PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – PESI – 2019-2022

FASE I (INICIO-CONTEXTO-SITUACION ACTUAL- METODOLOGIA)
FASE II (NIVEL DE MADUREZ DEL MSPI)

Elaborado por: Julián Adolfo Vásquez Ospina – Asesor de Informática
Revisado Por: Comité de Gobierno Digital – INCIVA
Aprobado Por: Jonathan Velásquez Álzate – Director del INCIVA

OFICINA ASESORA DE INFORMATICA
OCTUBRE DE 2019

TABLA DE CONTENIDO

FASE I

FASE II

1. INTRODUCCION

El INCIVA como ente descentralizado de la Gobernación del Valle, está en la obligación de cumplir la política de gobierno digital impuesta en el decreto No 1008 del 14 de junio del 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Que en la política de gobierno digital en su artículo 2.2.9.1.1.3 –Principios, tiene como prioridad la seguridad de la información, el cual dice así textualmente: “Este principio busca crear condiciones de uso confiable V en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano”.

La oficina asesora de informática en conjunto con la oficina asesora de planeación, vienen actualizando los riesgos informáticos que puedan afectar las labores de los funcionarios.

Por lo tanto el INCIVA, en asesoría de la oficina de informática, implementara, socializara y actualizara el plan estratégico de seguridad de la información – PESI, teniendo como primera base, la sede central del INCIVA.

Para la realización del documento se tomara en base los lineamientos de seguridad de la información establecidos en la política de gobierno digital del 14 de junio del 2018.

El INCIVA adoptara los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como GTC/ISO 27002:2015, ISO 27005:2009, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas las partes interesadas.

2. OBJETIVO

Establecer un plan estratégico de seguridad para la información para la sede central del INCIVA, en asesoría de la oficina de informática, para la vigencia 2019-2002, tomando en base la norma internacional NTC ISO IEC 27001:2013, la GTC ISO/IEC 27002:2015, la norma técnica colombiana NTC-ISO/IEC 27005 y la guía técnica colombiana GTC-ISO 19011.

2.1. OBJETIVOS ESPECIFICOS

- Implementar y socializar el plan estratégico de seguridad de la información – PESI, para la sede central del INCIVA.
- Aplicar efectivamente la norma internacional NTC ISO IEC 27001:2013 y la GTC ISO/IEC 27002:2015, para determinar el nivel de madurez del INCIVA.

3. ALCANCE

Teniendo en cuenta que el INCIVA cuenta con una sede central y 5 centros operativos, los cuales 4 se encuentran fuera de la ciudad de Cali, el alcance de este plan estratégico de seguridad de la información será para la sede central del INCIVA y el Museo de Ciencias Naturales Federico Carlos Lehmann, ubicado en la Avenida Roosevelt # 24-80 de la ciudad de Cali, Valle del Cauca, aplicando todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, sin excepción alguna.

4. 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.

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).

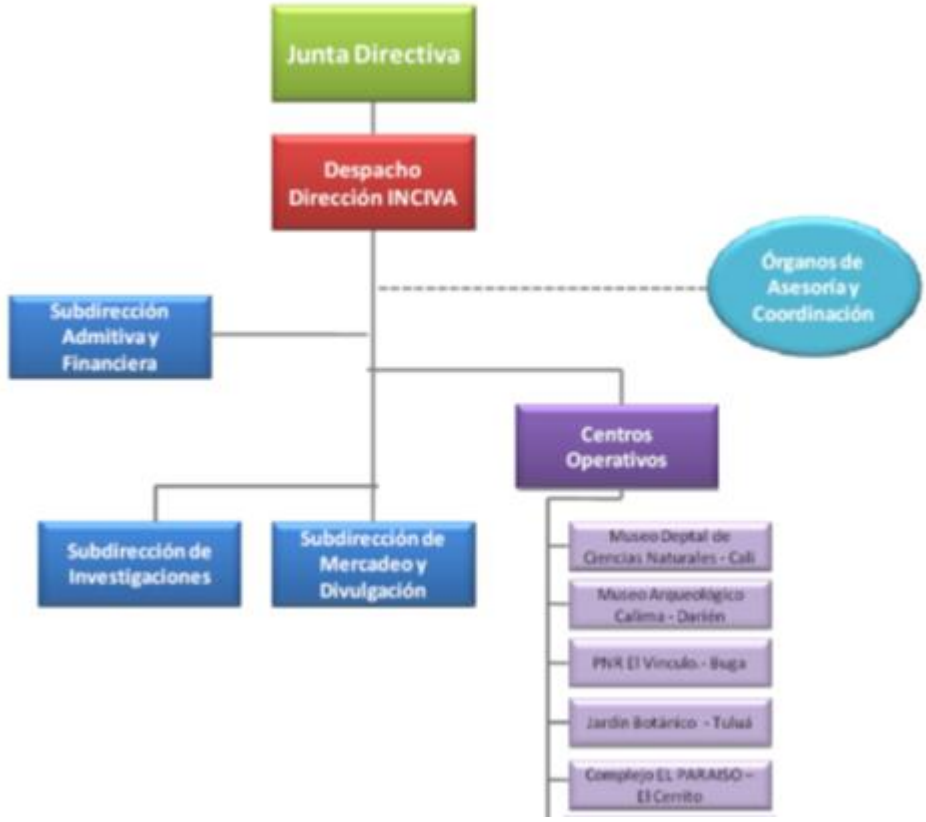
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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).

5. NORMAS APLICABLES

- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27005
- GTC-ISO/IEC 27002:2015
- GTC-ISO 19011

6. ESTRUCTURA ORGANIZACIONAL



7. PLANEACION DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

De acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones y actualizado según el decreto No 1008 del 14 de junio del 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, El INCIVA en asesoría de la oficina de informática, trabajan en la implementación de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

El modelo se va a basar en el ciclo PHVA, el cual recomienda la norma NTC-ISO/IEC 27001:2013 y la GTC-ISO/IEC 27002:2015.

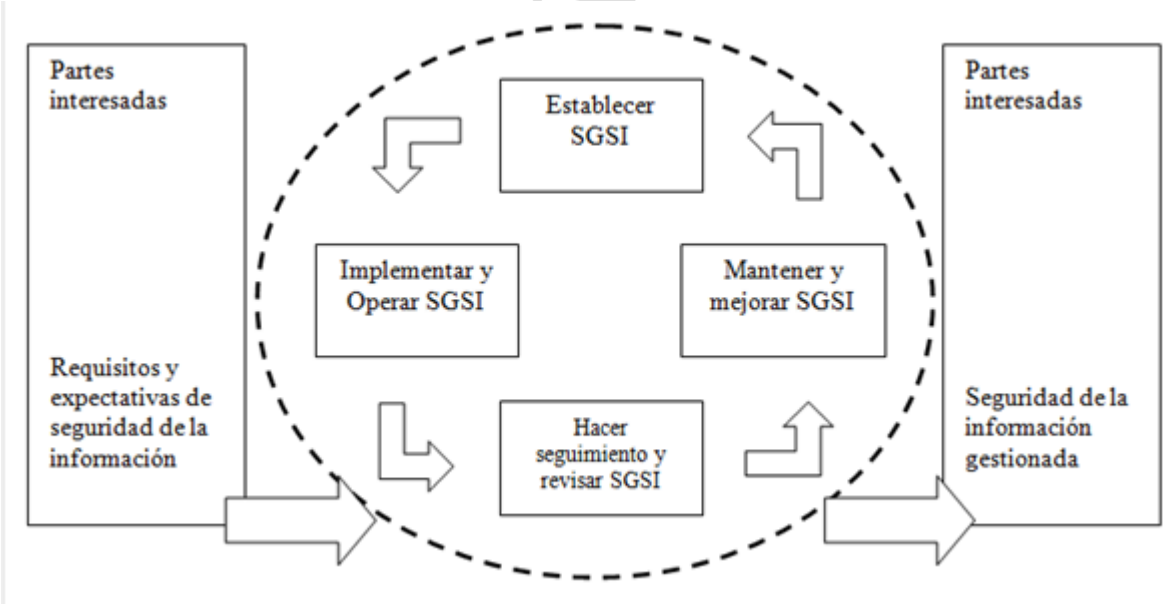


Figura tomada de: http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html

DESCRIPCION DEL MODELO PHVA

PROCESO PHVA	DESCRIPCION
Planificar: Establecer el SGSI	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer: Implementar y operar el SGSI	Implementar y operar la política, los controles, procesos y procedimientos del SGSI
Verificar: Hacer seguimiento y revisar el SGSI	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la dirección para su revisión.
Actuar: Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoria interna del SGSI y la revisión por la dirección para lograr la mejora continua.

