

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

**Bogotá, D.C.,**

**(FEBRERO DE 2019)**

CONTENIDO

[1. INTRODUCCIÓN 3](#_Toc979369)

[3. OBJETIVO GENERAL 3](#_Toc979370)

[4. OBJETIVOS ESPECIFICOS. 3](#_Toc979371)

[5. ALCANCE 4](#_Toc979372)

[6. METODOLOGÍA 5](#_Toc979373)

[7. PLAN PARA LA IMPLEMENTACION DEL SGSI EN LA ENTIDAD. 5](#_Toc979374)

[8. DOMINIOS DE CONTROL 7](#_Toc979375)

[9. DESARROLLO DE LAS POLITICAS 8](#_Toc979376)

[10. REFERENCIA NORMATIVA 8](#_Toc979377)

[11. IMPORTANCIA DE SU APLICACIÓN: 9](#_Toc979378)

# INTRODUCCIÓN

El presente documento corresponde al diagnóstico del estado actual de la seguridad de la información en la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACION Y MANTENIMIENTO VIAL (UAERMV). Para la evaluación se tiene como referencia las normas ISO 27001:2013, 27002, los lineamientos dados por MINTIC.

1. **GLOSARIO DE TERMINOS**

* **Análisis de brecha (GAP):** El GAP Análisis es un estudio preliminar que permite conocer la manera en la que se desempeña una empresa en **materia de seguridad de la información**, con relación a las mejores prácticas reconocidas en la industria, para esto se utilizan criterios establecidos en normas o estándares. El análisis establece las **diferencias entre el desempeño actual y el deseado**. Este análisis se puede aplicar a cualquier estándar certificable, lo normal es que se lleve a cabo para nuevos esquemas de certificación.
* **ISO 27001: ISO 27001** es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
* **GAP:** Análisis de deficiencias, es un análisis que mide cómo una organización está llevando a cabo su desempeño con respecto a una serie de criterios establecidos en base a normas o procedimientos internos, controles seleccionados, las mejores prácticas de competencia, etc. El resultado de este análisis establece la diferencia entre el desempeño actual y el esperado, con un informe presentado con indicaciones sobre dónde están las deficiencias y “qué” falta para cumplir con cada requisito de la norma.
* **SOA:** Statement Of Applicability, en español DDA, documento de aplicabilidad.

# OBJETIVO GENERAL

Verificar los alcances establecidos en el Modelo de Privacidad y Seguridad de la Información (MPSI) y la documentación base con la que cuenta la entidad para la implentacion de sun SGSI.

# OBJETIVOS ESPECIFICOS.

* Identificar las orientaciones, directrices e instrumentos que le permiten a la UMV gestionar la seguridad de la información.
* Identificar los controles de seguridad de la información definidos en el anexo A de la norma ISO 27001:2013 que se aplican actualmente a la UMV.
* Identificar los controles y mecanismos de seguridad que utilizan actualmente los sistemas de información de la UMV.
* Identificar riesgos de seguridad asociados a los recursos tecnológicos a los que está expuesta la UMV.
* Describir los principales problemas de seguridad que presenta la entidad.
* Definir las medidas de seguridad más apropiadas a aplicarse.
* Definir políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.
* Plantear un SGSI para la UMV bajo la norma ISO/IEC 27001 con el fin de garantizar confidencialidad, integridad y disponibilidad de la información.
* Implementar un SGSI para la UMV que permita proteger los activos de la entidad.
* Ser la guía que deben aplicar los usuarios para mantener un correcto uso de los recursos tecnológicos.
* Definir los lineamientos para ayudar a garantizar la seguridad de la información en la UAERMV.
* Lograr un adecuado nivel de confidencialidad, integridad, disponibilidad de la información que se produce o recibe en la entidad.
* Cumplir con los principios de seguridad de la información.
* Apoyar la innovación tecnológica.
* Proteger los activos de información, tecnológicos y de seguridad digital.
* Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
* Fortalecer la cultura de seguridad de la información en los servidores públicos, terceros, y demás usuarios externos de la UAERMV.
* Garantizar la continuidad del negocio frente a incidentes de seguridad.

# ALCANCE

El presente documento describe el Plan de Seguridad y Privacidad de la entidad, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Se definen políticas y lineamientos con el propósito de cumplir con los objetivos de la institución en seguridad de la informacon y seguridad informática; y para ello se establecen:

