raspas y etiquetas con códigos inteligentes de trazabilidad, gran capacidad offset para valores y para impresión, armado y personalización de pasaportes.
- **Cadena - Logística:** Se Tiene la capacidad de integrar los procesos logísticos con otros procesos de mercadeo, seguridad, impresión y gestión documental. Movilizando millones de unidades de manera segura y oportuna con tecnologías de trazabilidad y georreferenciación.
- **Cadena - Digital:** Se Ofrece soluciones digitales agiles y confiables. Acompañamos a las empresas a desarrollar juntos soluciones de automatización de procesos, digitalización y virtualización de flujos de información a través de formularios y tecnología.
- **Cadena - Suministros de oficina:** Se administra el proceso de formas y suministros de oficina de manera integral, inteligente y eficiente para clientes que operan en varias sedes y que están geográficamente dispersos.
- **Cadena - MSP:** Se entiende audiencias digitales, datos transaccionales y motivaciones del ser humano. Con base en esto desarrollamos planes de relacionamiento y programas de motivación para ayudar a nuestros clientes a lograr resultados de negocio efectivos.

La COMPAÑÍA apunta hacia la siguiente misión y visión:

MISIÓN.

En Cadena brindamos confiabilidad, apoyamos a las organizaciones a ser mejores, facilitando procesos críticos a través de información y tecnología en tres frentes de trabajo: seguridad y protección contra el fraude, logística y comercio electrónico y mercadeo y comunicaciones. Valoramos el respeto, la vocación de servicio, la confiabilidad, la flexibilidad y la innovación. Estamos profundamente comprometidos con un crecimiento rentable de la Compañía y contribuimos con el de nuestros clientes, buscando siempre el bienestar para todos los empleados, accionistas y las comunidades donde nos desempeñamos.

VISIÓN

Trabajamos para ser una compañía y un equipo que brinda confiabilidad. Con conocimiento, innovación, tecnología y un excelente servicio, somos la mejor opción de las empresas para desarrollar sus procesos críticos.

1.2 Objetivo de la práctica empresarial.

Cumplir con ley 1780 en la cual, realizando la práctica profesional en la empresa CADENA S.A; es requisito para la graduación de la carrera profesional

1.3 Funciones

- Realizar el análisis de aplicabilidad de los controles del anexo A de la norma ISO 27001.
- Realizar seguimiento a las áreas involucradas en el proceso de certificación de la ISO 27001.
- Reportar las novedades y hallazgos que se encuentren durante el proceso de análisis del sistema de gestión.
- Verificar la documentación que se requiere para la certificación del sistema de gestión de seguridad de la información, según la norma ISO 27001.
- Verificar la metodología del riesgo implantada en la compañía.

1.4 Justificación de la práctica empresarial.

CADENA S.A como entidad prestadora de servicios, con forme a la ley 789 del 2002, articulo 32 el cual menciona que: las personas naturales o jurídicas, que realicen cualquier tipo de actividad económica diferente de la construcción, que ocupen un número de trabajadores no inferior a quince (15), se encuentran obligadas a vincular aprendices para los oficios u ocupaciones que requieran formación académica o profesional metódica y completa en la actividad económica que desempeñan. Las empresas industriales y comerciales del Estado y las de Economía mixta del orden Nacional, departamental, distrital y municipal, estarán obligadas a la vinculación de aprendices en los términos de esta ley.

CADENA S.A debe contratar aprendices con el fin de promover y apoyar el trabajo. El número de aprendices o practicantes dependerá del número de empleados con el que cuente la empresa, es decir, para empresas por cada 20 trabajadores deberá contratar 1 practicante y uno adicional por fracción de diez (10) o superior que no exceda de veinte. Las Empresas que tengan entre quince (15) y veinte (20) trabajadores, tendrán un aprendiz. Así mismo en calidad de estudiante de la institución universitaria de envigado se debe realizar como requisito un trabajo de grado o practica en el cual se ponga a prueba la calidad del aprendizaje adquirido durante toda la carrera.

Lo más importante al realizar la práctica empresarial es adquirir conocimiento y experiencia laboral. es por esto que se cuenta con 6 meses realizando las prácticas laborales, para aplicar los conocimientos adquiridos en la universidad y de igual forma la empresa se beneficia en dos aspectos:

1. Cumplir un requisito legal.

2. Con el trabajo desarrollado por cada practicante.

1.5 Equipo de trabajo.

NOMBRE	CARGO
Daniel Pérez Martínez	**Coordinador de la Seguridad de la Información**
Julián Andrés Guisao Osorio	**Aprendiz**

2. PROPUESTA PARA LA AGENCIA O CENTRO DE PRÁCTICAS

2.1 Título de la propuesta.

Analizar el sistema de gestión de la seguridad de la información basado en la norma ISO 27001.

2.2 Planteamiento del problema.

En CADENA S.A empresa del sector privado, la cual se especializa en la producción masiva de documentación física como facturación y recaudo, medios directos, y comunicaciones inteligentes con modelo CCM, la impresión de juegos promocionales, raspas y etiquetas con códigos inteligentes de trazabilidad, gran capacidad offset para valores y para impresión, armado y personalización de pasaportes, además de integrar los procesos logísticos con otros procesos de mercadeo, seguridad, impresión y gestión documental, soluciones digitales agiles y confiables. Acompañando a las empresas a desarrollar juntos soluciones de automatización de procesos, digitalización y virtualización de flujos de información a través de formularios y tecnología, mediante sus unidades estratégicas de negocios

- Cadena – Relacionamiento.

- Cadena – Protección contra el Fraude.
- Cadena – Relacionamiento.
- Cadena – Logística.
- Cadena – Digital.
- Cadena – MSP.

