 [Traducido del inglés al español - www.onlinedoctranslator.com](https://www.onlinedoctranslator.com/es/?utm_source=onlinedoctranslator&utm_medium=docx&utm_campaign=attribution)

INTERNACIONALESTÁNDAR

ISO/CEI 27011

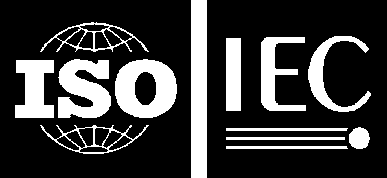
Segunda edición 2016-12-01

**Tecnología de la información — Técnicas de seguridad — Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para organizaciones de telecomunicaciones**

Tecnologías de la información — Técnicas de seguridad — Código de

Buena práctica para el control de la seguridad de la información almacenada.

sobre la norma ISO/IEC 27002 para los organismos de telécomunicaciones

Número de referencia ISO/IEC 27011:2016(E)

©ISO/CEI 2016

**ISO/IEC 27011:2016(E)**

# VISTA PREVIA DEL ESTÁNDAR iTeh

**(estándares.iteh.ai)**

### ISO/CEI 27011:2016

https://standards.iteh.ai/catalog/standards/sist/399a67cc-7efc-417c-8001-24a5665afe78/iso-iec-27011-2016

#### DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR

© ISO/CEI 2016

Reservados todos los derechos. A menos que se especifique lo contrario, ninguna parte de esta publicación puede reproducirse ni utilizarse de ninguna forma ni por ningún medio, electrónico o mecánico, incluidos fotocopias y microfilmes, sin el permiso por escrito de ISO en la dirección que figura a continuación o del organismo miembro de ISO en el país de el solicitante.

Oficina de derechos de autor ISO

Cap. de Blandonnet 8CP 401 tel. + 41 22 749 01 11

Fax +41 22 749 09 47

[copyri](mailto:copyright@iso.org)[ght@iso.org](mailto:ght@iso.org) Web[www.iso.org](http://www.iso.org/)

Publicado en Suiza

ii © ISO/IEC 2016 – Todos los derechos reservados

#### ISO/IEC 27011:2016(E)

**Prefacio**

ISO (la Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para abordar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. También participan en el trabajo otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Las normas internacionales se redactan de acuerdo con las reglas establecidas en las Directivas ISO/IEC, Parte 2.

La principal tarea del comité técnico conjunto es preparar normas internacionales. Los proyectos de normas internacionales adoptados por el comité técnico conjunto se distribuyen a los organismos nacionales para su votación. La publicación como Norma Internacional requiere la aprobación de al menos el 75 % de los organismos nacionales con derecho a voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no serán responsables de identificar cualquiera o todos estos derechos de patente.

Esta segunda edición cancela y reemplaza la primera edición de ISO/IEC 27011:2008 que ha sido técnicamente

revisado.

ISO/IEC 27011 fue preparada por el Comité Técnico Conjunto ISO/IEC JTC 1,*Tecnologías de la información*, Subcomité SC 27*,Técnicas de seguridad informática,*en colaboración con el UIT-T. El texto idéntico se publica como Rec. UIT-T X.1051.

# VISTA PREVIA DEL ESTÁNDAR iTeh

**(estándares.iteh.ai)**

### ISO/CEI 27011:2016

https://standards.iteh.ai/catalog/standards/sist/399a67cc-7efc-417c-8001-24a5665afe78/iso-iec-27011-2016

##### CONTENIDO

*Página*

1 Alcance ................................................. ................................................. ................................................. ......... 1

2 Normativo referencias................................................. ................................................. ................................... 1

3 Definiciones y abreviaturas ............................................... ................................................. ........................ 1

3.1 Definiciones................................................. ................................................. ........................................ 1

3.2 Abreviaturas ................................................. ................................................. ................................... 2

4 Descripción general ................................................. ................................................. ................................................. ... 2

4.1 Estructura de esta Recomendación | Estándar internacional ................................................ ................ 2

4.2 Sistemas de gestión de seguridad de la información en organizaciones de telecomunicaciones ................................ 3

5 Políticas de seguridad de la información................................................ ................................................. ......................... 5

6 Organización de seguridad de la información................................................. ................................................. ............. 5

6.1 Interno organización ................................................. ................................................. ........................ 5

6.2 Móvil Dispositivos y teletrabajo................................................. ................................................. ......... 6