Cuadro tomado de: http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html

8. CONTEXTO DE LA ENTIDAD

Somos el Instituto para la Investigación y la Preservación del Patrimonio Cultural y Natural del Valle del Cauca, su sigla INCIVA corresponde a la Institución pública a nivel departamental, cuyos objetivos se centran en las acciones que procuren el desarrollo, estímulo y apoyo de procesos de investigación, aprobación, divulgación y gestión del conocimiento, para la conservación, preservación y uso del patrimonio natural y cultural del Valle del Cauca y la región.

INCIVA es la institución gubernamental del orden departamental creado el 23 de septiembre de 1979. Es una entidad sui generis en el desarrollo de la región, que cuenta con seis centros para la investigación, la divulgación y el turismo y cuenta

También con un centro de análisis de información especializada, puestos al servicio de la comunidad científica y a la ciudadanía en general.

Sus áreas de acción son:

- Conocimiento de la biodiversidad y la arqueología.
- Conservación, preservación y protección del patrimonio natural y cultural.
- Gestión ambiental y cultural.
- Educación y divulgación.
- Turismo sostenible.

9. CLIENTES Y PARTES INTERESADAS

Los clientes y las partes interesadas del INCIVA, están definidas en el manual de la calidad de la institución, en su versión 01 del 28 de noviembre de 2016 y puede ser consulta en la carpeta publica de la entidad.

CLIENTE		
DESCRIPCION	**PRECESO RESPONSABLE**	**DOCUMENTO – REGISTRO SOPORTE**
COMUNIDAD	P1 – Direccionamiento estratégico	Rendición publica de cuentas
		Elaboración plan anticorrupción y de atención ciudadana
	P2 – Investigaciones	Convenios
		Registro de ingreso de colecciones
		Estudios de arqueología
		Proyectos de inversión
	P3 – Mercadeo y Divulgación	Informes PQRS
		Informes encuestas de satisfacción
		Buzón de sugerencias
		Registro de visitas
	P4 - Jurídica	Direccionamiento de derechos de petición
	P6 – Administración de recursos	Asignación y ejecución de recursos para funcionamiento y

COMUNIDAD			mantenimiento de los Centros
	P9 – Evaluación y Mejora		Informe pormenorizado del estado de Control Interno (WEB institucional)
			Informe sobre las solicitudes, peticiones, quejas y reclamos (Art 76 de la ley 1474 de 2011) se publica en la WEB institucional
			Seguimiento al Plan Anticorrupción y de Atención Ciudadana
PARTES INTERESADAS			
DESCRIPCION	**PRECESO RESPONSABLE**		**DOCUMENTO – REGISTRO SOPORTE**
ASAMBLEA	P1- Direccionamiento Estratégico		Informe Financiero Presupuestal
			Informe de Gestión
			Aprobación Plan Estratégico
JUNTA DIRECTIVA	P6- Recursos Administrativos		Presupuesto Anual
			Los demás que corresponda por estatutos y otros
			Ejecución presupuestal
ORGANOS DE CONTROL	Contraloría Departamental del Valle del Cauca	P8- Evaluación y mejora	Informes de Auditoría regular o especial. Planes de mejoramiento
	Control Interno	P8- Evaluación y mejora	Informes de Auditoría Interna
	Contaduría General de la Nación	P6- Recursos Administrativos	Informe CHIP
	Contraloría General de la República	P8- Evaluación y mejora	Informes Auditoría al Sistema General de Regalías
	DNP (Departamento	P1 y P6- Direccionamiento	Rendición ejecución proyectos con fondos

	Nacional de Planeación)	Estratégico y Administración de Recursos	del Sistema General de Regalías
ICAHN	P2- Investigaciones		Permisos para excavaciones
UNIVERSIDADES	Procesos Misionales, (P2 y P3)		Certificación de tesistas, pasantes

10. CONTEXTO INTERNO

- **Factor humano:** Las personas son parte de los activos de información del INCIVA, y se encuentran discriminadas en funcionarios públicos, contratistas, proveedores, clientes y ciudadanos, que continuamente hacen interacción con la entidad, y, por ende, gestionan, procesan, almacenan, distribuyen, intercambian y/o consultan información que puede ser reservada, sensible o interna.