La empresa en este momento se encuentra en la búsqueda de la certificación ISO 27001, Sistema de Gestión de Seguridad de la Información, como meta para enero del año próximo, cumpliendo así con los requisitos impuestos por la DIAN, según el decreto 2242 del 2015; generando valor y confianza en los clientes y potenciando las futuras ventas en su UEN Digital.

Por esto se debe analizar el sistema de gestión de seguridad de la información que actualmente aplican y compararlo con la norma ISO 27001, para avanzar en el proceso de certificación de su sistema de gestión

2.3 Justificación.

Cadena empresa con 35 años de conformación, dedicada a apoyar a las organizaciones a ser mejores y transformarse de la mano con los clientes buscando innovar con productos y servicios para encontrar soluciones únicas a sus procesos críticos a través de sus 6 unidades de negocio.

- Cadena - Relacionamiento.
- Cadena – Protección contra fraudes.
- Cadena – Logística.
- Cadena – Digital.
-
- Cadena – Suministros de oficina.
- Cadena – MSP

Con la misión de brindar confiabilidad y seguridad y así poder ofrecer bienestar a los empleados, socios, clientes y comunidades donde se desempeña, se adquirió un compromiso de parte de la alta dirección con la DIAN de implementar y certificar su sistema de gestión de seguridad de la información ISO 27001 y dar tranquilidad del manejo de la información personal de sus clientes, esto se convertiría en un plus mas para los servicios que ofrece la compañía y para la alta dirección el saber que su sistema de gestión de seguridad de la información trabaja conforme con la certificación ISO 27001.

El sistema de gestión de seguridad de la información son una serie de políticas, procedimientos, y manuales los cuales apuntan asegurar todos los medios y canales por los cuales se transmite información sea internamente como externamente, y poder certificar el sistema de gestión reconoce

que se está realizando una excelente labor con la seguridad de la información, da un parte de tranquilidad a la compañía y se tiene que un excelente know how de cara con los clientes.

2.4 Objetivos (Objetivo General y Objetivos Específicos).

Objetivo General.

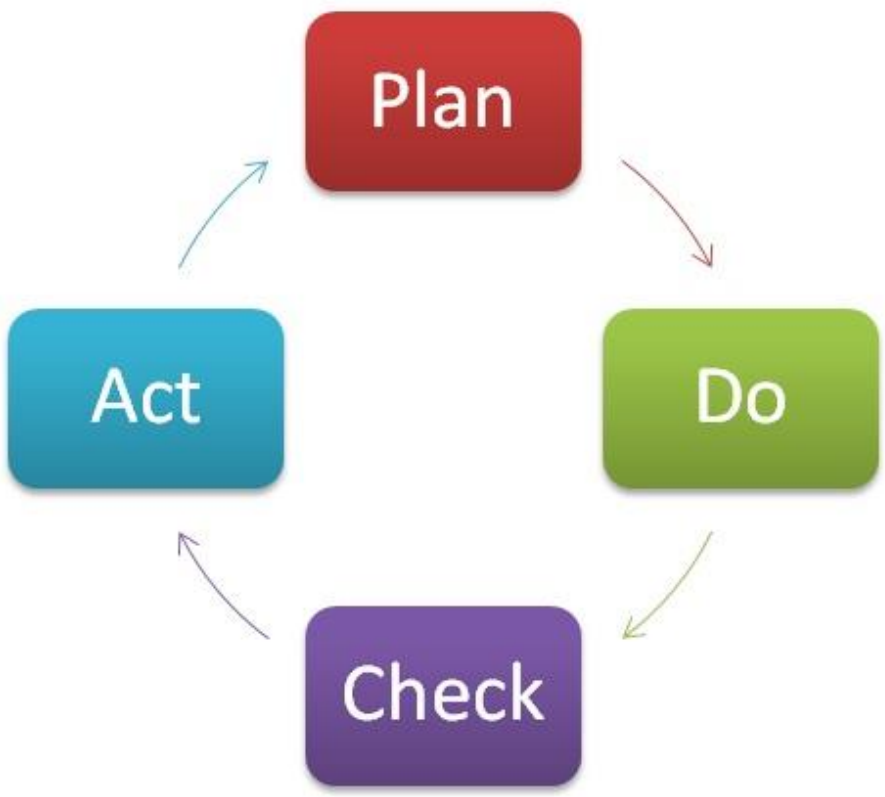
Analizar el sistema de gestión de seguridad de la información implantado en CADENA S.A; basado en la norma internacional ISO 27001 Sistema de Gestión en Seguridad de la Información (SGSI); Y así aplicar para la certificación de su sistema de gestión de riesgos con el alcance inicial en la UEN Digital y cumplir con el compromiso adquirido ante la DIAN

Objetivos Específicos.

- Interpretar toda la documentación que tiene la norma internacional ISO 27000; haciendo diagramas de flujo, listas de chequeo y reuniones periódicas con los especialistas; comprendiendo los requisitos y la mejor forma de gestionar el sistema y la metodología del riesgo que actualmente se encuentra implementada.
- Realizar un análisis de los controles existentes en la compañía VS los controles sugeridos por la norma; mediante una metodología brecha la cual busca el estado de madurez de cada control existente y sí se requiere demás controles sugeridos por la norma; finalmente los controles faltantes deben ser evaluados para buscar su aplicabilidad.
- Diagnosticar el estado actual del sistema de gestión de la seguridad de la información; basado en la norma ISO 27000 y todos sus anexos; para una futura recomendación en la certificación de la norma ISO 27000

2.5 Diseño Metodológico.

El método que se realizara para el análisis del sistema de gestión de la empresa CADENA S.A es el círculo de Deming o ciclo de mejoramiento continuo.



Las 4 etapas que lo conforman son:

1. Planificar (Plan): Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc.

2. Hacer (Do): Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

3. Controlar o Verificar (Check): Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados.

4. Actuar (Act): Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

Este método fue el sugerido por parte de la COMPAÑÍA, ya que todos los proyectos anteriores fueron realizados con la misma metodología.

2.6 Cronograma de Actividades.

			2017					
#	DESCRIPCION	TIEMPO	JUL	AGO	SEP	OCT	NOV	DIC
1	Leer documentación	1 mes						
2	Revisar la aplicabilidad de la metodologia del riesgo	1 mes						
3	Revisar los controles del plan de tratamiento	2 meses						
4	Auditar el proceso de UEN Digital	1 mes						
5	Retroalimentación de la auditoria	1 mes						
6	Revisar la mejora de los hallagos de la auditoria	2 meses						

2.7 Presupuesto (Ficha de presupuesto)

CANT	DESCRIPCIÓN	VALOR	TOTAL
2	Personal	$ 1.700.000	$ 10.200.000
2	Computadores	$ 1.000.000	$ 2.000.000
1	Espacio de trabajo	$ 1.000.000	$ 6.000.000
Total			$ 18.200.000

3. DESARROLLO DE LA PROPUESTA.

3.1 MARCO DE REFERENCIA (antecedentes, marco teórico, marco conceptual, Marco legal.

3.2 Desarrollo y logro de objetivos.

En la primera fase de la práctica, se realiza una lectura de la documentación relacionada con la norma ISO 27000, sistema de gestión de seguridad de la información, buscando entender los requerimientos que debe tener una empresa para la implementación, del la norma se logro identificar el listado de requerimientos para la implementación.

ID CONTROL	CLAUSULA
4.0	**CONTEXTO DE LA ORGANIZACIÓN**
4.1	Conocimiento de la organización y su contexto
4.2	Comprensión de las necesidades y expectativas de las partes interesadas
4.3	Determinación del alcance del SGSI
4.4	Sistema de gestión de seguridad de la información
5.0	**LIDERAZGO**
5.1	Liderazgo y compromisos
5.2	Políticas
5.3	Roles, responsabilidades y autoridades de la organización
6.0	**PLANIFICACION**
6.1	Acciones para tratar riesgos y oportunidades
6.1.1	Generalidades
6.1.2	Evaluación de riesgos de la seguridad de la información
6.1.3	Tratamiento de riesgos de la seguridad de la información
6.2	Objetivos de la seguridad de la información y planes logrados
7.0	**SOPORTES**
7.1	Recursos
7.2	Competencia
7.3	Toma de conciencia
7.4	Comunicación
7.5	Información documentada
7.5.1	Generalidades
7.5.2	Creación y actualización
7.5.3	Control de la información documentada
8.0	**OPERACIÓN**
8.1	Planificación y control operacional
8.2	Evaluación de riesgo de la seguridad de la información
8.3	Tratamiento de riesgos de la seguridad de la información
9.0	**EVALUACION Y DESEMPEÑO**
9.1	Seguimiento, medición, análisis y evaluación
9.2	Auditoria interna
9.3	Revisión por la dirección
10.0	**MEJORA**
10.1	No conformidades y acciones correctivas
10.2	Mejora continua

	ANEXO A
A.5	**POLITICA DE LA SEGURIDAD DE LA INFORMACION**
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información
A.5.1.1	Políticas de seguridad de la información
A.5.1.2	Revisión de las políticas para seguridad de la información
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**
A.6.1	Organización Interna
A.6.1.1	Seguridad de la información roles y responsabilidades
A.6.1.2	Separación de deberes
A.6.1.3	Contacto con autoridades
A.6.1.4	Contacto con grupos de interés especial
A.6.1.5	Seguridad de la información en gestión de proyectos
A.6.2	**DISPOSITIVOS MOVILES Y TELETRABAJO**
A6.2.1	Política para dispositivos móviles
A.6.2.2	Teletrabajo
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**
A.7.1	Antes de asumir el empleo
A.7.1.1	Selección
A.7.1.2	Términos y condiciones del empleo
A.7.2	**DURANTE LA EJECUCION DEL EMPLEO**
A.7.2.1	Responsabilidad de la dirección
A.7.2.2	Toma de conciencia, educación y formación de la seguridad de la Información
A.7.2.3	Proceso disciplinario
A.7.3	**TERMINACION Y CAMBIO DE EMPLEO**
A.7.3.1	Terminación o cambio de responsabilidades de empleo
A.8	**GESTION DE ACTIVOS**
A.8.1	**RESPONSABILIDAD POR LOS ACTIVOS**
A.8.1.1	Inventario de Activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de activos
A.8.2	**CLASIFICACIÓN DE LA INFORMACIÓN**
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A8.2.3	Manejo de activos
A.8.3	**MANEJO DE MEDIOS DE SOPORTE**
A.8.3.1	Gestión de medios de soporte removibles
A.8.3.2	Disposición de los medios de soporte
A.8.3.3	Transferencia de medios de soporte físicos
A.9	**CONTROL DE ACCESO**
A.9.1	Requisitos del negocio para el control de acceso
A.9.1.1	Políticas del control de acceso
A.9.1.2	Acceso a redes y a servicios de red

