GUÍA TÉCNICA COLOMBIANA GTC-ISO/IEC 27003

2012-12-12

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

E: INFORMATION TECHNOLOGY- SECURITY TECHNIQUES. INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION GUIDANCE

CORRESPONDENCIA:	esta norma es una adopción idéntica (IDT) de la norma ISO/IEC 27003: 2010.
DESCRIPTORES:	tecnología de la información; técnicas de seguridad; información; seguridad de la información; sistema de gestión.

I.C.S.: 35.040

Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)
Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888 - Fax (571) 2221435

 Editada 2012-12-21

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 2269 de 1993.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

La GTC-ISO/IEC 27003 fue ratificada por el Consejo Directivo de 2012-12-12.

Esta guía está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se relacionan las empresas que colaboraron en el estudio de esta guía a través de su participación en el Comité Técnico 181 Gestión de T.I..

BANCO AGRARIO DE COLOMBIA S.A.
CROSS BORDER TECHNOLOGY S.A.S.
HOSPITAL PABLO TOBÓN URIBE
INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR -ICBF-
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
PROJECT ADVANCED MANAGEMENT
SUN GEMINI S.A.
TOP FACTORY S.A.
UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

Además de las anteriores, en Consulta Pública el Proyecto se puso a consideración de las siguientes empresas:

A TODA HORA S.A ATH
ACH COLOMBIA S.A.
ACTUALIZACIONES DE SISTEMAS LTDA.
AEROVÍAS DEL CONTINENTE AMERICANO S.A. -AVIANCA S.A.-
AGENDA DE CONECTIVIDAD
ALIANZA SINERTIC
ARCHIVO GENERAL DE LA NACIÓN
BANCO CAJA SOCIAL
BANCO COMERCIAL AV VILLAS
BANCO DAVIVIENDA S.A.
BANCO DE BOGOTÁ
BANCO DE LA REPÚBLICA
BANCO GNB SUDAMERIS
BRANCH OF MICROSOFT COLOMBIA INC
CAJA COLOMBIANA DE SUBSIDIO FAMILIAR COLSUBSIDIO
CENTRO DE INVESTIGACIÓN Y DESARROLLO EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
CENTRO POLICLÍNICO DEL OLAYA C.P.O. S.A.
CHOUCAIR TESTING S.A.
CIBERCALL S.A.
COLOMBIA TELECOMUNICACIONES S.A. E.S.P.
COMERCIO ELECTRÓNICO EN INTERNET CENET S.A.
COMPUREDES S.A.
CONTRALORÍA DE CUNDINAMARCA

COOPERATIVA DE PROFESIONALES DE LA SALUD -PROSALCO I.P.S.-
CREDIBANCO
DAKYA LTDA.
ECOPETROL S.A.
ENLACE OPERATIVO S.A.
ETB S.A. E.S.P.
FLUIDSIGNAL GROUP S.A.
FONDO DE EMPLEADOS DEL DEPARTAMENTO DE ANTIOQUIA
FUNDACIÓN PARQUE TECNOLÓGICO DEL SOFTWARE DE CALI -PARQUESOFT-
FUNDACIÓN UNIVERSITARIA INPAHU
GESTIÓN & ESTRATEGIA S.A.S.
GETRONICS COLOMBIA LTDA.
GIT LTDA.
HERRAMIENTAS PARA EL MEJORAMIENTO DEL TRABAJO LTDA.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
INFOCOMUNICACIONES S.A.S.
INFOTRACK S.A.
INSTITUTO DE ORTOPEDIA INFANTIL ROOSEVELT
IPX LTDA.
IQ CONSULTORES
IT SERVICE LTDA.
JAIME TORRES C. Y CÍA. S.A.
JIMMY EXENOVER ESPINOSA LÓPEZ
KEXTAS LTDA.
LOGIN LEE LTDA.
MAKRO SUPERMAYORISTA S.A.
MAREIGUA LTDA.
MEGABANCO
MICROCOM COMUNICACIÓN Y SEGURIDAD LTDA.
NEGOTEC NEGOCIOS Y TECNOLOGÍA LTDA.
NEWNET S.A.
NEXOS SOFTWARE S.A.S
OUTSOURCING S.A
PARQUES Y FUNERARIAS S.A.
JARDINES DEL RECUERDO
PIRAMIDE ADMINISTRACION DE INFORMACION LTDA.
POLITÉCNICO MAYOR AGENCIA CRISTIANA DE SERVICIO Y EDUCACIÓN LTDA.
PONTIFICIA UNIVERSIDAD JAVERIANA
QUALITY SYSTEMS LTDA.
SISTEMAS Y FORMACIÓN S.A.S
SOCIEDAD COLOMBIANA DE ARCHIVISTAS
SYNAPSIS COLOMBIA LTDA.
TEAM FOODS COLOMBIA S.A.
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES DE COLOMBIA LTDA.
TELMEX COLOMBIA S.A.
TIQAL S.A.S
TOMÁS MORENO CRUZ Y CÍA. LTDA.
TRANSFIRIENDO S.A.
TRANSPORTADORA DE VALORES ATLAS LTDA.
TUS COMPETENCIAS LTDA.
UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS
UNIVERSIDAD JAVERIANA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
UNIVERSIDAD NACIONAL DE COLOMBIA
UNIVERSIDAD SANTIAGO DE CALI

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

Página

Página

Página

TECNOLOGÍA DE LA INFORMACIÓN.
TÉCNICAS DE SEGURIDAD.
GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. OBJETO Y CAMPO DE APLICACIÓN

Esta guía se enfoca en los aspectos críticos necesarios para el diseño e implementación exitosos de un Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo con la norma ISO/IEC 27001:2005 (NTC-ISO/IEC 27001:2006). En la misma se describen los procesos de especificación y diseño de un SGSI, desde el inicio hasta la producción de los planes de implementación. Aquí se describe el proceso para obtener la aprobación de la dirección para implementar un SGSI, se define un proyecto para implementar un SGSI (referido en esta norma como el proyecto de SGSI), y se brinda orientación sobre cómo planificar el proyecto de SGSI, que da como resultado un plan de implementación final del proyecto de SGSI.