- **Infraestructura física:** La sede del INCIVA se encuentra ubicada en la Avenida Roosevelt No 24-80 de la ciudad de Cali, Valle del Cauca, Colombia. Cuenta con una edificación de 4 pisos más el sótano para parqueadero, se cuenta con un ascensor, una entrada principal por la avenida Roosevelt y una salida de emergencia por la misma avenida, para acceder a las oficinas del INCVA, se deben cumplir unos controles como la exigencia del porte del carnet por parte de los funcionarios y contratistas, y un registro para visitantes y elementos tecnológicos. En cada uno de los pisos se cuenta con:

  ✓Áreas de evacuación.

  ✓Áreas seguras.

  ✓Señalización de áreas.

  ✓Un ascensor

- **Infraestructura tecnológica:** En la sede central del INCIVA, se cuenta con una oficina de informática donde reposa los servidores principales de la institución, además del punto de distribución de la fibra óptica de internet entregada por la E.R.T., un router en el cual se coordina las direcciones IP a entregar a cada estación de trabajo.

11. SITUACION ACTUAL

Para describir la situación actual y el nivel de madurez de la sede central del INCIVA en el sistema de seguridad de la información, se necesita saber los niveles de madurez alcanzados por cada uno de los dominios y sus objetivos de control de la ISO 27001:2013, en la siguiente imagen se ilustra los dominios y los objetivos de control con los cuales se determinará el nivel de madurez.

Dominio ISO 27001	Objetivo de control
Política de seguridad de la información.	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 del entorno	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 de la información	Objetivo de control A.16
Aspectos de seguridad de la información en la Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Imagen: dominio ISO 27001. Imagen tomada del plan estratégico de la seguridad de la información ICA

12. INFORME DE AUDITORIA DE LA NTC ISO 27001:2013 EN LA SEDE CENTRAL DEL INCIVA.

12.1. ASPECTOS GENERALES

12.2. Términos del informe

Se utilizo para el informe los términos y definiciones establecidos en la GTC-ISO 19011 – Directrices para la auditoria de los sistemas de gestión, en el punto 3.10. Hallazgos de la auditoria en su nota 3: En

inglés, sí los criterios de auditoria se seleccionan de entre los requisitos legales o los reglamentarios, el hallazgo de la auditoria se denomina cumplimiento o no cumplimiento.

12.3. Metodología de la auditoria

La auditoría se ejecutó de acuerdo con el procedimiento PEM1 – Auditorías internas, publicado en la intranet de la institución. La auditoría se hizo de manera presencial en la sede central del INCIVA, utilizando técnicas como entrevistas con funcionarios, intranet, revisión de información, revisión documental, cruce de información, entre otras, durante la ejecución de la misma, tomando selectivo (muestreo no estadísticas) para verificación de controles, en puestos de trabajo del personal de las siguientes dependencias: Oficina de informática, Almacén, Gestión Humana, Gestión documental o Archivo, Jurídica.

12.4. Herramientas de diagnostico

Se utilizaron dos herramientas de diagnóstico, la primera es la recomendada por el MINTIC, la cual se puede descargar del siguiente enlace: https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx y la segunda herramienta para la evaluación de los controles de la ISO 27001:2013 se encuentra en el siguiente en link de fuente de la Universidad Cooperativa de Colombia http://repository.ucc.edu.co/bitstream/ucc/304/4/EVALUACION%20DE%20CONTROLES%20ISO%2027002-2013.xlsx

Para diagnosticar el estado del modelo de seguridad y privacidad de la información con los controles de la ISO 27001:2013 se utilizaron los siguientes criterios de evaluación:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A (MINTIC)		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Porcentaje	Criterio	Descripción
0%	No realizado	No hay controles de seguridad de la información establecidos.
20%	Realizado informalmente	Existen procedimientos para llevar a cabo ciertas acciones en determinado momento. Estas prácticas no se adoptaron formalmente y/o no se les hizo seguimiento y/o no se informaron adecuadamente.
40%	Planificado	Los controles de seguridad de la información establecidos son planificados, implementados y repetibles.
60%	Bien definido	Los controles de seguridad de la información además de planificados son documentados, aprobados e implementados en toda la organización.
80%	Cuantitativamente controlado	Los controles de seguridad de la información están sujetos a verificación para establecer su nivel de efectividad.
100%	Mejora continua	Los controles de seguridad de la información definidos son periódicamente revisados y actualizados. Estos reflejan una mejora al momento de evaluar el impacto.