A.9.2	**GESTION DE ACCESO A USUARIOS**
A.9.2.1	Registro y cancelación de registros de usuarios
A.9.2.2	Suministros de acceso de usuarios
A.9.2.3	Gestión de derechos de acceso privilegiados
A.9.2.4	Gestión de la información de autenticación secreta de usuarios
A.9.2.5	Revisión de los derechos de accesos de usuarios
A.9.2.6	Cancelación o ajustes de los derechos de usuarios
A.9.3	**RESPONSABILIDADES DEL USUARIO**
A.9.3.1	Uso de información secreta
A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**
A.9.4.1	Restricción de acceso a la información
A.9.4.2	Procedimiento de conexión segura
A.9.4.3	Sistema de gestión de contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados
A.9.4.5	Control de acceso a códigos fuentes de los programas
A.10	**CRIPTOLOGIA**
A.10.1	Controles Criptográficos
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de claves
A.11	**SEGURIDAD FISICA Y AMBIENTAL**
A.11.1	Áreas seguras
A.11.1.1	Perímetros de seguridad física
A.11.1.2	Controles físicos de entrada
A.11.1.3	Seguridad de oficinas, salones e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales
A.11.1.5	Trabajo en área segura
A.11.1.6	Áreas de despacho y carga
A.11.2	**EQUIPOS**
A.11.2.1	Ubicación y protección de los equipos
A.11.2.2	Servicios públicos de soporte
A.11.2.3	Seguridad de cableado
A.11.2.4	Mantenimiento de equipos
A.11.2.5	Retiro de activos
A.11.2.6	Seguridad de equipos y activos fuera del predio
A.11.2.7	Disposición segura o reutilización de equipos
A.11.2.8	Equipos sin supervisión de usuarios
A.11.2.9	Política de escritorio limpio y pantalla limpia
A.12	**SEGURIDAD DE LAS OPERACIONES**
A.12.1	Procedimientos operacionales y responsabilidades
A.12.1.1	Procedimiento de operación documentada
A.12.1.2	Gestión de cambio
A.12.1.3	Gestión de capacidad
A.12.1.4	Separación de los ambientes de desarrollo, ensayo y operación

A.12.2	**PROTECCIÓN CONTRA CODIGO MALICIOSO**
A.12.2.1	Controles contra código malicioso
A.12.3	**COPIAS DE RESPALDO**
A.12.3.1	Copias de respaldo de la información
A.12.4	**REGISTROS Y SEGUIMIENTOS**
A.12.4.1	Registro de eventos
A.12.4.2	Protección de la información de registro
A.12.4.3	Registro del administrador y del operador
A.12.4.4	Sincronización de relojes
A.12.5	**CONTROL DEL SOFTWARE OPERACIONAL**
A.12.5.1	Instalación de software en los sistemas operativos
A.12.6	**GESTION DE VULNERABILIDADES TECNICAS**
A.12.6.1	Gestión de vulnerabilidades técnicas
A.12.6.2	Restricción sobre la instalación de software
A.12.7	**CONSIDERACIONES DE AUDITORIA SOBRE EL SISTEMA DE INFORMACION**
A.12.7.1	Controles sobre las auditorias de sistemas de información
A.13	**SEGURIDAD DE LAS COMUNICACIONES**
A.13.1	Gestión de seguridad de redes
A.13.1.1	Controles de redes
A.13.1.2	Seguridad de los servicios de redes
A.13.1.3	Separación de las redes
A.13.2	**TRANSPARECIA EN LA INFORMACION**
A.13.2.1	Políticas y procedimientos de transferencias de información
A.13.2.2	Acuerdos sobre transferencias de información
A.13.2.3	Mensajes electrónicos
A.13.2.4	Acuerdo de confidencialidad y de no divulgación
A.14	**ADQUISICION, DESARROLLO Y MANTENIMIENTOS DEL SISTEMA**
A.14.1	Requisitos de seguridad de los sistemas de información
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas
A.14.1.3	Protección de transacciones de servicios de aplicaciones
A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**
A.14.2.1	Políticas de desarrollo seguro
A.14.2.2	Procedimiento de control de cambios de sistemas
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones
A.14.2.4	Restricciones sobre los cambios de paquete de software
A.14.2.5	Principios de construcción de sistemas seguro
A.14.2.6	Ambiente de desarrollo seguro
A.14.2.7	Desarrollo contratado externamente
A.14.2.8	Pruebas de seguridad de los sistemas
A.14.2.9	Pruebas de aceptación de sistemas
A.14.3	**DATOS DE ENSAYO**

A.14.3.1	Protección de datos de ensayo
A.15	**RELACIONES CON LOS PROVEEDORES**
A.15.1	Seguridad de la información en relaciones con los proveedores
A.15.1.1	Políticas de seguridad de la información para las relaciones con los proveedores
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores
A.15.1.3	Cadena de suministros de tecnología de la información y comunicación
A.15.2	**GESTION DE LA PRESTACION DE SERVICIOS CON LOS PROVEEDORES**
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores
A.15.2.2	Gestión de cambios a los servicios de los proveedores
A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Informes de eventos de seguridad de la información
A.16.1.3	Informe de debilidades de seguridad de la información
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.16.1.6	Aprendizaje obtenido de los incidentes de la información
A.16.1.7	Recolección de evidencia
A.17	**ASPECTO DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DE NEGOCIO**
A.17.1	Continuidad de seguridad de la información
A.17.1.1	Planificación de la continuidad de la seguridad de la información
A.17.1.2	Implementación de la continuidad de la seguridad de la información
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la información
A.17.2	**REDUNDANCIA**
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información
A.18	**CUMPLIMIENTO**
A.18.1	Cumplimiento de requisitos legales y contractuales
A.18.1.1	Identificación de los requisitos de la legislación y contractuales aplicables
A.18.1.2	Derechos de propiedad intelectual
A.18.1.3	Protección de registros
A.18.1.4	Privacidad y protección de la información identificable personalmente
A.18.1.5	Reglamentación de controles criptográficos
A.18.2	**REVISIONES DE SEGURIDAD DE LA INFORMACION**
A.18.2.1	Revisión independiente de la seguridad de la información
A.18.2.2	Cumplimiento con las políticas y normas de seguridad
A.18.2.3	Revisión de cumplimiento técnico

La anterior lista se divide en:

Dominios: Son 21 dominios, están resaltados en negrilla y son los títulos de los puntos a implementar

Controles: Son 140 controles, y se identifican porque comienzan con la letra A.