7 Seguridad de los recursos humanos ................................................. ................................................. ................................. 6

7.1 Previo al empleo................................................ ................................................. .......................... 6

7.2 Durante empleo ................................................. ................................................. ......................... 7

7.3 Terminación o cambio de empleo ................................................ ................................................. 7

8 Activo gestión................................................. ................................................. ......................................... 7

8.1 Responsabilidad por los bienes ................................................ ................................................. .................... 7

8.2 Información clasificación................................................. ................................................. ................. 8

8.3 Medios de comunicación manejo................................................. ................................................. ................................. 8

9 Acceso control ................................................. ................................................. ................................................. 8

9.1 Negocio Requisitos para el control de acceso................................................ ................................................. 8

9.2 UsarrGestión de Acceso ................................................ ................................................. .................... 9

9.3 Responsabilidades del usuario ................................................ ................................................. .......................... 9

9.4 sistematemaund solicitud control de acceso ................................................ ................................................. ... 9

10 criptartografia.......................................................................... ................................................. ................................. 9

11 fisicoicaly seguridad ambiental. ................................................. ................................................. ..... 9

11.1 Seguro áreas................................................. ................................................. ........................................ 9

11.2 Equipo 10

1. Seguridad de las operaciones 12
   1. Procedimientos operativos y responsabilidades. 12
   2. Protección contra malware 13
   3. Respaldo 13
   4. Registro y monitoreo 13
   5. Control del software operativo. 13
   6. Gestión técnica de vulnerabilidades 14
   7. Consideraciones de auditoría de sistemas de información 14
2. Seguridad de las comunicaciones 14
   1. Gestión de seguridad de red 14
   2. Transferencia de información 15
3. Adquisición, desarrollo y mantenimiento del sistema. dieciséis
   1. Requisitos de seguridad de los sistemas de información. dieciséis
   2. Seguridad en los procesos de desarrollo y soporte. dieciséis
   3. Datos de prueba dieciséis
4. Relaciones con proveedores dieciséis
   1. Seguridad de la información en las relaciones con proveedores dieciséis
   2. Gestión de prestación de servicios de proveedores. 17
5. Gestión de incidentes de seguridad de la información. 17
   1. Gestión de incidencias y mejoras de seguridad de la información. 17
6. Aspectos de seguridad de la información de la gestión de la continuidad del negocio. 19

*Página*

* 1. Continuidad de la seguridad de la información 19
  2. Despidos 20

1. Cumplimiento 20

Anexo A – Conjunto de control ampliado de telecomunicaciones 21

Anexo B – Orientación adicional para la seguridad de la red 29

* 1. Medidas de seguridad contra ataques a la red 29
  2. Medidas de seguridad de la red para la congestión de la red. 30

Bibliografía 31

# VISTA PREVIA DEL ESTÁNDAR iTeh

**(estándares.iteh.ai)**

### ISO/CEI 27011:2016

https://standards.iteh.ai/catalog/standards/sist/399a67cc-7efc-417c-8001-24a5665afe78/iso-iec-27011-2016

##### Introducción

Esta recomendación | Norma Internacional proporciona pautas de interpretación para la implementación y gestiónde controles de seguridad de la información en organizaciones de telecomunicaciones basados ​​en ISO/IEC 27002.

TelecomunicacionesLas organizaciones brindan servicios de telecomunicaciones facilitando las comunicaciones de los clientes a través de su infraestructura. Para proporcionar servicios de telecomunicaciones, las organizaciones de telecomunicaciones necesitan interconectar y/o compartir sus servicios e instalaciones y/o utilizar los servicios e instalaciones de otras organizaciones de telecomunicaciones. Además, la ubicación del sitio, como sitios de radio, ubicaciones de antenas, cables de tierra y suministro de servicios públicos (energía, agua), puede ser accedido no solo por el personal de la organización, sino también por contratistas y proveedores externos a la organización.

Por tanto, la gestión de la seguridad de la información en las organizaciones de telecomunicaciones es compleja, potencialmente:

* dependiendo de actores externos;
* tener que cubrir todas las áreas de infraestructura de red, aplicaciones de servicios y otras instalaciones;
* incluyendo una variedad de tecnologías de telecomunicaciones (por ejemplo, cableadas, inalámbricas o de banda ancha);
* compatible con una amplia gama de escalas operativas, áreas de servicio y tipos de servicios.