Las dos herramientas de diagnóstico utilizan una escala de porcentaje de cumplimiento:

Porcentaje	Criterio MINTIC	Criterio U.C.C
0%	Inexistente	No realizado
20%	Inicial	Realizado informalmente
40%	Repetible	Planificado
60%	Efectivo	Bien definido
80%	Gestionado	Cuantitativamente controlado
100%	Optimizado	Mejora continua

La ponderación de cumplimiento de los requisitos legales de la norma ISO 27001:2013 se determinó de la siguiente manera:

Porcentaje	Criterio MINTIC	Criterio U.C.C	Ponderación
0%	Inexistente	No realizado	No cumple
20%	Inicial	Realizado informalmente	No cumple
40%	Repetible	Planificado	No cumple
60%	Efectivo	Bien definido	No cumple
80%	Gestionado	Cuantitativamente controlado	cumple
100%	Optimizado	Mejora continua	cumple

13. RESULTADOS DE LA AUDITORIA

13.1. No cumplimiento de requisitos legales o reglamentarios

NORMA	SECCION	CUMPLIMIENTO LEGAL (SI O NO)
6	ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN	
6,1	Organización interna	
6.1.3	Contacto con las autoridades	NO
6,2	Dispositivos móviles y teletrabajo	
6.2.1	Política para dispositivos móviles	NO
6.2.2	Teletrabajo	NO
7	SEGURIDAD DEL RECURSO HUMANO	
7,2	Durante la ejecución del empleo	
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	NO
7.2.3	Proceso disciplinario	NO
8	GESTION DE ACTIVOS	
8,1	Responsabilidad sobre los Activos	
8.1.1	Inventario de activos.	NO
8.1.2	Propiedad de los activos.	NO
8.1.3	Uso aceptable de los activos.	NO
8,2	Clasificación de la Información	
8.2.1	Directrices de clasificación.	NO
8.2.2	Etiquetado y manipulado de la información.	NO
8,3	Manejo de los soportes de almacenamiento	
8.3.2	Eliminación de soportes.	NO

8.3.3	Soportes físicos en tránsito	**NO**
9	**CONTROL DE ACCESO**	
9,1	**Requisitos de negocio para el control de accesos**	
9.1.1	Política de control de accesos.	**NO**
11	**SEGURIDAD FISICA Y AMBIENTAL**	
11,1	**Áreas Seguras**	
11.1.1	Perímetro de seguridad física.	**NO**
11.1.2	Controles físicos de entrada.	**NO**
11.1.4	Protección contra las amenazas externas y ambientales.	**NO**
11.1.6	Áreas de acceso público, carga y descarga	**NO**
11,2	**Seguridad de los Equipos**	
11.2.1	Emplazamiento y protección de equipos.	**NO**
11.2.2	Instalaciones de suministro.	**NO**
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	**NO**
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	
13,2	**Intercambio de información con partes externas.**	
13.2.1	Políticas y procedimientos de intercambio de información.	**NO**
13.2.2	Acuerdos de intercambio	**NO**
13.2.4	Acuerdos de confidencialidad y secreto	**NO**
16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**	
16,1	**Seguridad de la información en las relaciones con los proveedores**	
16.1.3	Reporte de debilidades de seguridad de la información	**NO**

