ADALID

Security, Legal & Forensic Corporation

MANUAL DEL SUBSISTEMA DE SEGURIDAD DE LA INFORMACIÓN
ÁMBITO 6 – VALORACIÓN DE LA MADUREZ DE SEGURIDAD

Bogotá D.C., septiembre de 2018

Phones: (+571) 7432015 - (+571) 7550414 / **E-mail:** info@adalid.com
Address: Calle 70 A # 11–28 Barrio Quinta Camacho Bogotá D.C. – Colombia / www.adalid.com

INFORMACIÓN DEL DOCUMENTO

Título	Documento Manual del subsistema de seguridad de la información		
Fecha de elaboración	15 de septiembre de 2018		
Sumario	Por medio del presente se presenta en un diagrama la relación de actores del estado, marco legal y aspectos relacionados con el ciudadano en el marco de la gestión de la seguridad de la información.		
Palabras Claves	Modelo de seguridad y privacidad de la información, MIPG, política de Gobierno Digital.		
Categoría:	Seguridad de la información	**Consecutivo:**	
Autor:	Clara Patricia MUÑOZ JIMÉNEZ (Gerente de Proyecto) Giovanni Esteban MARTÍNEZ BUENO (Profesional Senior) Oscar Eduardo MONDRAGÓN MACA (Profesional Junior) Oscar Andrés RIVEROS MOYANO (Analista de seguridad) Elkin Guillermo TORRES GARCÍA (Analista de seguridad)		
Revisó:	Andrés GUZMÁN CABALLERO		

HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción del cambio
15/sept/2018	1.0	Creación del documento

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Los manuales de los sistemas de gestión de seguridad de la información han evolucionado de documentos de textos pesados en cuanto a densidad de contenido y complejidad del área de conocimiento técnica que maneja, a manuales sencillos en donde aspectos como la usabilidad, la disponibilidad y un lenguaje claro.

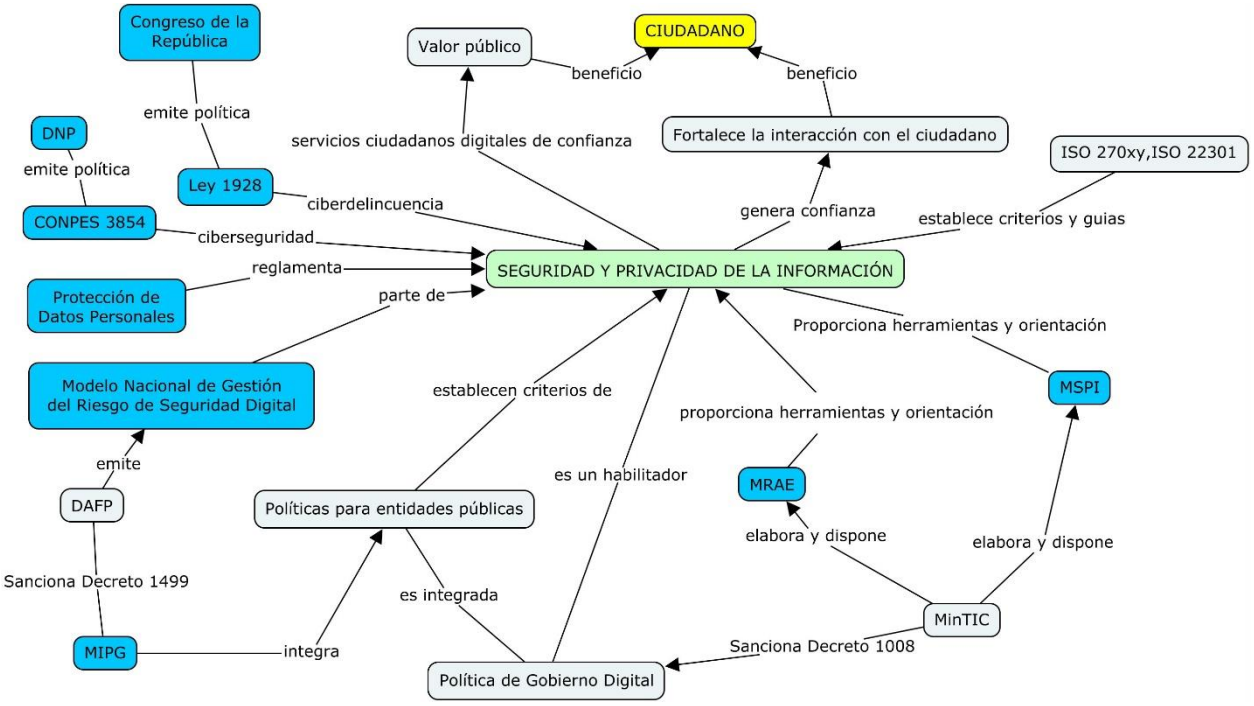
El presente manual busca contextualizar al grupo de talento humano con mayor responsabilidad en la gestión de la seguridad de la información en el entendimiento de la relación entre gestión institucional en materia de seguridad, la administración pública y el ordenamiento jurídico en gestión de las Tecnologías de la Información y las Comunicaciones.

