PLAN ESTRATEGICO Y PRIVACIDAD DE LA INFORMACION - PESI

2019-2022

FASE I (INICIO-CONTEXTO-SITUACION ACTUAL- METODOLOGIA)

ELABORADO POR: Julián Adolfo Vásquez Ospina –Asesor de Informática-

REVISADO POR : Comité de Gobierno Digital -INCIVA-

APROBADO POR : Álvaro Rodríguez Morante –Director INCIVA-

Enero 22 de 2019

TABLA DE CONTENIDO

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 se guiará bajo 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 de la información para la sede central del INCIVA, en asesoría de la oficina de informática, para la vigencia 2019-2022, tomando como referencia ~~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 los lineamientos de 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, de los cuales 4 se encuentran fuera de la ciudad de Cali, el alcance inicial 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).

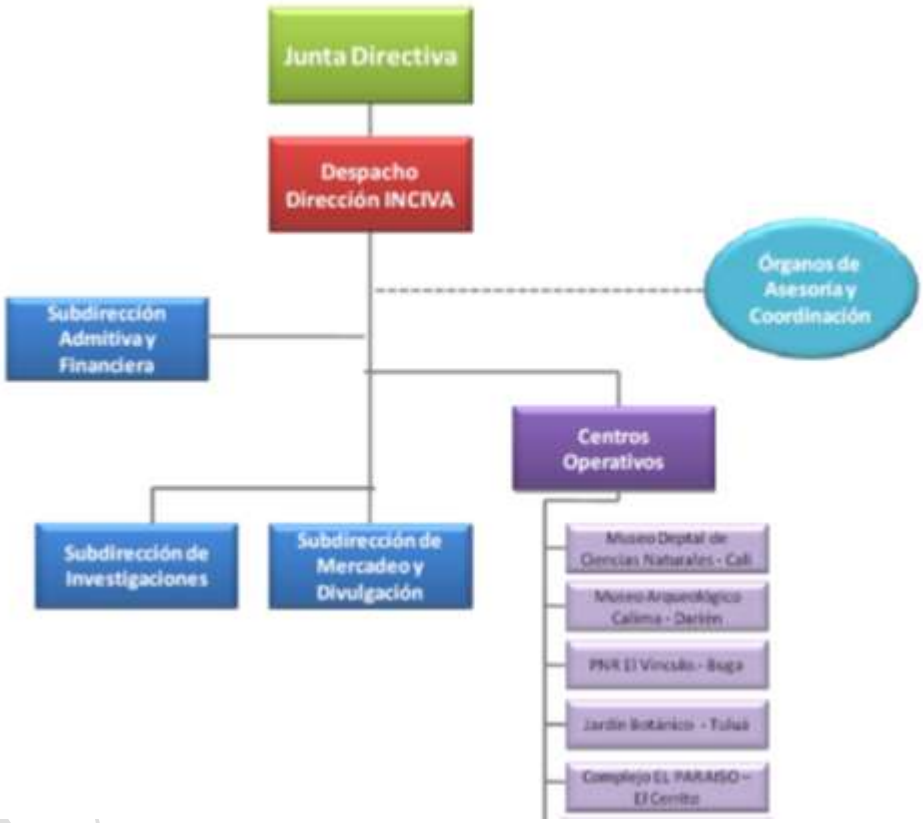
Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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.

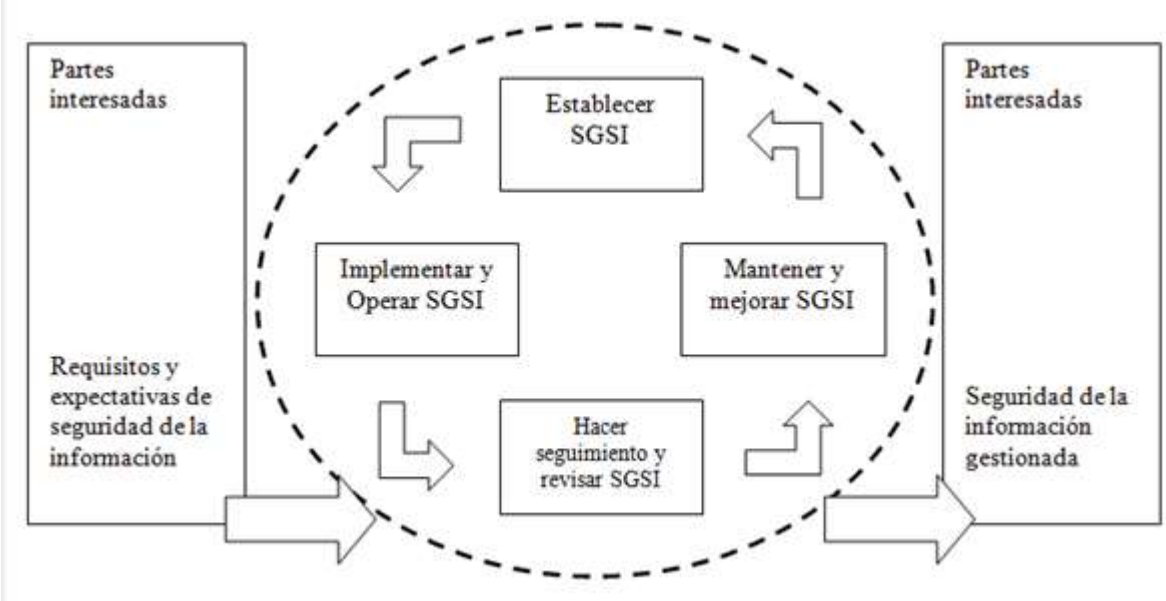


Figura tomada de: http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html

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 mantenimiento de los Centros

COMUNIDAD			
	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 Nacional de Planeación)	P1 y P6- Direccionamiento Estratégico y Administración de Recursos	Rendición ejecución proyectos con fondos 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 27001:2005, en la siguiente imagen se ilustra los dominios y los objetivos de control con los cuales se determinara 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

(ORIGINAL FIRMADO)

_____

ALVARO RODRIGUEZ MORANTE

DIRECTOR