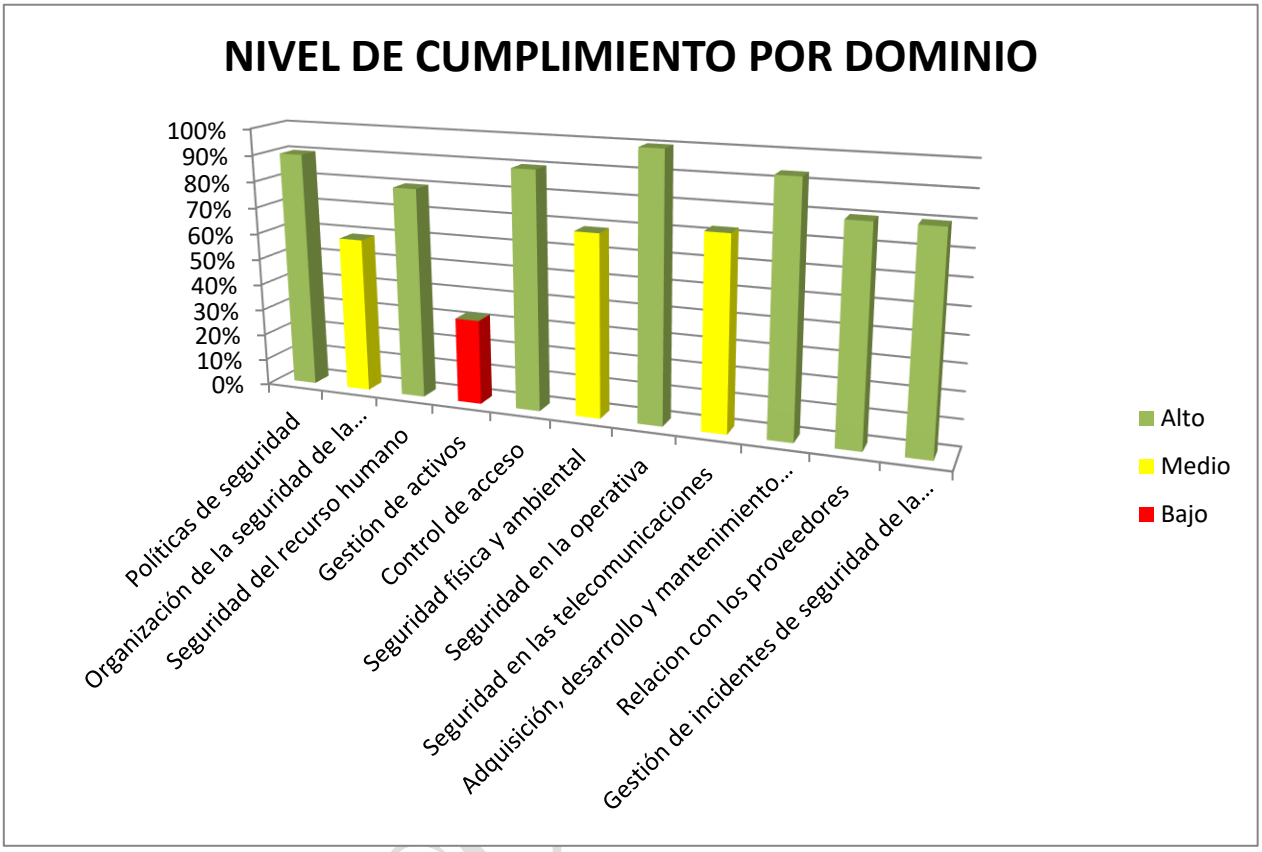
En total fueron 24 ítems de incumpliendo de requisitos legales.

13.2. Cumplimiento de dominios

Norma	Dominios	Estado
5	Políticas de seguridad	90%
6	Organización de la seguridad de la información	59%
7	Seguridad del recurso humano	80%
8	Gestión de activos	32%
9	Control de acceso	90%
11	Seguridad física y ambiental	69%
12	Seguridad en la operativa	100%
13	Seguridad en las telecomunicaciones	73%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	93%
15	Relación con los proveedores	80%
16	Gestión de incidentes de seguridad de la información	80%

Cumplimiento General	77%

Dominios	Bajo	Medio	Alto
Políticas de seguridad	0%	0%	90%
Organización de la seguridad de la información	0%	59%	0%
Seguridad del recurso humano	0%	0%	80%
Gestión de activos	32%	0%	0%
Control de acceso	0%	0%	90%
Seguridad física y ambiental	0%	69%	0%
Seguridad en la operativa	0%	0%	100%
Seguridad en las telecomunicaciones	0%	73%	0%
Adquisición, desarrollo y mantenimiento de los sistemas de información	0%	0%	93%
Relación con los proveedores	0%	0%	80%
Gestión de incidentes de seguridad de la información	0%	0%	80%