Además de la aplicación de los objetivos y controles de seguridad descritos en ISO/IEC 27002, las organizaciones de telecomunicaciones pueden necesitar implementar controles adicionales para garantizar la confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad de las telecomunicaciones para gestionar el riesgo de seguridad de manera adecuada.

* + 1. *Confidencialidad*

Proteger la confidencialidad de la información relacionada con las telecomunicaciones contra la divulgación no autorizada. Esteimplica no divulgaciónde las comunicaciones en cuanto a la existencia, el contenido, la fuente, el destino y la fecha y hora de la información comunicada.

Es crítico queLas organizaciones de telecomunicaciones garantizan que no se viole la confidencialidad de las comunicaciones que manejan. Esto incluye garantizar que las personas contratadas por la organización de telecomunicaciones mantengan la confidencialidad de cualquier información relativa a otros que pueda haber llegado a conocer durante sus funciones laborales.

NOTA – El término "secreto de las comunicaciones" se utiliza en algunos países en el contexto de la "no divulgación de las comunicaciones".

* + 1. *Integridad*

PAGprotegerthmientegridadohF La información de telecomunicaciones incluye el control de la instalación y el uso de las instalaciones de telecomunicaciones para garantizar la autenticidad, exactitud e integridad de la información.

transmitido, retransmitido o recibido por cable, radio o cualquier otro método.

* + 1. *Disponibilidad*

La disponibilidad de información de telecomunicaciones incluye garantizar que el acceso a las instalaciones y al medio utilizado para la prestación de servicios de comunicación esté autorizado, independientemente de que las comunicaciones se proporcionen por cable, radio o cualquier otro método. Normalmente, las organizaciones de telecomunicaciones dan prioridad a las comunicaciones esenciales en caso de emergencias, gestionando la falta de disponibilidad de comunicaciones menos importantes de conformidad con los requisitos reglamentarios.

##### Audiencia

El público de esta Recomendación | Norma Internacional está formada por organizaciones de telecomunicaciones y responsables de la seguridad de la información; junto con proveedores de seguridad, auditores, proveedores de terminales de telecomunicaciones y proveedores de contenido de aplicaciones. Esta recomendación | Norma Internacional proporciona un conjunto común de objetivos generales de control de seguridad basados ​​en ISO/IEC 27002, controles específicos del sector de telecomunicaciones y directrices de gestión de seguridad de la información que permiten la selección e implementación de dichos controles.

# VISTA PREVIA DEL ESTÁNDAR iTeh

**(estándares.iteh.ai)**

### ISO/CEI 27011:2016

https://standards.iteh.ai/catalog/standards/sist/399a67cc-7efc-417c-8001-24a5665afe78/iso-iec-27011-2016

##### ISO/IEC 27011:2016 (ES)

**INTERNACIONALRECOMENDACIÓN ESTÁNDAR UIT-T**

**Tecnología de la información – Técnicas de seguridad – Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para organizaciones de telecomunicaciones**

1. **Alcance**

El alcance de esta Recomendación | Norma Internacional es definir directrices que respalden la implementación de controles de seguridad de la información en organizaciones de telecomunicaciones.

La adopción de esta Recomendación | Norma Internacional permitirá a las organizaciones de telecomunicaciones cumplir con los requisitos básicos de gestión de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.

## Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante referencia en este texto, constituyen disposiciones de esta Recomendación | Estándar internacional. En el momento de la publicación, las ediciones indicadas eran válidas. Todas las Recomendaciones y Normas están sujetas a revisión, y las partes en acuerdos basados ​​en esta Recomendación | Norma Internacional se recomienda investigar la posibilidad de aplicar la edición más reciente de las Recomendaciones y Normas que se enumeran a continuación. Los miembros de IEC e ISO mantienen registros de las normas internacionales actualmente válidas. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de Recomendaciones UIT-T actualmente válidas.