Documentación obligatoria: Es la documentación que debe presentarse al ente certificador y se identifican porque van después de los dominios.

adicional a esto se realizó la lectura de los libros:

Implantación de un sistema de gestión de seguridad de la información según ISO 27001 un enfoque práctico, cristina merino bada, Ricardo cañizares sales, ed. FC editorial.

Este trata desde un enfoque practico todo el tema de la implementación con ejemplos claros, y de campo.

De este libro se obtiene la metodología la siguiente tabla de un modelo de madurez.

DESCRIPTOS	DESCRIPCION
Total, Falta de proceso reconocible	Inexistente
No hay procesos estandarizados, pero hay métodos	Iniciado
Hay documentación y estándar, pero hay carencia de seguimiento	Definido
Es posible medir y documentar el seguimiento	Gestionado
Los procesos han sido depurados hasta su máxima optimización	Optimizado

De este modelo se hablará más adelante.

Se realizan reuniones de gestión para definir la forma de desplegar la metodología del riesgo definida por la compañía, la cual basada en:

Análisis del riesgo. Es un proceso de identificar los riesgos de seguridad que podrían impedir a la compañía lograr sus objetivos. Esta actividad se divide en las siguientes tareas

1. Identificar los activos
2. Identificar las amenazas
3. Identificar las vulnerabilidades
4. Identificar el impacto
5. Obtener el riesgo intrínseco
6. Identificar las salvaguardas
7. Obtener el riesgo residual

Cada proceso de debe identificar las respuestas a cada una de las tareas anteriormente descrita y llenar los formatos respectivos

En el análisis brecha se tiene ya aplicado las dos primeras tablas.

ID CONTROL	CLAUSULA	NIVEL DE MADUREZ
4.0	**CONTEXTO DE LA ORGANIZACIÓN**	
4.1	Conocimiento de la organización y su contexto	**Iniciado**
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	**Iniciado**
4.3	Determinación del alcance del SGSI	**Iniciado**
4.4	Sistema de gestión de seguridad de la información	**Iniciado**
5.0	**LIDERAZGO**	
5.1	Liderazgo y compromisos	**Iniciado**
5.2	Políticas	**Gestionado**
5.3	Roles, responsabilidades y autoridades de la organización	**Gestionado**
6.0	**PLANIFICACION**	
6.1	Acciones para tratar riesgos y oportunidades	**Iniciado**
6.1.1	Generalidades	**Iniciado**
6.1.2	Evaluación de riesgos de la seguridad de la información	**Iniciado**
6.1.3	Tratamiento de riesgos de la seguridad de la información	**Iniciado**
6.2	Objetivos de la seguridad de la información y planes logrados	**Optimizado**
7.0	**SOPORTES**	
7.1	Recursos	**Iniciado**
7.2	Competencia	**Definido**
7.3	Toma de conciencia	**Gestionado**
7.4	Comunicación	**Gestionado**
7.5	Información documentada	**Gestionado**
7.5.1	Generalidades	**Gestionado**
7.5.2	Creación y actualización	**Iniciado**
7.5.3	Control de la información documentada	**Iniciado**
8.0	**OPERACIÓN**	
8.1	Planificación y control operacional	**Optimizado**
8.2	Evaluación de riesgo de la seguridad de la información	**Iniciado**
8.3	Tratamiento de riesgos de la seguridad de la información	**Iniciado**
9.0	**EVALUACION Y DESEMPEÑO**	
9.1	Seguimiento, medición, análisis y evaluación	**Inexistente**
9.2	Auditoria interna	**Iniciado**
9.3	Revisión por la dirección	**Inexistente**
10.0	**MEJORA**	
10.1	No conformidades y acciones correctivas	**Inexistente**
10.2	Mejora continua	**Definido**
	ANEXO A	
A.5	**POLITICA DE LA SEGURIDAD DE LA INFORMACION**	
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información	

A.5.1.1	Políticas de seguridad de la información	**Optimizado**
A.5.1.2	Revisión de las políticas para seguridad de la información	**Gestionado**
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	Organización Interna	
A.6.1.1	Seguridad de la información roles y responsabilidades	**Optimizado**
A.6.1.2	Separación de deberes	**Optimizado**
A.6.1.3	Contacto con autoridades	**Optimizado**
A.6.1.4	Contacto con grupos de interés especial	**Optimizado**
A.6.1.5	Seguridad de la información en gestión de proyectos	**Optimizado**
A.6.2	**DISPOSITIVOS MOVILES Y TELETRABAJO**	
A6.2.1	Política para dispositivos móviles	**Gestionado**
A.6.2.2	Teletrabajo	**Optimizado**
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	Antes de asumir el empleo	**Optimizado**
A.7.1.1	Selección	**Optimizado**
A.7.1.2	Términos y condiciones del empleo	**Optimizado**
A.7.2	**DURANTE LA EJECUCION DEL EMPLEO**	
A.7.2.1	Responsabilidad de la dirección	**Definido**
A.7.2.2	Toma de conciencia, educación y formación de la seguridad de la Información	**Gestionado**
A.7.2.3	Proceso disciplinario	**Optimizado**
A.7.3	**TERMINACION Y CAMBIO DE EMPLEO**	
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**Definido**
A.8	**GESTION DE ACTIVOS**	
A.8.1	**RESPONSABILIDAD POR LOS ACTIVOS**	
A.8.1.1	Inventario de Activos	**Gestionado**
A.8.1.2	Propiedad de los activos	**Optimizado**
A.8.1.3	Uso aceptable de los activos	**Optimizado**
A.8.1.4	Devolución de activos	**Optimizado**
A.8.2	**CLASIFICACIÓN DE LA INFORMACIÓN**	
A.8.2.1	Clasificación de la información	**Optimizado**
A.8.2.2	Etiquetado de la información	**Optimizado**
A8.2.3	Manejo de activos	**Optimizado**
A.8.3	**MANEJO DE MEDIOS DE SOPORTE**	
A.8.3.1	Gestión de medios de soporte removibles	**Optimizado**
A.8.3.2	Disposición de los medios de soporte	**Definido**
A.8.3.3	Transferencia de medios de soporte físicos	**Definido**
A.9	**CONTROL DE ACCESO**	
A.9.1	Requisitos del negocio para el control de acceso	
A.9.1.1	Políticas del control de acceso	**Optimizado**
A.9.1.2	Acceso a redes y a servicios de red	**Optimizado**
A.9.2	**GESTION DE ACCESO A USUARIOS**	
A.9.2.1	Registro y cancelación de registros de usuarios	**Definido**

