NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001

2013-12-11

TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. REQUISITOS

E: INFORMATION TECHNOLOGY. SECURITY TECHNIQUES. INFORMATION SECURITY MANAGEMENT SYSTEMS. REQUIREMENTS.

CORRESPONDENCIA:	esta norma es una adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001: 2013.
DESCRIPTORES:	sistemas de gestión - seguridad de la información; información, técnicas de seguridad, 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

Primera actualización
Editada 2013-12-20

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 norma NTC-ISO-IEC 27001 (Primera actualización) fue ratificada por el Consejo Directivo de 2013-12-11.

Esta norma 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 norma a través de su participación en el Comité Técnico 181 Gestión de la tecnología de la información.

AVIANCA S.A.
AZTECA COMUNUCACIONES
BANCO AGRARIO DE COLOMBIA S.A.
CENET S.A.
CROSS BORDER TECHNOLOGY S.A.S.
ECOPETROL - SLB
ESICENTER - SINERTIC
GEOCONSULT - ECP
HALLIBURTON - ECOPETROL
HELM BANK
INFOTRACK S.A.
INLAC
LA POLAR- CF
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
NEWNET S.A.
PROJECT ADVANCED MANAGEMENT
QUALITIC LTDA
SERVIENTREGA
TOP FACTORY

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.
AGENDA DE CONECTIVIDAD
ALFAPEOPLE ANDINO S.A.
ALIANZA SINERTIC
BANCO CAJA SOCIAL
BANCO COMERCIAL AV VILLAS
BANCO DAVIVIENDA S.A.
BANCO DE BOGOTÁ
BANCO DE LA REPÚBLICA
BANCO DE OCCIDENTE
BRANCH OF MICROSOFT COLOMBIA INC
CAJA COLOMBIANA DE SUBSIDIO FAMILIAR COLSUBSIDIO
CENTRO DE INVESTIGACIÓN Y DESARROLLO EN TECNOLOGIAS DE LA INFORMACION 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.-
CORREDOR EMPRESARIAL CREDIBANCO
CRUZ ROJA COLOMBIANA SECCIONAL CUNDINAMARCA Y BOGOTÁ
DAKYA LTDA.
DIGIWARE
ECOPETROL S.A.
ENLACE OPERATIVO S.A.
ESCUELA COLOMBIANA DE CARRERAS INDUSTRIALES
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
GEMAS INGENIERIA Y CUNSULTORIA SAS
GESTIÓN & ESTRATEGIA S.A.S.
GETRONICS COLOMBIA LTDA.
GIT LTDA.
HMT S.A.S.
HOSPITAL SAN VICENTE ESE DE MONTENEGRO
INFOCOMUNICACIONES S.A.S.
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.
NEXOS SOFTWARE S.A.S.
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
SUN GEMINI S.A.
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 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

INTRODUCCIÓN

0.1 GENERALIDADES

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.

La presente Norma puede ser usada por partes internas y externas para evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la propia organización.

El orden en que se presentan los requisitos en esta Norma no refleja su importancia ni el orden en el que se van a implementar. Los elementos de la lista se enumeran solamente para propósitos de referencia.

La ISO/IEC 27000 describe la visión general y el vocabulario de sistemas de gestión de la seguridad de la información, y referencia la familia de normas de sistemas de gestión de la seguridad de la información (incluidas las NTC-SO/IEC 27003[2], ISO/IEC 27004[3] y ISO/IEC 27005[4]), con los términos y definiciones relacionadas.

0.2 COMPATIBILIDAD CON OTRAS NORMAS DE SISTEMAS DE GESTIÓN

Esta Norma aplica la estructura de alto nivel, títulos idénticos de numerales, texto idéntico, términos comunes y definiciones esenciales definidas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado, y por tanto, mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que decidan poner en funcionamiento un único sistema de gestión que cumpla los requisitos de dos o más normas de sistemas de gestión.

TECNOLOGÍA DE LA INFORMACIÓN.
TÉCNICAS DE SEGURIDAD.
SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
REQUISITOS

1. OBJETO Y CAMPO DE APLICACIÓN

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Cuando una organización declara conformidad con esta Norma, no es aceptable excluir cualquiera de los requisitos especificados de los numerales 4 al 10.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

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

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información.

NOTA La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.3 de la NTC-ISO 31000:2011[5].

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La organización debe determinar:

a) las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información; y

b) los requisitos de estas partes interesadas pertinentes a seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.

4.3 DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Cuando se determina este alcance, la organización debe considerar:

a) las cuestiones externas e internas referidas en el numeral 4.1, y

b) los requisitos referidos en el numeral 4.2; y

c) las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información:

a) asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización;

b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;

d) comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;

e) asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos;

f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) promoviendo la mejora continua, y

h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.