* + ISO/IEC 27000, Tecnología de la información –*Técnicas de seguridad – Sistemas de gestión de seguridad de la información*

*– Visión general y vocabulario.*

* + ISO/IEC 27002:2013, Tecnología de la información – Técnicas de seguridad – Código de prácticas para la información

*seguridadcontrol S.*

## Definiciones y abreviaturas

* 1. **Definiciones**

### 

A los efectos de esta Recomendación | Norma Internacional, se aplican las definiciones dadas en ISO/IEC 27000 y lo siguiente:

* + 1. **coubicación**: Instalación de instalaciones de telecomunicaciones en instalaciones de otros operadores de telecomunicaciones.
    2. **centro de comunicacion**: Edificio donde se ubican instalaciones para la prestación de servicios de telecomunicaciones.
    3. **comunicaciones esenciales**: Comunicaciones cuyo contenido sea necesario para la prevención o socorro de desastres y para el mantenimiento del orden público en condiciones adversas.
    4. **no divulgación de comunicaciones**: Obligación de no revelar la existencia, el contenido, la fuente, el destino y la fecha y hora de la información comunicada.
    5. **llamada prioritaria**: Telecomunicaciones realizadas por terminales específicos en caso de emergencias, que deberán atenderse prioritariamente restringiendo las llamadas públicas.

NOTA – Los terminales específicos pueden abarcar diferentes servicios (vozsobre protocolo de Internet (VoIP), voz de red telefónica pública conmutada (PSTN), tráfico de datos de protocolo de Internet (IP), etc.) para redes cableadas e inalámbricas.

* + 1. **aplicaciones de telecomunicaciones**: Aplicaciones como Voz sobre IP (VoIP) que consumen los usuarios finales y se basan en los servicios basados ​​en la red.
    2. **negocio de telecomunicaciones**: Empresa destinada a prestar servicios de telecomunicaciones con el fin de satisfacer la demanda de otros.
    3. **sala de equipos de telecomunicaciones**: Un lugar o habitación segura dentro de un edificio general donde se ubican los equipos para proporcionar negocios de telecomunicaciones.
    4. **instalaciones de telecomunicaciones**: Máquinas, equipos, alambres y cables, edificios físicos u otras instalaciones eléctricas para la operación de telecomunicaciones.

##### ISO/IEC 27011:2016 (ES)

* + 1. **organizaciones de telecomunicaciones**: Entidades comerciales que brindan servicios de telecomunicaciones con el fin de satisfacer la demanda de otros.
    2. **registros de telecomunicaciones**: Información relativa a las partes en una comunicación, excluyendo el contenido de la comunicación, y la hora y duración de la telecomunicación que tuvo lugar.
    3. **servicios de telecomunicaciones**: Comunicaciones utilizando instalaciones de telecomunicaciones, o cualquier otro medio para proporcionar comunicaciones ya sea entre usuarios de servicios de telecomunicaciones o clientes de servicios de telecomunicaciones.
    4. **cliente de servicio de telecomunicaciones**: Persona u organización que celebra un contrato con organizaciones de telecomunicaciones para que éstas les ofrezcan servicios de telecomunicaciones.
    5. **usuario de servicios de telecomunicaciones**: Persona u organización que utiliza servicios de telecomunicaciones.
    6. **instalaciones terminales**: Instalaciones de telecomunicaciones que se conectarán a un extremo de las instalaciones del circuito de telecomunicaciones y parte de las cuales se instalarán en el mismo local (incluidas las áreas consideradas como el mismo local) o en el mismo edificio donde también se instalará cualquier otra parte del mismo. estar instalado.
    7. **usuario**: Persona u organización que utiliza instalaciones o sistemas de procesamiento de información, por ejemplo, empleado, contratista o usuario externo.
  1. **Abreviaturas**

A los efectos de esta Recomendación | Norma Internacional, se aplican las siguientes abreviaturas:

CIA Confidencialidad, Integridad y Disponibilidad

CNI Infraestructura Nacional Crítica

DDoS Denegación de servicio distribuida

DNS sistema de nombres de dominio

DoS Negación de servicio

climatización Calefacción, ventilación y aire acondicionado

IP InternetProtocolo

IRC InternetChat de retransmisión

ISAC Centro de análisis e intercambio de información

SGSI Sistema de gestión de seguridad de la información

NMS Administración de redesSistema

OAM&P Operaciones, Administración, Mantenimiento y Aprovisionamiento

PSTN Red Telefónica Conmutada

SORBO protocolo de Iniciacion de Sesion

SLA Acuerdo de nivel de servicio

SMS CortoServicio de mensajes

SOA Declaración de aplicabilidad

URL Localizador Uniforme de Recursos

VoIP Voz sobre Protocolo de Internet

|  |  |  |
| --- | --- | --- |
| **4** | **Descripción general** |  |

#### Estructura de esta Recomendación | Estándar internacional

Esta recomendación | La Norma Internacional se ha estructurado en un formato similar a ISO/IEC 27002. En los casos en los que los objetivos y controles especificados en ISO/IEC 27002 son aplicables sin necesidad de información adicional, solo se proporciona una referencia a ISO/IEC 27002. Una norma de telecomunicaciones El conjunto de orientaciones de control e implementación específicos del sector se describe en el Anexo normativo A.

En los casos en que los controles necesiten orientación adicional específica para las telecomunicaciones, el control ISO/IEC 27002 se repite sin modificaciones, seguido de la orientación específica de telecomunicaciones relacionada con este control. En las siguientes cláusulas se incluye orientación e información específica del sector de las telecomunicaciones:

* + - Organización de la seguridad de la información (cláusula 6)

##### ISO/IEC 27011:2016 (ES)

* + - Seguridad de los recursos humanos (cláusula 7)
    - Gestión de activos (cláusula 8)
    - Control de acceso (cláusula 9)
    - Seguridad física y ambiental (cláusula 11)
    - Seguridad de las operaciones (cláusula 12)
    - Seguridad de las comunicaciones (cláusula 13)
    - Adquisición, desarrollo y mantenimiento de sistemas (cláusula 14)
    - Relaciones con proveedores (cláusula 15)
    - Gestión de incidentes de seguridad de la información (cláusula 16)
    - Aspectos de seguridad de la información de la gestión de la continuidad del negocio (cláusula 17)

#### Sistemas de gestión de seguridad de la información en organizaciones de telecomunicaciones.

##### Meta

La información es fundamental para toda organización. En el caso de las telecomunicaciones, la información consiste en datos transmitidos entre dos puntos cualesquiera en una formación electrónica, así como metadatos de cada transmisión, por ejemplo, datos de posicionamiento del remitente y del receptor. Independientemente de cómo se transmita la información y de si se almacena en caché o durante la transmisión, la información siempre debe protegerse adecuadamente.

Las organizaciones de telecomunicaciones y sus sistemas y redes de información están expuestos a amenazas a la seguridad provenientes de una amplia gama de fuentes, entre ellas: escuchas telefónicas; amenazas persistentes avanzadas; terrorismo; espionaje; sabotaje; vandalismo; fuga de información; errores; y eventos de fuerza mayor. Estas amenazas a la seguridad pueden originarse desde dentro o fuera de la organización de telecomunicaciones, lo que resulta en daños a la organización.

Una vez que se viola la seguridad de la información, por ejemplo, mediante escuchas telefónicas en las líneas de telecomunicaciones, la organización puede sufrir

daño. Por lo tanto, es esencial que una organización garantice la seguridad de su información mediante la mejora continua de su

sistema de gestión de seguridad de la información (SGSI).

La seguridad efectiva de la información se logra implementando un conjunto adecuado de controles basados ​​en los descritos en este

Recomendación | Estándar internacional. Estos controles deben establecerse, implementarse, monitorearse, revisarse y

mejorado en instalaciones, servicios y aplicaciones de telecomunicaciones. Estas actividades permitirán a una organización cumplir

sus objetivos de seguridad y por tanto su objetivo de negocio.

Las organizaciones de telecomunicaciones brindan facilidades a varios tipos de usuarios para procesar, transmitir y almacenar información. Esta información podría ser información de identificación personal o datos comerciales y privados confidenciales. En todos los casos, la información debe manejarse con el nivel correcto de cuidado y atención, y se deben proporcionar los niveles adecuados de protección para garantizar la confidencialidad, integridad y disponibilidad (CIA), siendo primordial la privacidad y la sensibilidad.

##### Consideraciones de seguridad en las telecomunicaciones

La necesidad de un marco de seguridad genérico en las telecomunicaciones tiene su origen en diferentes fuentes:

* + - 1. clientes/abonados que necesitan confianza en la red y en los servicios que se prestarán, incluida la disponibilidad de servicios (especialmente servicios de emergencia) en caso de catástrofes importantes;
      2. autoridades públicas que exigen seguridad mediante directivas, reglamentos y leyes, para garantizar la disponibilidad de servicios, la competencia leal y la protección de la privacidad;
      3. Los propios operadores de redes y proveedores de servicios necesitan seguridad para salvaguardar sus intereses operativos y comerciales, y para cumplir con sus obligaciones para con sus clientes y el público.

Además, las organizaciones de telecomunicaciones deberían considerar los siguientes incidentes de seguridad ambiental y operativa.

1. Los servicios de telecomunicaciones dependen en gran medida de diversas instalaciones interconectadas, como enrutadores, conmutadores, servidores de nombres de dominio, sistemas de retransmisión de transmisión y un sistema de gestión de red (NMS). Por lo tanto, pueden ocurrir incidentes de seguridad de las telecomunicaciones en varios equipos/instalaciones y los incidentes pueden propagarse rápidamente a través de la red hacia otros equipos/instalaciones.
2. Además de las instalaciones de telecomunicaciones, las vulnerabilidades en los protocolos y la topología de la red pueden provocar graves incidentes de seguridad. En particular, la convergencia de redes cableadas e inalámbricas puede imponer desafíos importantes para el desarrollo de protocolos interoperables.

##### ISO/IEC 27011:2016 (ES)

1. Una de las principales preocupaciones de las organizaciones de telecomunicaciones es la posibilidad de que la seguridad se vea comprometida y provoque tiempos de inactividad en la red. Este tiempo de inactividad puede resultar extremadamente costoso en términos de relaciones con los clientes, pérdida de ingresos y costos de recuperación. Los ataques deliberados a la disponibilidad de la infraestructura nacional de telecomunicaciones pueden considerarse una preocupación de seguridad nacional.
2. Las redes y sistemas de gestión de telecomunicaciones son susceptibles a las intrusiones de piratas informáticos. Una motivación común para tales intrusiones es el robo de servicios de telecomunicaciones. Dicho robo se puede diseñar de varias maneras, como invocando funciones de diagnóstico, manipulando registros contables, alterando bases de datos de aprovisionamiento y escuchando las llamadas de los suscriptores.
3. Además de las intrusiones externas, a los operadores les preocupan los compromisos de seguridad de fuentes internas, como cambios no válidos en las bases de datos de administración de la red y configuraciones por parte de personal no autorizado. Estos sucesos pueden ser accidentales o deliberados.
4. Los servicios de telecomunicaciones pueden verse afectados por malware, como gusanos y virus, que atacan los sistemas finales o la infraestructura de comunicaciones. DoS/DDoS es una causa importante de incidentes en las comunicaciones y puede ser causado por varios métodos para interrumpir o bloquear señales de comunicación, o enviar datos a un sistema o red desde muchos cientos de sistemas al mismo tiempo para sobrecargarlo (ver TEL 13.1. 6).

Con el fin de proteger los activos de información en telecomunicaciones provenientes de diferentes fuentes en diversos entornos de telecomunicaciones, las pautas de seguridad para las telecomunicaciones son indispensables para respaldar la implementación de la gestión de seguridad de la información en las organizaciones de telecomunicaciones.

Las pautas de seguridad deben ser aplicables a lo siguiente:

1. organizaciones de telecomunicaciones que buscan confianza en que se cumplirán los requisitos de seguridad de la información de sus partes interesadas (por ejemplo, proveedores, clientes, reguladores);
2. organizaciones de telecomunicaciones que buscan una ventaja comercial mediante la implementación de un SGSI;
3. usuarios y proveedores de productos y servicios relacionados con la seguridad de la información para la industria de las telecomunicaciones;
4. esosmi internos o externos a la organización de telecomunicaciones que evalúan y auditan el SGSI para determinar su conformidad con los requisitos de ISO/IEC 27001;
5. aquellos internos o externosa las organizaciones de telecomunicaciones que brindan asesoramiento o capacitación sobre el SGSI apropiado para esa organización;
6. asegurando cumplimientoWisconsinth trans-requisitos legales y reglamentarios fronterizos, y el cumplimiento de las normas

Requisitos en todos los países de operación o tránsito.

##### Activos de información a proteger

Para establecer la gestión de la seguridad de la información, es esencial que una organización aclare e identifique todos los activos de la organización. La clarificación de los atributos y la importancia de los activos permite implementar controles adecuados.

Los activos de información que las organizaciones de telecomunicaciones deben proteger se pueden encontrar en la cláusula 8.1.1.

##### Establecimiento de la gestión de seguridad de la información.

* + - 1. **Cómo establecer requisitos de seguridad**

Es esencial que las organizaciones de telecomunicaciones identifiquen sus requisitos de seguridad. Hay tres fuentes principales de requisitos de seguridad que se detallan a continuación.

* + - * 1. Los derivados de la evaluación de riesgos paraun operador de telecomunicaciones, teniendo en cuenta su estrategia y objetivos comerciales generales. A través de la evaluación de riesgos, se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de que ocurran y se estima el impacto potencial.
        2. Los requisitos legales, estatutarios, regulatorios y contractuales que las organizaciones de telecomunicaciones deben satisfacer, el cumplimiento legal y regulatorio transfronterizo y el entorno sociocultural. Ejemplos de requisitos legislativos para organizaciones de telecomunicaciones son la no divulgación de comunicaciones (TEL.18.1.6 en el Anexo A) y la garantía de comunicaciones esenciales (TEL.18.1.7 en el Anexo A). Ejemplos de requisitos socioculturales son garantizar la integridad de las telecomunicaciones que se transmiten, retransmiten y reciben por cualquier medio, la disponibilidad de instalaciones de telecomunicaciones por cable o inalámbricas por parte de personas autorizadas y no dañar otras instalaciones de telecomunicaciones.
        3. El conjunto particular de principios, objetivos y requisitos comerciales para el procesamiento de información que un operador de telecomunicaciones ha desarrollado para respaldar sus operaciones.

##### ISO/IEC 27011:2016 (ES)

* + - 1. **Evaluación de riesgos de seguridad**

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debe equilibrarse con el daño empresarial que probablemente resulte de las fallas de seguridad. Los resultados de la evaluación de riesgos ayudarán a guiar y determinar las acciones y prioridades de gestión apropiadas para gestionar los riesgos de seguridad de la información y para implementar controles seleccionados para proteger contra estos riesgos.

La evaluación de riesgos debe repetirse periódicamente y al menos anualmente, para abordar cualquier cambio que pueda influir en los resultados de la evaluación de riesgos.

##### Seleccionar controles

Una vez que se han identificado los requisitos y riesgos de seguridad y se han tomado decisiones para el tratamiento de los riesgos, se deben seleccionar e implementar controles apropiados para garantizar que los riesgos se reduzcan a un nivel aceptable.

Esta recomendación | Norma Internacional proporciona orientación adicional y controles específicos de las telecomunicaciones, además de la gestión general de la seguridad de la información, teniendo en cuenta los requisitos específicos de las telecomunicaciones. Por lo tanto, se recomienda a las organizaciones de telecomunicaciones que seleccionen controles de esta Recomendación | Norma Internacional e implementarlas. Además, se pueden diseñar nuevos controles para satisfacer necesidades específicas según corresponda.

La selección de controles de seguridad depende de decisiones organizativas basadas en los criterios de aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque general de gestión de riesgos aplicado a las organizaciones de telecomunicaciones; Además, la selección debe estar sujeta a todas las leyes y regulaciones nacionales e internacionales pertinentes.

1. **Políticas de seguridad de la información**

Se aplican el objetivo de control y el contenido de la cláusula 5 de ISO/IEC 27002.

NOTA – Podría ser necesario tener en cuenta la legislación y los requisitos reglamentarios específicos de las telecomunicaciones y los requisitos asociados sobre cómo se cumplen y demuestran.

## Organización de la seguridad de la información.

* 1. **Organización interna**

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y operación de la información.

seguridad dentro de la organización.

##### Funciones y responsabilidades de seguridad de la información

**Control**

Todas las responsabilidades de seguridad de la información deben definirse y asignarse.

##### Guía de implementación

Se aplica la guía de implementación de ISO/IEC 27002 6.1.1.

##### Guía de implementación específica de telecomunicaciones

Debería nombrarse un director ejecutivo que sea responsable de todos los riesgos para la infraestructura de telecomunicaciones y rinda cuentas de su gestión.

Las organizaciones de telecomunicaciones deberían nombrar ingenieros de telecomunicaciones y otro personal, que tengan las credenciales adecuadas o conocimientos y habilidades apropiados, para que se encarguen de la supervisión de los asuntos relacionados con la instalación, mantenimiento y operación de las instalaciones de telecomunicaciones para el negocio de las telecomunicaciones. Se debe notificar a los ingenieros de telecomunicaciones y demás personal pertinentes y aceptar formalmente sus funciones y responsabilidades asignadas.

Cuando se utiliza criptografía, debe haber funciones específicas de criptocustodio y el personal que ocupe estos puestos debe estar debidamente capacitado en la gestión del material criptográfico y el uso y protección de los sistemas criptográficos.

##### Otra información

Se aplica el resto de la información de ISO/IEC 27002 6.1.1.