A.9.2.2	Suministros de acceso de usuarios	**Definido**
A.9.2.3	Gestión de derechos de acceso privilegiados	**Definido**
A.9.2.4	Gestión de la información de autenticación secreta de usuarios	**Definido**
A.9.2.5	Revisión de los derechos de accesos de usuarios	**Definido**
A.9.2.6	Cancelación o ajustes de los derechos de usuarios	**Definido**
A.9.3	**RESPONSABILIDADES DEL USUARIO**	
A.9.3.1	Uso de información secreta	**Definido**
A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	
A.9.4.1	Restricción de acceso a la información	**Definido**
A.9.4.2	Procedimiento de conexión segura	**Iniciado**
A.9.4.3	Sistema de gestión de contraseñas	**Optimizado**
A.9.4.4	Uso de programas utilitarios privilegiados	**Optimizado**
A.9.4.5	Control de acceso a códigos fuentes de los programas	**Iniciado**
A.10	**CRIPTOLOGIA**	
A.10.1	Controles Criptográficos	
A.10.1.1	Política sobre el uso de controles criptográficos	**Optimizado**
A.10.1.2	Gestión de claves	**Inexistente**
A.11	**SEGURIDAD FISICA Y AMBIENTAL**	
A.11.1	Áreas seguras	
A.11.1.1	Perímetros de seguridad física	**Gestionado**
A.11.1.2	Controles físicos de entrada	**Optimizado**
A.11.1.3	Seguridad de oficinas, salones e instalaciones	**Optimizado**
A.11.1.4	Protección contra amenazas externas y ambientales	**Optimizado**
A.11.1.5	Trabajo en área segura	**Optimizado**
A.11.1.6	Áreas de despacho y carga	**Optimizado**
A.11.2	**EQUIPOS**	
A.11.2.1	Ubicación y protección de los equipos	**Inexistente**
A.11.2.2	Servicios públicos de soporte	**Inexistente**
A.11.2.3	Seguridad de cableado	**Inexistente**
A.11.2.4	Mantenimiento de equipos	**Inexistente**
A.11.2.5	Retiro de activos	**Gestionado**
A.11.2.6	Seguridad de equipos y activos fuera del predio	**Inexistente**
A.11.2.7	Disposición segura o reutilización de equipos	**Definido**
A.11.2.8	Equipos sin supervisión de usuarios	**Definido**
A.11.2.9	Política de escritorio limpio y pantalla limpia	**Optimizado**
A.12	**SEGURIDAD DE LAS OPERACIONES**	
A.12.1	Procedimientos operacionales y responsabilidades	
A.12.1.1	Procedimiento de operación documentada	**Iniciado**
A.12.1.2	Gestión de cambio	**Optimizado**
A.12.1.3	Gestión de capacidad	**Optimizado**
A.12.1.4	Separación de los ambientes de desarrollo, ensayo y operación	**Gestionado**
A.12.2	**PROTECCIÓN CONTRA CODIGO MALICIOSO**	
A.12.2.1	Controles contra código malicioso	**Optimizado**