2. MARCO LEGAL

1. Constitución Política de Colombia: **Artículo 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. || **Artículo 20.** Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.
2. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
3. Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
4. Ley 1266 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
5. Decreto 103 de 2015 **"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".**
6. Decreto 1494 de 2015 **"Por el cual se corrigen yerros en la Ley** 1712 **de 2014"**
7. Decreto 1377 de 2013" Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
8. Decreto de 886 del 2014 "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos"
9. Decreto 1081 de 2015 "por el cual se expide el decreto reglamentario único del sector de la Presidencia de la República".
10. Ley 527 de 1999 "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
11. Resolución 3564 de 2015 "Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública"
12. Ley 599 de 2000 "Por la cual se expide el Código Penal."
13. Ley 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones."
14. Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"

3. SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR PÚBLICO

En el diagrama a continuación se presente el mapa conceptual de la articulación del estado en torno a la gestión pública de la seguridad de la información gestionada en las entidades del estado.



Así las cosas, se hace entrega formal del plan de trabajo del proyecto de la consultoría mencionada.

Cordialmente,

Andrés GUZMÁN CABALLERO
C.E.O.
ADALID CORP

Clara Patricia MUÑOZ JIMÉNEZ
Gerente de Proyecto ACDTIC
ADALID CORP

Phones: (+571) 7432015 - (+571) 7550414 / **E-mail:** info@adalid.com
Address: Calle 70 A # 11–28 Barrio Quinta Camacho Bogotá D.C. – Colombia / www.adalid.com

4. GLOSARIO

MSPI
Modelo de Seguridad y Privacidad de la Información. Es el marco de trabajo construido por el MinTIC y puesto a disposición de las entidades del estado para su implementación como mecanismo de fortalecimiento institucional en materia de gestión de información.

Ciberataque
Un ciberataque es cualquier tipo de maniobra ofensiva hecha por individuos u organizaciones que atacan a sistemas de información como lo son infraestructuras, redes computacionales, bases de datos que están albergadas en servidores remotos, por medio de actos maliciosos usualmente originados de fuentes anónimas que también roban, alteran o destruyen un blanco específico mediante hackeo de un sistema vulnerable.

Ciberseguridad
La ciberseguridad o seguridad informática, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta, especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Confidencialidad
Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados. [ISO/IEC 27000:2014]

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.

Disponibilidad
Propiedad de ser accesible y utilizable a demanda por una entidad autorizada. [ISO/IEC 27000:2017]

Framework (Entornos de trabajo)
Es una abstracción en la cual el software que proporciona una funcionalidad genérica, puede ser cambiado selectivamente por un código adicional escrito por el usuario, proporcionando así un software específico para cierta aplicación.

Integridad
Propiedad de exactitud y completitud. [ISO/IEC 27000:2017]

OWASP - Open Web Application Security Project

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

Vulnerabilidad
Debilidad de un activo o de un control que puede ser explotada por una o más amenazas. [ISO/IEC 27000:2017]

5. BIBLIOGRAFÍA

https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

http://www.cursodehackers.com/metasploit.html

Ley 527 de 1999, https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

http://www.lacnic.net/966/1/lacnic/acerca-de-lacnic

http://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

http://www.isecom.org/mirror/OSSTMM.3.pdf

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines