ADALID

Security, Legal & Forensic Corporation

ANEXO TECNICO

BUENAS PRÁCTICAS Y MARCO NORMATIVO DE LA SEGURIDAD DIGITAL

Doctores:
Sergio MARTÍNEZ MEDINA - Alto Consejero Distrital de TIC
María Del Pilar NIÑO CAMPOS - Profesional Especializado en Seguridad de la Información de la Alta Consejería Distrital de TIC

Bogotá D.C., septiembre de 2018

INFORMACIÓN DEL DOCUMENTO

Título	Anexo técnico buenas prácticas y marco normativo de seguridad digital.		
Fecha de elaboración	18 de septiembre de 2018		
Sumario	Por medio del presente se desarrolla el anexo técnico que complementa los documentos metodológicos.		
Palabras Claves	Buenas prácticas, normas, guías, seguridad digital, anexo.		
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
05/Diciembre/2018	1.0	Creación del documento
09/Diciembre/2018	1.1	Actualización del documento

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Junto al marco normativo colombiano de la seguridad digital existe una serie de buenas prácticas o estándares -de facto y de jure[1]-, que deben ser considerados al momento de realizar estudios sobre la misma, como es el caso del fortalecimiento de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI-, establecido por el Ministerio de Tecnologías de la información y Comunicaciones (MinTIC, 2015).

En ese orden de ideas, el presente documento recoge y describe el marco normativo y las buenas prácticas que soporta los documentos de metodología construidos por ADALID CORP. para la Alta Consejería Distrital de las TIC.

2. MARCO NORMATIVO

La tabla 1 recoge los referentes del marco normativo de la seguridad digital en Colombia e incluye un descripción de cada uno. Esto con el propósito de complementar los documentos de metodología construidos por ADALID CORP. para la Alta Consejería Distrital de las TIC y facilitar su entendimiento.

Tabla 1. Referentes normativos

Referente	Descripción
Ley 527 de 1999 (Congreso de la República de Colombia, 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.
Ley 1273 de 2009 (Congreso de la República de Colombia, 2009)	A través de esta Ley se crearon nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

[1] También llamados "de iure".

Referente	Descripción
Ley 1581 de 2012 (Congreso de la Republica, 2012)	Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Ley 1712 de 2014 (Congreso de la República de Colombia, 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. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013)	Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Derogado Parcialmente por el Decreto 1081 de 2015. Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Decreto 103 de 2015 (Presidencia de la República de Colombia, 2015)	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 en lo relativo a la gestión de la información pública y se dictan otras disposiciones.
Decreto 1499 de 2017 (Presidencia de la República de Colombia, 2017)	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
CONPES 3701 (Departamento Nacional de Planeación, 2011)	Lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

Referente	Descripción
CONPES 3854 (Departamento Nacional de Planeación, 2016)	Política Nacional de Seguridad digital. Establece un marco institucional claro en torno a la seguridad digital. Se crean las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital. Fortalecer la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos. Finalmente, generar mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.
Guía 5 de gestión y clasificación de activos de información del MSPI de MinTIC (2015)	Entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del estado, con el fin de determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.
Guía Metodológica de Pruebas de Efectividad – Guía No. 1 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016b)	Tiene como finalidad, indicar los procedimientos de seguridad que pueden generarse durante el proceso de evaluación en los avances en la implementación del modelo de seguridad y privacidad de la información. Se procura que las entidades tengan un enfoque de seguridad en el cual se incluya el desarrollo y mantenimiento de la misma, realizando mejoras en las áreas que se requiera.
Guía No. 7 Gestión de riesgos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016a)	Marco de trabajo para la gestión de riesgos del Modelo de Seguridad y Privacidad de la Información -MSPI- (MinTIC, 2016). A través de ésta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.

Referente	Descripción
Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP, 2018)	Guía que unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos.
Manual de Gobierno digital (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)	Manual que permite la adopción de la política de Gobierno Digital establecida en el Decreto 1008 de 2018, que modifica el Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1. Dicha política forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores.
Modelo de Gestión de Riesgos de Seguridad Digital (MinTIC, 2017)	Elaborado como respuesta a lo definido en la estrategia E.1.2 del documento CONPES 3854 y su plan de acción y seguimiento (PAS).

3. BUENAS PRÁCTICAS

Complementando el marco normativo, en la tabla 2 se recogen las buenas prácticas o estándares de facto y de jure de la seguridad digital, incluyendo una descripción de cada uno de ellos.

Tabla 2. Buenas prácticas/estándares de la seguridad digital

Estándares	Descripción
BICSI 002 (BICSI, 2014)	Mejores prácticas de diseño e implementación de Centros de Cómputo. Considerada la norma base para el diseño de centros de datos alrededor del mundo. ANSI/BICSI 002-2014 continúa su misión de proporcionar requisitos, directrices y mejores prácticas aplicables a cualquier centro de datos.
COBIT (ISACA, 2018)	Objetivos de control para tecnologías de la información y relacionadas. Denominado COBIT por sus siglas en inglés: *Control Objectives for Information and related Technology*.
ISO 21827 (ISO, 2008)	Modelo de Capacidad de Madurez en la seguridad de la información.
ISO/IEC 24764 (2010)	Especifica el cableado genérico que admite una amplia gama de servicios de comunicaciones para su uso dentro de un centro de datos. Cubre el cableado balanceado y el cableado de fibra óptica. Se basa en los requisitos de referencia de ISO / IEC 11801 y contiene requisitos adicionales que son apropiados para los centros de datos en los que la distancia máxima a la que deben distribuirse los servicios de comunicaciones es de 2.000 m.
ISO/IEC 27001:2013 (Icontec, 2013)	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.
ISO-IEC 27002:2013 (Icontec, 2015)	Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

Estándares	Descripción
ISO/IEC 27000:2018 (ISO/IEC, 2018b)	Proporciona una visión general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones.
ISO/IEC 27005:2018 (ISO/IEC, 2018a)	Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información. Proporciona pautas para la gestión de riesgos de seguridad de la información.
ISO 31000:2018 (Icontec, 2018)	Gestión del riesgo. Directrices. Proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto.
ITIL (AXELOS, 2011)	Biblioteca de infraestructura de tecnología de la información, ITIL por sus siglas en inglés: *Information Technology Infrastructure Library*. Es el enfoque más ampliamente aceptado para la gestión de servicios de TI en el mundo.
Magerit versión 3 (Ministerio de Hacienda y Administraciones Públicas de España, 2012)	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.
Marco de trabajo de ciberseguridad de la NIST (National Institute of Standards and Technology, 2014)	Marco voluntario consta de estándares, directrices y mejores prácticas para gestionar el riesgo relacionado con la seguridad cibernética del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio del Gobierno Estadounidense -NIST, por sus siglas en inglés National Institute of Standards and Technology-.
Modelo Abierto de Madurez de la Gestión de la Seguridad de la Información (The open group, 2018a)	Modelo Abierto de Madurez de la Gestión de la Seguridad de la Información del "The Open Group", una comunidad ampliamente reconocida por las buenas prácticas y estándares que han aportado a la industria de las TIC.

Estándares	Descripción
PTES Standard (PTES, 2012)	Estándar de ejecución de pruebas de penetración consta de siete (7) secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, a través de la recopilación de inteligencia y las fases de modelado de amenazas en las que los evaluadores trabajan entre bambalinas para comprender mejor a la organización probada, a través de la investigación de vulnerabilidad.
NIST-800-30 (Stoneburner, Goguen, & Feringa, 2002)	Guía de gestión de riesgos para los sistemas de tecnología de la información. Publicación especial del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio del Gobierno Estadounidense -NIST, por sus siglas en inglés National Institute of Standards and Technology-.
NIST-800-39 (Locke & Gallagher, 2011)	Publicación especial del NIST: Gestión de riesgos de seguridad de la información. Organización, misión y sistema de información.
NIST-800-53r5 (Ross & Rochford, 2017)	Controles de seguridad y privacidad para sistemas de información y organizaciones. Proporciona un catálogo de controles de seguridad y privacidad para sistemas de información y organizaciones para proteger las operaciones y activos de la organización, individuos, otras organizaciones y la nación de un conjunto diverso de amenazas que incluyen ataques hostiles, desastres naturales, fallas estructurales, errores humanos, y riesgos de privacidad.
TOGAF (The open group, 2018b)	Estándar de arquitectura empresarial, TOGAF, por sus siglas en inglés: *The Open Group Architecture Framwork*. Un estándar de The Open Group. Es una metodología y un marco de arquitectura empresarial probados y utilizados por las organizaciones líderes en el mundo para mejorar la eficiencia del negocio.
OSSTMM 3 - The Open Source Security Testing methodology Manual V- 3 (ISECOM, 2010)	Es una metodología para probar la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de comunicación, como las inalámbricas, por cable, analógicas y digitales.

4. BIBLIOGRAFÍA

AXELOS. (2011). ITIL | IT Service Management | ITSM | AXELOS. Recuperado 4 de diciembre de 2018, a partir de https://www.axelos.com/best-practice-solutions/itil

BICSI. (2014). *ANSI/BICSI 002-2014*. Recuperado a partir de https://www.bicsi.org/docs/default-source/publications/bicsi_002_esp_sample.pdf?sfvrsn=f4bce3b9_0

Congreso de la Republica. (2012). Ley estatutaria No. 1581 del 17 de Oct de 2012. *Ministerio de comerico, industria y turismo*. https://doi.org/10.1017/CBO9781107415324.004

Congreso de la República de Colombia. (1999). Ley 527 de 1999. https://doi.org/10.1364/OE.25.030651

Congreso de la República de Colombia. (2009). *Diario Oficial. Ley 1273 de 2009*. *Diario Oficial LEY*. Bogotá D.C. Recuperado a partir de http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Congreso de la República de Colombia. (2014). *Ley 1712 de transparencia y del derecho a la información pública nacional*. *6 De Marzo De 2014*. Recuperado a partir de https://www.alcaldiabogota.gov.co/sisjurMantenimiento/normas/Norma1.jsp?i=60556

DAFP. (2018). *Guía para la Administración de los Riesgos de Gestión , Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas*. Bogotá D.C. Recuperado a partir de http://www.funcionpublica.gov.co/documents/418548/34150781/Guía+para+la+Administración+de+los+Riesgos+de+Gestión%2C+Corrupción+y+Seguridad+Digital+y+el+Diseño+de+Controles+en+Entidades+Públicas+-+Agosto+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?dow

Departamento Nacional de Planeación. (2011). *CONPES 3701 - Lineamientos de política para la ciberseguridad y ciberdefensa*. Bogotá D.C.

Departamento Nacional de Planeación. (2016). *CONPES 3854 - Política Nacional de Seguridad Digital*. Bogotá D.C. Recuperado a partir de https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Icontec. (2013). *NTC-ISO-IEC 27001:2013 – TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS*. Bogotá D.C. Recuperado a partir de https://tienda.icontec.org/producto/impreso-ntc-iso-iec27001-tecnologia-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-la-seguridad-de-la-informacion-requisitos/?v=42983b05e2f2

Icontec. (2015). *NTC-ISO-IEC 27002:2015 – TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN – Tienda ICONTEC*. Bogotá. Recuperado a partir de

https://tienda.icontec.org/producto/e-book-gtc-iso-iec27002-tecnologia-de-la-informacion-tecnicas-de-seguridad-codigo-de-practica-para-controles-de-seguridad-de-la-informacion/?v=42983b05e2f2

Icontec. (2018). *NTC-ISO 31000 - Gestión de riesgos: Principios y directrices*. Recuperado a partir de https://tienda.icontec.org/producto/impreso-ntc-iso31000-gestion-del-riesgo-principios-y-directrices/?v=42983b05e2f2

ISACA. (2018). COBIT 2019. Recuperado 4 de diciembre de 2018, a partir de https://www.isaca.org/cobit/pages/default.aspx

ISECOM. (2010). *OSSTMM 3 – The Open Source Security Testing Methodology Manual*. Recuperado a partir de www.osstmm.org

ISO/IEC. (2018a). ISO/IEC 27005:2018 - Information technology -- Security techniques -- Information security risk management. Recuperado 9 de diciembre de 2018, a partir de https://www.iso.org/standard/75281.html

ISO/IEC. (2018b). ISO / IEC 27000: 2018 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario. Recuperado 9 de diciembre de 2018, a partir de https://www.iso.org/standard/73906.html

ISO. (2008). ISO/IEC 21827:2008 - Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®). Recuperado 4 de diciembre de 2018, a partir de https://www.iso.org/standard/44716.html

Locke, G., & Gallagher, P. D. (2011). *Managing Information Security Risk Organization, Mission, and Information System View JOINT TASK FORCE TRANSFORMATION INITIATIVE*. https://doi.org/10.6028/NIST.SP.800-39

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid. Recuperado a partir de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XAOD02j0mUk

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015a). Modelo de Seguridad. Recuperado 16 de agosto de 2018, a partir de https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015b). *Modelo de Seguridad y Privacidad de la Información*. Bogotá D.C. Recuperado a partir de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016a). *Guía de gestión de riesgos - Guía No. 7*. Bogotá D.C. Recuperado a partir de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016b). *Guía Metodológica de Pruebas de Efectividad*. Bogotá D.C. Recuperado a partir de

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

Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). *Modelo de Gestión de Riesgos de Seguridad Digital –MGRSD-*. Bogotá D.C. Recuperado a partir de https://www.mintic.gov.co/portal/604/articles-61854_documento.docx

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Manual de gobierno digital*. Bogotá. Recuperado a partir de http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_recurso_1.pdf

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*. Recuperado a partir de https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013*. Recuperado a partir de https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Presidencia de la República de Colombia. (2015). *Decreto 0103 de 2015*. Recuperado a partir de http://wsp.presidencia.gov.co/secretaria-transparencia/Prensa/2015/Documents/decreto_presidencial_103_del_20_de_enero_2015.pdf

Presidencia de la República de Colombia. (2017). *Decreto 1499 de 2017*. Bogotá D.C. Recuperado a partir de http://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=83433

PTES. (2012). Pautas técnicas de PTES - El estándar de ejecución de pruebas de penetración. Recuperado 9 de diciembre de 2018, a partir de http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Ross, W. L., & Rochford, K. (2017). *Draft NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations*. Recuperado a partir de http://csrc.nist.gov/publications.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. Recuperado a partir de https://www.archives.gov/files/era/recompete/sp800-30.pdf

The open group. (2018a). *Modelo abierto de madurez de la gestión de la seguridad de la información (O-ISM3), versión 2.0*. Recuperado a partir de https://publications.opengroup.org/c17b

The open group. (2018b). *TOGAF 9.2 | The Open Group*. Recuperado a partir de http://www.opengroup.org/togaf