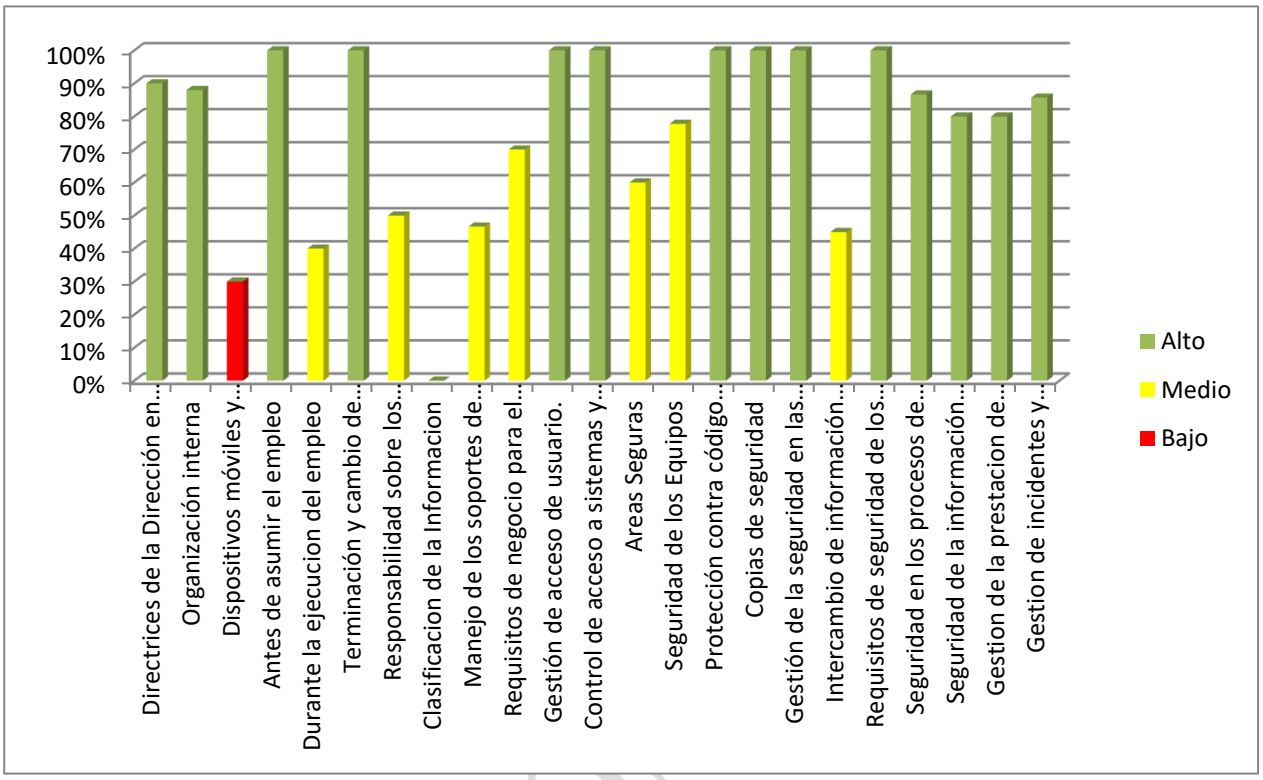


13.3. Cumplimiento de objetivos de control

Norma	Objetivos de Control	Estado
5,1	Directrices de la Dirección en seguridad de la información	90%
6,1	Organización interna	88%
6,2	Dispositivos móviles y teletrabajo	30%
7,1	Antes de asumir el empleo	100%
7,2	Durante la ejecución del empleo	40%
7,3	Terminación y cambio de empleo	100%
8,1	Responsabilidad sobre los Activos	50%
8,2	Clasificación de la Información	0%
8,3	Manejo de los soportes de almacenamiento	47%
9,1	Requisitos de negocio para el control de accesos	70%
9,2	Gestión de acceso de usuario.	100%

9,4	Control de acceso a sistemas y aplicaciones	100%
11,1	Áreas Seguras	60%
11,2	Seguridad de los Equipos	78%
12,2	Protección contra código malicioso	100%
12,3	Copias de seguridad	100%
13,1	Gestión de la seguridad en las redes.	100%
13,2	Intercambio de información con partes externas.	45%
14,1	Requisitos de seguridad de los sistemas de información	100%
14,2	Seguridad en los procesos de desarrollo y soporte	87%
15,1	Seguridad de la información en las relaciones con los proveedores	80%
15,2	Gestión de la prestación de servicios de proveedores	80%
16,1	Gestión de incidentes y mejoras en la seguridad de la información	86%

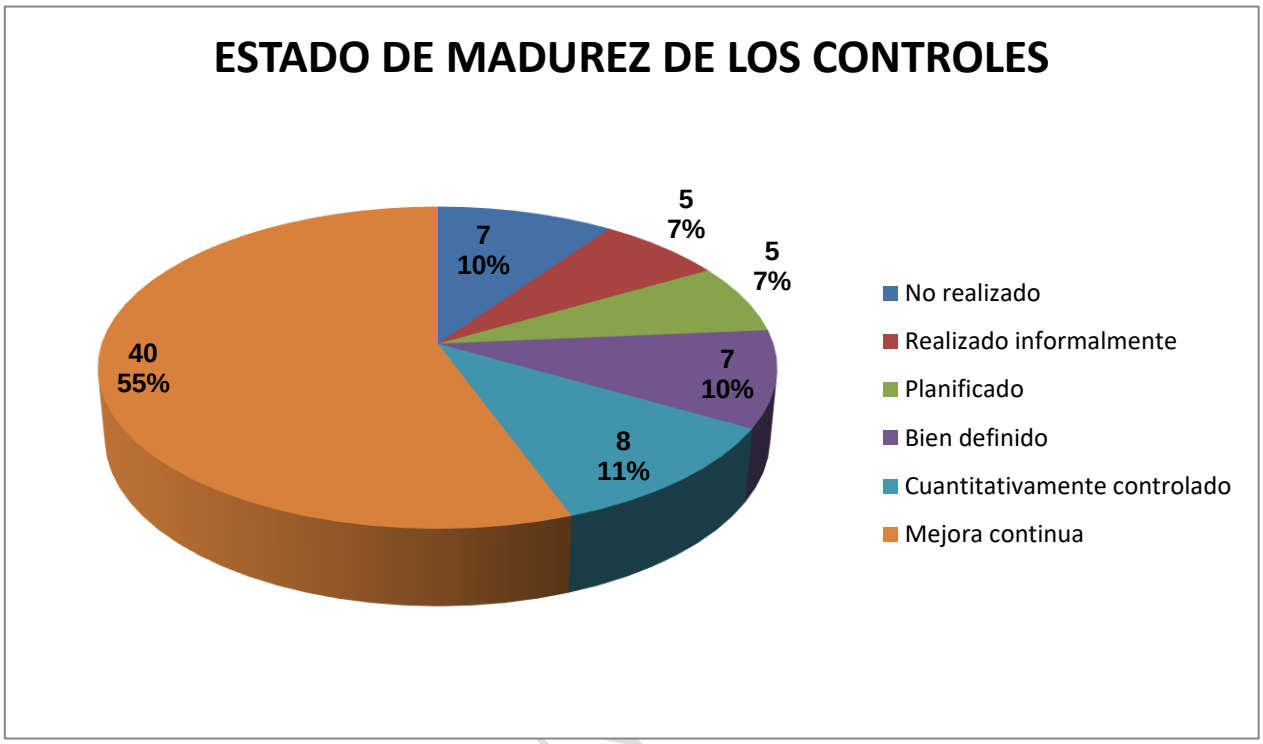
Objetivos de Control	Bajo	Medio	Alto
Directrices de la Dirección en seguridad de la información	0%	0%	**90%**
Organización interna	0%	0%	**88%**
Dispositivos móviles y teletrabajo	**30%**	0%	0%
Antes de asumir el empleo	0%	0%	**100%**
Durante la ejecución del empleo	0%	**40%**	**0%**
Terminación y cambio de empleo	0%	0%	**100%**
Responsabilidad sobre los Activos	0%	**50%**	0%
Clasificación de la Información	**0%**	0%	0%
Manejo de los soportes de almacenamiento	0%	**47%**	0%
Requisitos de negocio para el control de accesos	0%	**70%**	0%
Gestión de acceso de usuario.	0%	0%	**100%**
Control de acceso a sistemas y aplicaciones	0%	0%	**100%**
Áreas Seguras	0%	**60%**	0%
Seguridad de los Equipos	0%	**78%**	0%
Protección contra código malicioso	0%	0%	**100%**
Copias de seguridad	0%	0%	**100%**
Gestión de la seguridad en las redes.	0%	0%	**100%**
Intercambio de información con partes externas.	0%	**45%**	0%
Requisitos de seguridad de los sistemas de información	0%	0%	**100%**
Seguridad en los procesos de desarrollo y soporte	0%	0%	**87%**
Seguridad de la información en las relaciones con los proveedores	0%	0%	**80%**
Gestión de la prestación de servicios de proveedores	0%	0%	**80%**
Gestión de incidentes y mejoras en la seguridad de la información	0%	0%	**86%**



13.4. Madurez de los controles

Nivel	N° controles
No realizado	7
Realizado informalmente	5
Planificado	5
Bien definido	7
Cuantitativamente controlado	8
Mejora continua	40

Total de Controles	**72**


ESTADO DE MADUREZ DE LOS CONTROLES
7
10%
5
7%
5
7%
7
10%
8
11%
40
55%
No realizado
Realizado informalmente
Planificado
Bien definido
Cuantitativamente controlado
Mejora continua