* Políticas de seguridad: Para definir controles que proporcionan directivas y consejos de gestión para mejorar la seguridad de los activos de información.
* Políticas de navegación en internet: Establece la configuración de perfiles de navegación para optimizar el uso del canal de internet y reducir el riesgo de descarga de software nocivo.
* Políticas de tratamiento y manejo de datos personales: Establece los lineamientos para el manejo y tratamiento de los datos personales de acuerdo con la ley 1581 de 2012 de la SIC (Súper intendencia de industria y comercio).
* Políticas de seguridad de activos de información: establece controles para catalogar los activos y protegerlos eficazmente.
* Política de protección y respaldo de la información: Establece los lineamientos para garantizar las copias o respaldos de la información.
* Política del escritorio limpio y bloqueo de pantalla.: Establece los lineamientos para proteger los documentos ubicados en los escritorios y el bloqueo de los equipos de computo cuando el usuario no se encuentre en su puesto de trabajo.
* Política de seguridad para gestión de contraseñas: Establece los lineamientos para la gestión segura de las credenciales (usuario y contraseña) de los aplicativos y equipos de computo.
* Política de responsabilidades operacionales y control de cambios: Establece los lineamientos para cuando se requieren hacer cambios importantes en la infraestructura tecnológica o sistemas de información que pueden afectar la continuidad de la operación.
* Política de protección contra software nocivo: Establece los lineamientos para evitar la descarga, instalación y propagación de software nocivo (virus y sus variantes)
* Política de gestión de riesgos: Establece los lineamientos para la identificación y mitigación de los riesgos asociados a los activos de la entidad.
* Política para el buen uso del correo electrónico institucional: Establece los lineamientos para el uso eficiente y seguro del correo electrónico de la entidad.
* Política de registro histórico de actividades (log): Establece los lineamientos para almacenar los logs de los aplicativos críticos de la entidad, para en caso de presentarse un incidente de seguridad poder realizar un análisis forense.
* Política sobre el uso de equipos de computo y el acceso a la red: Establece los lineamientos para el buen uso de los equipos de computo de la entidad y la protección del acceso a la red lan o wifi de la entidad

# METODOLOGÍA

Tomando como referencia la norma internacional ISO 27001:2013, 27002, los lineamientos del Ministerio de Tecnologías de Información y Comunicación (MINTIC), y la Alta Consejería, la unidad cuenta con el material suficiente para dar inicio a la implementación del SGSI.

# PLAN PARA LA IMPLEMENTACION DEL SGSI EN LA ENTIDAD.

A continuación, se listan los HITOS definidos para la implementación del SGSI.

*Tabla 1. Hitos implementación SGSI*

|  |  |  |
| --- | --- | --- |
| Descripción | Actividad | Entregables |
| Hito Nº 1 | Diagnóstico | * Diagnóstico de Seguridad de la Información. * Propuesta del Alcance del SGSI |
| Hito No 2 | Establecimiento y Estructura del SGSI, Definición del Alcance | * Generación parcial de Políticas del SGSI. * Generación de formatos aplicables. * Inventario de activos. * Generación de SoA (documento de aplicabilidad) * Documentación básica inicial del SGSI. * Comunicación y socialización a los usuarios de la entidad. |
| Hito No 3 | Gestión de Riesgos | * Matriz de Gestión de Riesgos. * Metodología de Gestión de Riesgos * Definición del Plan de Tratamiento de Riesgos. * Informe de Gestión de Riesgos. * Comunicación y socialización a los usuarios de la entidad. |
| Hito Nº 4 | Implementación y Operación del SGSI | * Actualización de documentación vigente. * Informe de * Medición del SGSI. * Seguimiento del SGSI. * Políticas específicas del SGSI. * Seguimiento de los controles de seguridad de la información. * Manual del SGSI. * Medición, Métricas de procedimientos de seguridad. * Comunicación y socialización a los usuarios de la entidad. |
| Hito Nº 5 | Monitorear y Revisar | * Informe de auditoría interna. * Planes de acción de auditoria del SGSI. * Mejora continua. * Acciones Correctivas, y de mejora. |
| Hito Nº 6 | Mantener y Mejorar | * Implementar Mejoras. * Generar acciones correctivas. * Comunicación y socialización a los usuarios de la entidad. |
| Hito Nº 7 | Acompañamiento en la Auditoria Externa (\*) | * Preauditoria. * Cierre de hallazgos * Revisión, planes de acción, análisis y seguimiento a los hallazgos del Ente Certificador |

Fuente: Proceso EGTI

# DOMINIOS DE CONTROL

La norma ISO 27001:2013 en su anexo A tomado de la norma ISO 27002 nos habla de una serie:

* 14 dominios.
* 10 clausulas o capítulos.
* 114 controles.
* 35 objetivos de control.

Los lineamientos y buenas practicas para la implementación de los controles que apliquen a la entidad de acuerdo con los procesos y procedimientos establecidos para cada (proceso o dependencia de ésta), según MINTIC, la UMV para finales del año 2017 debe tener una calificación del 60% sobre 100% de acuerdo con los 14 dominios que menciona la norma.

Revisando los controles de seguridad que aplican a la entidad, ver tabla 4 (Dominios de control), la entidad obtuvo como calificación 6,57% del 60% que debería tener implementado de acuerdo a MINTIC para finales del año 2017, esto evidencia la brecha ente lo que se tiene y lo requerido, sin embargo la meta es cumplir el 100% de los controles de seguridad, alineados a la implementación del SGSI

*Tabla 2. Dominios de control de la ISO 27001:2013*

|  |  |  |
| --- | --- | --- |
| NOMBRE DOMINIOS DE CONTROL | RESULTADO | CALIFICACIÓN OBJETIVO |
| Políticas de seguridad de la información | 10 | 60 |
| Organización de la seguridad de la información | 3 | 60 |
| Seguridad de los recursos humanos | 7 | 60 |
| Gestión de activos | 6 | 60 |
| Control de acceso | 14 | 60 |
| Criptografía | 0 | 60 |
| Seguridad física y del entorno | 23 | 60 |
| Seguridad de las operaciones | 9 | 60 |
| Seguridad de las comunicaciones | 9 | 60 |
| Adquisición, desarrollo y mantenimiento de sistemas | 0 | 60 |
| Relación con los proveedores | 0 | 60 |
| Gestión de incidentes de seguridad de la información | 0 | 60 |
| Aspectos de la seguridad de la información de la gestión de la continuidad del negocio | 0 | 60 |
| Cumplimiento | 9 | 60 |

Fuente: Proceso EGTI

## DESARROLLO DE LAS POLITICAS

* Las estrategias en cuanto a seguridad de información de la UAEMRV son directrices de largo plazo, que sirven como base para la planeación adecuada y la definición de soluciones de seguridad para ajustarse a las necesidades de la entidad, tanto actuales como futuras.
* Las decisiones y disposiciones de seguridad de información estarán basadas en análisis de riesgos y métodos de evaluación.
* La seguridad de información considera revisiones continuas del valor para la institución de las medidas de seguridad en uso.
* La administración de la seguridad de información se desarrollará sobre lineamientos y guías dadas por las entidades del distrito como lo son el MINTIC, Alta Consejería, y otros.
* Las políticas de Seguridad deberán ser revisadas cada vez que se cumpla un ciclo de gestión de seguridad de la información.
* Las políticas de Seguridad deberán ser aprobadas por el(la) secretario(a) General de la entidad.

## REFERENCIA NORMATIVA

* **Norma Técnica Colombiana NTC-ISO-IEC 27002:2015:** Norma técnica de seguridad. Código de practica para controles de seguridad de la información.
* **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
* **Decreto No. 2573 de 2014:** establece como lineamiento la Seguridad y privacidad de la Información y comprende acciones transversales además de componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.
* **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:** Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
* **Decreto 1377 De 2013:** Protección de Datos, decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano.

1. **Capitulo Primero:** De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos;
2. **Capitulo Segundo:** De los atentados informáticos y otras infracciones. Como se puede ver en el primer capitulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así́ la posibilidad de nuevas entradas con este tema.

* **Articulo 230 de la ley 1450 de 2011:** Estableció́ que todas las Entidades deben adelantar acciones señaladas por el Gobierno Nacional, concernientes a implementar las estrategias de Gobierno en Línea que se definen por el Ministerio de Tecnologías de la Información y las comunicaciones.
* **Norma Técnica Colombiana NTC-ISO-IEC 31000:2018:** Norma técnica de gestión del riesgo. Principios directrices.
* **Ley 1341 del 30 de Julio de 2009:** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
* **Ley 1273 DE 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
* **Ley Estatutaria 1266 del 31 De diciembre de 2008:** Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales.
* **Ley 603 de 2000:** Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales. Ver esta ley.

## IMPORTANCIA DE SU APLICACIÓN:

Este documento interno está orientado a brindar los lineamientos para:

* Proteger la información de la UAERMV ya sea dentro de las instalaciones o por fuera de ella.
* Garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, impresoras, tabletas, celulares de última generación, etc.) y de los servicios tecnológicos como el Internet, Correo Electrónico, pagina Web y demás aplicativos que pone a disposición la entidad para los funcionarios.
* Establecer pautas para la utilización eficiente y racional de los recursos tecnológicos.
* Minimizar los riesgos de que se materialice algún ataque informático o amenaza que pueda comprometer a la entidad en una eventual pérdida de información o indisponibilidad del servicio tecnológico.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por**  **EQUIPO OPERATIVO SIG del Proceso:** | **Validado por**  **RESPONSABLE DIRECTIVO SIG**  **del Proceso:** | **Aprobado por:** |
| **OMAR FERNANDO GARZON /**  **GLORIA MENDEZ**  **Contratista / Proceso EGTI** | Firma: | Firma: |
| **Acompañamiento EQUIPO TÉCNICO SIG:** |
| **ANDREA DEL PILAR ZAMBRANO**  **Contratista/ Proceso DESI** |
| **MARCELA ROCIO MARQUEZ ARENAS**  **(Secretaria General)** | **MARTHA PATRICIA AGUILAR COPETE**  **Representante de la Alta Dirección** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección SIG** |
| 1 | Elaborada por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC. | Febrero 2019 | Jefe Oficina Asesora de Planeación |