Esta guía está prevista para ser usada por organizaciones que se encuentren implementando un SGSI. Es aplicable a todos los tipos de organizaciones (por ejemplo, empresas comerciales, organismos gubernamentales, organizaciones sin fines de lucro) de cualquier tamaño. La complejidad y los riesgos de las organizaciones son únicos, y sus requisitos específicos dirigirán la implementación del SGSI. Las organizaciones pequeñas encontrarán que las actividades descritas en esta guía son aplicables a ellas y que se pueden simplificar. Las organizaciones grandes o complejas pueden requerir una organización o un sistema de gestión estratificados para administrar las actividades de esta norma de forma eficaz. Sin embargo, en ambos casos, las actividades pertinentes se pueden planificar aplicando esta guía.

Esta norma brinda recomendaciones y explicaciones, sin especificar requisito alguno. La intención de esta norma es que se utilice en conjunto con la ISO/IEC 27001:2005 (NTC-ISO/IEC 27001:2006) y la ISO/IEC 27002:2005 (NTC-ISO/IEC 27002:2007), pero sin modificar o reducir, o ambos, los requisitos especificados en ISO/IEC 27001:2005 (NTC-ISO/IEC 27001:2006), o las recomendaciones provistas en ISO/IEC 27002:2005 (NTC-ISO/IEC 27002:2007). No es adecuado declarar conformidad con esta norma.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos son indispensables para la aplicación de esta norma. Para las referencias con fecha sólo se aplica la edición citada. Para referencias sin fecha, se aplica la última edición del documento referenciado (incluida cualquier corrección).

ISO/IEC 27000:2009, *Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary.*

ISO/IEC 27001:2005 (NTC-ISO/IEC 27001:2006), Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento se aplican los términos y definiciones de la norma ISO/IEC 27000, NTC-ISO/IEC 27001 y los siguientes.

3.1 Proyecto de SGSI. Actividades estructuradas, llevadas a cabo por una organización para implementar un SGSI.

BIBLIOGRAFÍA

[1] ISO 9001:2008, *Quality Management Systems. Requirements.*

[2] ISO 14001:2004, *Environmental Management Systems. Requirements with Guidance for Use.*

[3] ISO/IEC 15026 (*All Parts*), *Systems and Software Engineering. Systems and Software Assurance*[1].

[4] ISO/IEC 15408-1:2009, *Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 1: Introduction and General Model.*

[5] ISO/IEC 15408-2:2008, *Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 2: Security Functional Components.*

[6] ISO/IEC 15408-3:2008, *Information Technology. Security Techniques. Evaluation criteria for IT Security. Part 3: Security Assurance Components.*

[7] ISO/IEC TR 15443-1:2005, *Information Technology. Security Techniques. A Framework for IT Security Assurance. Part 1: Overview and Framework.*

[8] ISO/IEC TR 15443-2:2005, *Information Technology. Security Techniques. A Framework for IT Security Assurance. Part 2: Assurance Methods.*

[9] ISO/IEC TR 15443-3:2007, *Information Technology. Security Techniques. A Framework for IT Security Assurance. Part 3: Analysis of Assurance Methods.*

[10] ISO/IEC 15939:2007, *Systems and Software Engineering. Measurement Process*

[11] ISO/IEC 16085:2006, *Systems and Software Engineering. Life Cycle Processes .Risk Management.*

[12] ISO/IEC 16326:2009, *Systems and Software Engineering. Life Cycle Processes. Project Management.*

[13] ISO/IEC 18045:2008, *Information Technology. Security Techniques. Methodology for IT Security Evaluation.*

[14] ISO/IEC TR 19791:2006, *Information Technology. Security Techniques. Security Assessment of Operational Systems.*

[15] ISO/IEC 20000-1:2005, *Information Technology. Service Management. Part 1: Specification*

[16] ISO/IEC 27001:2005, *Information Technology. Security Techniques. Information Security Management Systems. Requirements*

[17] ISO/IEC 27004:2009, *Information Technology. Security Techniques. Information Security Management. Measurement.*

[1] To be published

[18] ISO/IEC 27005:2008, *Information Technology. Security Techniques. Information Security Risk Management.*

[19] ISO 21500, *Project Management. Guide to Project Management*[2]*.*

[20] ISO/IEC 27006:2007 *Information Technology. Security Techniques. Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.*

...

[2] Under preparation

IMPORTANTE

Este resumen no contiene toda la información necesaria para la aplicación del documento normativo original al que se refiere la portada. ICONTEC lo creo para orientar a su cliente sobre el alcance de cada uno de sus documentos y facilitar su consulta. Este resumen es de libre distribución y su uso es de total responsabilidad del usuario final.

El documento completo al que se refiere este resumen puede consultarse en los centros de información de ICONTEC en Bogotá, Medellín, Barranquilla, Cali o Bucaramanga, también puede adquirirse a través de nuestra página web o en nuestra red de oficinas (véase www.icontec.org).

Información de servicios aplicables al documento aquí referenciado la encuentra en: www.icontec.org o por medio del contacto cliente@icontec.org.

ICONTEC INTERNACIONAL