5.2 POLÍTICA

La alta dirección debe establecer una política de la seguridad de la información que:

a) sea adecuada al propósito de la organización;

b) incluya objetivos de seguridad de la información (véase el numeral 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información;

c) incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; y

d) incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de la seguridad de la información debe:

e) estar disponible como información documentada;

f) comunicarse dentro de la organización; y

g) estar disponible para las partes interesadas, según sea apropiado.

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;

b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.

6. PLANIFICACIÓN

6.1 ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

6.1.1 Generalidades

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones referidas en el numeral 4.1 y los requisitos a que se hace referencia en el numeral 4.2, y determinar los riesgos y oportunidades que es necesario tratar, con el fin de:

a) asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos;

b) prevenir o reducir efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para tratar estos riesgos y oportunidades; y

e) la manera de:

   1) integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información,

   2) evaluar la eficacia de estas acciones.

6.1.2 Valoración de riesgos de la seguridad de la información

La organización debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que:

a) establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan:

   1) Los criterios de aceptación de riesgos; y

   2) los criterios para realizar valoraciones de riesgos de la seguridad de la información;

b) asegure que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identifique los riesgos de la seguridad de la información:

   1) aplicar el proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e

   2) identificar a los dueños de los riesgos;

d) analice los riesgos de la seguridad de la información:

1) Valorar las consecuencias potenciales que resultaran si se materializaran los riesgos identificados en 6.1.2 c) 1);

2) Valorar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 c) 1); y

3) determinar los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a) y

2) priorizar los riesgos analizados para el tratamiento de riesgos.

La organización debe conservar información documentada acerca del proceso de valoración de riesgos de la seguridad de la información.

6.1.3 Tratamiento de riesgos de la seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para:

a) seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información;

NOTA Las organizaciones pueden diseñar los controles necesarios, o identificarlos de cualquier fuente.

c) comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se han omitidos controles necesarios;

NOTA 1 El Anexo A contiene una lista amplia de objetivos de control y controles. Se invita a los usuarios de esta Norma a consultar el Anexo A, para asegurar que no se pasen por alto los controles necesarios.

NOTA 2 Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles enumerados en el Anexo A no son exhaustivos, y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A;

e) formular un plan de tratamiento de riesgos de la seguridad de la información; y

f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información.

La organización debe conservar información documentada acerca del proceso de tratamiento de riesgos de la seguridad de la información.

NOTA El proceso de valoración y tratamiento de riesgos de la seguridad de la información que se presenta en esta Norma se alinea con los principios y directrices genéricas suministradas en la ISO 31000[5].

6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLOS

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

a) ser coherentes con la política de seguridad de la información;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la valoración y del tratamiento de los riesgos;

d) ser comunicados; y

e) ser actualizados, según sea apropiado.

La organización debe conservar información documentada sobre los objetivos de la seguridad de la información.

Cuando se hace la planificación para lograr sus objetivos de la seguridad de la información, la organización debe determinar:

f) lo que se va a hacer;

g) que recursos se requerirán;

h) quién será responsable;

i) cuándo se finalizará; y

j) cómo se evaluarán los resultados.

7. SOPORTE

7.1 RECURSOS

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

7.2 COMPETENCIA

La organización debe:

a) determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y

b) asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas;

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

d) conservar la información documentada apropiada, como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes.

7.3 TOMA DE CONCIENCIA

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de:

a) la política de la seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y

c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información.

7.4 COMUNICACIÓN

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan:

a) el contenido de la comunicación;

b) cuándo comunicar;

c) a quién comunicar;

d) quién debe comunicar; y

e) los procesos para llevar a cabo la comunicación.

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 Generalidades

El sistema de gestión de la seguridad de la información de la organización debe incluir:

a) la información documentada requerida por esta Norma; y

b) la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA El alcance de la información documentada para un sistema de gestión de la seguridad de la información puede ser diferente de una organización a otra, debido a:

a) el tamaño de la organización y a su tipo de actividades, procesos, productos y servicios,

b) la complejidad de los procesos y sus interacciones, y

c) la competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico);

c) la revisión y aprobación con respecto a la idoneidad y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta Norma se debe controlar para asegurarse de que:

a) esté disponible y adecuada para su uso, donde y cuando se necesite; y

b) esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluida la preservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión); y

f) retención y disposición.

La información documentada de origen externo, que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar y controlar, según sea adecuado.

NOTA El acceso implica una decisión concerniente al permiso solamente para consultar la información documentada, o el permiso y la autoridad para consultar y modificar la información documentada, etc.

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el numeral 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el numeral 6.2.

La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario.

La organización debe asegurar que los procesos contratados externamente estén controlados.

8.2 VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe llevar a cabo valoraciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2 a).

La organización debe conservar información documentada de los resultados de las valoraciones de riesgos de la seguridad de la información.

8.3 TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información.

La organización debe conservar información documentada de los resultados del tratamiento de riesgos de la seguridad de la información.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos;

NOTA Para ser considerados válidos, los métodos seleccionados deberían producir resultados comparables y reproducibles.

c) cuándo se deben llevar a cabo el seguimiento y la medición;

d) quién debe llevar a cabo el seguimiento y la medición;

e) cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición; y

f) quién debe analizar y evaluar estos resultados.

La organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

9.2 AUDITORÍA INTERNA

La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información:

a) es conforme con:

   1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y

   2) los requisitos de esta Norma;

b) está implementado y mantenido eficazmente.

La organización debe:

c) planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas;

d) para cada auditoría, definir los criterios y el alcance de ésta;

e) seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

f) asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y

g) conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.

NOTA Para mayor información consultar las normas NTC-ISO 19011 y NTC-ISO 27007

9.3 REVISIÓN POR LA DIRECCIÓN

La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

La revisión por la dirección debe incluir consideraciones sobre:

a) el estado de las acciones con relación a las revisiones previas por la dirección;

b) los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información;

c) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a:

   1) no conformidades y acciones correctivas;

   2) seguimiento y resultados de las mediciones;

3) resultados de la auditoría; y

4) cumplimiento de los objetivos de la seguridad de la información;

d) retroalimentación de las partes interesadas;

e) resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos; y

f) las oportunidades de mejora continúa.

Los elementos de salida de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de la seguridad de la información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones por la dirección.

10. MEJORA

10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Cuando ocurra una no conformidad, la organización debe:

a) reaccionar ante la no conformidad, y según sea aplicable

1) tomar acciones para controlarla y corregirla, y

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:

1) la revisión de la no conformidad

2) la determinación de las causas de la no conformidad, y

3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de las acciones correctivas tomadas, y

e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La organización debe conservar información documentada adecuada, como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior tomada; y

g) los resultados de cualquier acción correctiva.

10.2 MEJORA CONTINUA

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.

ANEXO A
(Normativo)

OBJETIVOS DE CONTROL Y CONTROLES DE REFERENCIA

Los objetivos de control y controles enumerados en la Tabla A.1 se obtienen directamente de la ISO/IEC 27002:2013[1], numerales 5 a 18 y están alineados con ella, y se deben usar en contexto con el numeral 6.1.3.

Tabla A.1. Objetivos de control y controles

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control* Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**	
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.

Continúa…

Tabla A.1. (Continuación)

A.6.2.2	Teletrabajo	*Control* Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
A.7.1	**Antes de asumir el empleo**	
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**	
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación y cambio de empleo**	
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Tabla A.1. (Continuación)

A.8	**GESTIÓN DE ACTIVOS**	
A.8.1	**Responsabilidad por los activos**	
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	**Clasificación de la información**	
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3	**Manejo de medios**	
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	*Control* Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Tabla A.1. (Continuación)

A.9	**CONTROL DE ACCESO**	
A.9.1	**Requisitos del negocio para control de acceso**	
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	**Gestión de acceso de usuarios**	
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

Tabla A.1. (Continuación)

A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas.
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		
A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

Tabla A.1. (Continuación)

A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control* Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Tabla A.1. (Continuación)

A.12.1.3	Gestión de capacidad	*Control* Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3 Copias de respaldo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4 Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5 Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		
A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Tabla A.1. (Continuación)

A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
A.12.7	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Tabla A.1. (Continuación)

A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

Tabla A.1. (Continuación)

A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15 RELACIONES CON LOS PROVEEDORES		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2 Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Tabla A.1. (Continuación)

A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	*Control* Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Tabla A.1. (Continuación)

A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* *Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización*
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Reglamentación de controles criptográficos	*Control* Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

BIBLIOGRAFÍA

[1] ISO/IEC 27002:2013, *Information Technology. Security Techniques. Code of Practice for Information Security Controls.*

[2] GTC-ISO/IEC 27003:2012, Tecnología de la información. técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información.

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

[4] ISO/IEC 27005:2011, *Information Technology. Security Techniques. Information Security Risk Management.*

[5] NTC-ISO 31000:2011, Gestión del riesgo. Principios y directrices.

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement. Procedures Specific to ISO*, 2012.

DOCUMENTO DE REFERENCIA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva*: ISO, 2013, 23 p. (ISO/IEC 27001:2013 (E)).