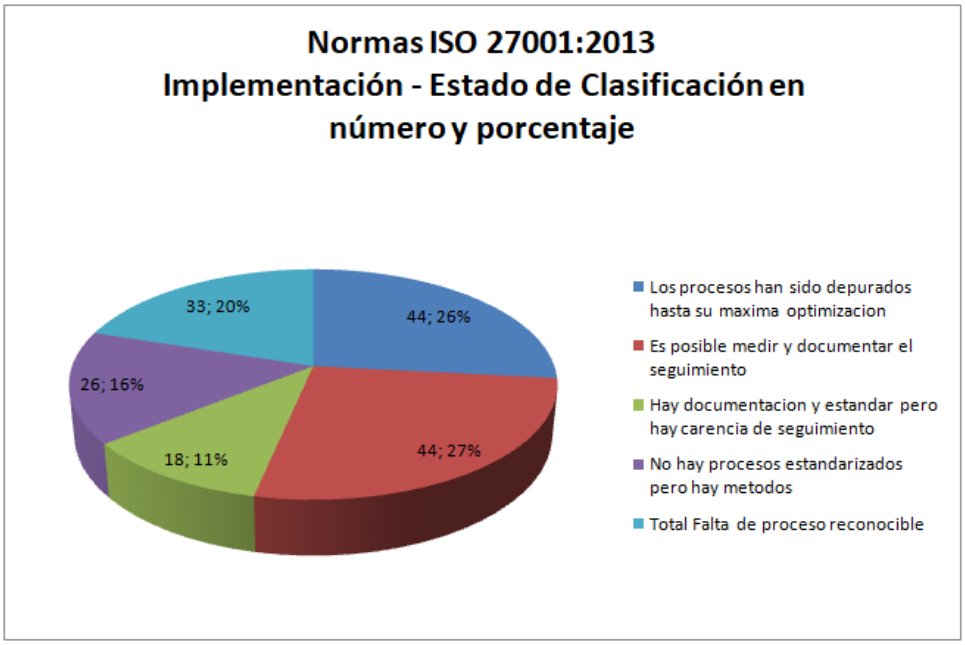
A.12.3	**COPIAS DE RESPALDO**	
A.12.3.1	Copias de respaldo de la información	**Gestionado**
A.12.4	**REGISTROS Y SEGUIMIENTOS**	
A.12.4.1	Registro de eventos	**Gestionado**
A.12.4.2	Protección de la información de registro	**Gestionado**
A.12.4.3	Registro del administrador y del operador	**Iniciado**
A.12.4.4	Sincronización de relojes	**Definido**
A.12.5	**CONTROL DEL SOFTWARE OPERACIONAL**	
A.12.5.1	Instalación de software en los sistemas operativos	**Optimizado**
A.12.6	**GESTION DE VULNERABILIDADES TECNICAS**	
A.12.6.1	Gestión de vulnerabilidades técnicas	**Optimizado**
A.12.6.2	Restricción sobre la instalación de software	**Gestionado**
A.12.7	**CONSIDERACIONES DE AUDITORIA SOBRE EL SISTEMA DE INFORMACION**	
A.12.7.1	Controles sobre las auditorias de sistemas de información	**Iniciado**
A.13	**SEGURIDAD DE LAS COMUNICACIONES**	
A.13.1	Gestión de seguridad de redes	
A.13.1.1	Controles de redes	**Optimizado**
A.13.1.2	Seguridad de los servicios de redes	**Inexistente**
A.13.1.3	Separación de las redes	**Iniciado**
A.13.2	**TRANSPARECIA EN LA INFORMACION**	
A.13.2.1	Políticas y procedimientos de transferencias de información	**Optimizado**
A.13.2.2	Acuerdos sobre transferencias de información	**Inexistente**
A.13.2.3	Mensajes electrónicos	**Optimizado**
A.13.2.4	Acuerdo de confidencialidad y de no divulgación	**Iniciado**
A.14	**ADQUISICION, DESARROLLO Y MANTENIMIENTOS DEL SISTEMA**	
A.14.1	Requisitos de seguridad de los sistemas de información	
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	**Inexistente**
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	**Inexistente**
A.14.1.3	Protección de transacciones de servicios de aplicaciones	**Inexistente**
A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**	
A.14.2.1	Políticas de desarrollo seguro	**Inexistente**
A.14.2.2	Procedimiento de control de cambios de sistemas	**Inexistente**
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	**Inexistente**
A.14.2.4	Restricciones sobre los cambios de paquete de software	**Inexistente**
A.14.2.5	Principios de construcción de sistemas seguro	**Inexistente**
A.14.2.6	Ambiente de desarrollo seguro	**Inexistente**
A.14.2.7	Desarrollo contratado externamente	**Gestionado**
A.14.2.8	Pruebas de seguridad de los sistemas	**Gestionado**
A.14.2.9	Pruebas de aceptación de sistemas	**Gestionado**
A.14.3	**DATOS DE ENSAYO**	

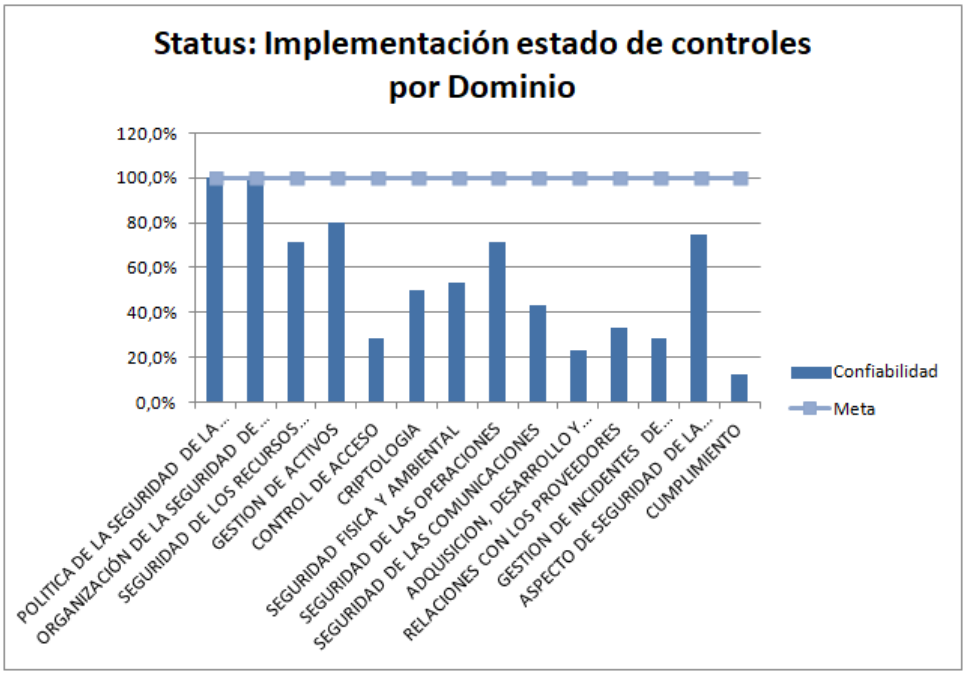
A.14.3.1	Protección de datos de ensayo	**Inexistente**
A.15	**RELACIONES CON LOS PROVEEDORES**	
A.15.1	Seguridad de la información en relaciones con los proveedores	**Gestionado**
A.15.1.1	Políticas de seguridad de la información para las relaciones con los proveedores	**Inexistente**
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**Inexistente**
A.15.1.3	Cadena de suministros de tecnología de la información y comunicación	**Iniciado**
A.15.2	**GESTION DE LA PRESTACION DE SERVICIOS CON LOS PROVEEDORES**	
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**Gestionado**
A.15.2.2	Gestión de cambios a los servicios de los proveedores	**Inexistente**
A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	
A.16.1.1	Responsabilidades y procedimientos	**Optimizado**
A.16.1.2	Informes de eventos de seguridad de la información	**Optimizado**
A.16.1.3	Informe de debilidades de seguridad de la información	**Inexistente**
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**Inexistente**
A.16.1.5	Respuesta a incidentes de seguridad de la información	**Inexistente**
A.16.1.6	Aprendizaje obtenido de los incidentes de la información	**Inexistente**
A.16.1.7	Recolección de evidencia	**Definido**
A.17	**ASPECTO DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE LA CONTINUIDAD DE NEGOCIO**	
A.17.1	Continuidad de seguridad de la información	
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**Optimizado**
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**Optimizado**
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la información	**Inexistente**
A.17.2	**REDUNDANCIA**	
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	**Optimizado**
A.18	**CUMPLIMIENTO**	
A.18.1	Cumplimiento de requisitos legales y contractuales	
A.18.1.1	Identificación de los requisitos de la legislación y contractuales aplicables	**Inexistente**
A.18.1.2	Derechos de propiedad intelectual	**Gestionado**
A.18.1.3	Protección de registros	**Inexistente**
A.18.1.4	Privacidad y protección de la información identificable personalmente	**Iniciado**
A.18.1.5	Reglamentación de controles criptográficos	**Iniciado**
A.18.2	**REVISIONES DE SEGURIDAD DE LA INFORMACION**	
A.18.2.1	Revisión independiente de la seguridad de la información	**Inexistente**
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**Inexistente**
A.18.2.3	Revisión de cumplimiento técnico	**Iniciado**

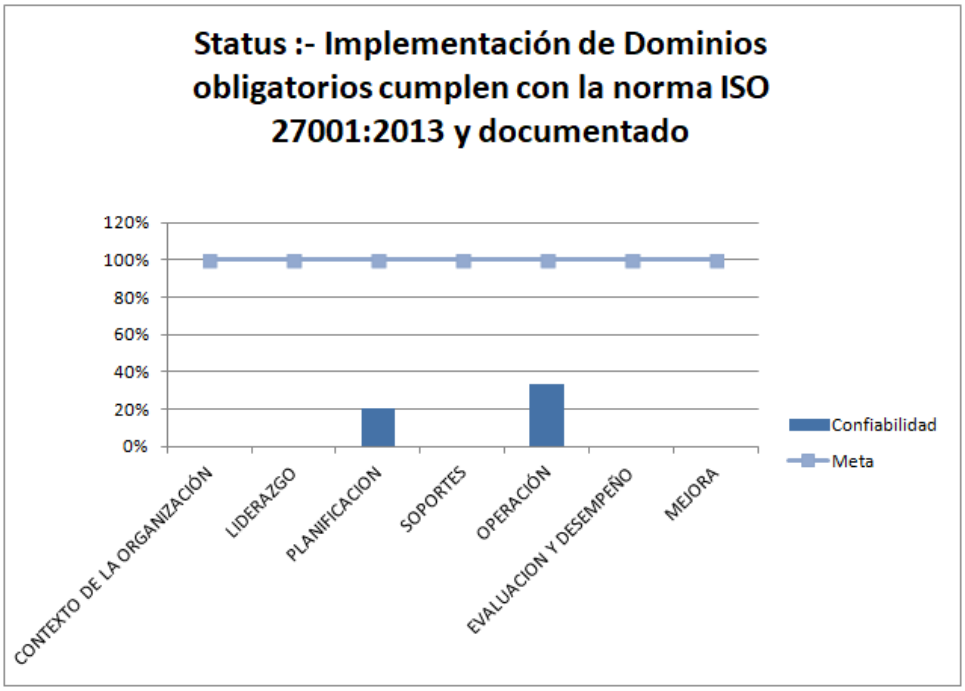
Y se atacan los estados de madurez que se encuentren en los siguientes estados:

1. Inexistente
2. Iniciado
3. Definido

Buscando siempre que el mínimo estado sea el gestionado, finalmente el atacar todo estos estados me arrojan los siguientes indicadores.







Donde la meta de cada indicador es el 100%, pero si los indicadores son mayores al 90 % se puede recomendar una certificación del sistema de gestión de seguridad de la información

4. CONCLUSIONES.

Es importante definir la estrategia idónea para abordar un proyecto, esto ayudara a optimizar los tiempos de ejecución de las etapas, comprender el que se hará y como se realizara, el analizar los diferentes estados del proyecto, y a tomar decisiones antes, durante y después de la realización de los mismos.

Realizando un análisis del estado actual de sistema de gestión de seguridad de la información de la compañía, se pudo medir el nivel de madurez del sistema, y así se identificaron las fortalezas y las oportunidades de mejora, definiendo finalmente los controles a implantar para hacer más asertivo al sistema de gestión de seguridad de la información de la compañía.

Realizar mediciones de los alcances, etapas y tareas, facilitan identificar los estados de madurez del proyecto, ayudan con la optimización del tiempo y finalmente son las que definen si se cumplir las metas dentro de los tiempos definidos.

Finalmente, el sistema de gestión de seguridad de la información que se encuentra definido en la compañía, cumple un nivel de madurez bueno para solicitar la acreditación de ISO 27001:2013 de parte de un ente.

5. RECOMENDACIONES.

El sistema de gestión de seguridad de la información requiere un mantenimiento y sostenimiento, actualmente existen en el mercado muchas herramientas que permiten automatizar muchas de las tareas que actualmente son manuales, o tener un responsable del sistema es la recomendación más optima

6. REFERENCIAS BIBLIOGRÁFICAS

Firma del estudiante: _____

Firma del asesor:_____

Firma del jefe en el Centro de Práctica: _____

NOTA IMPORTANTE: Los informes presentados deben estar acorde con la normas APA