**GNC**

**Gestión de Nacimiento y Cría**



**PLAN DE AUDITORÍA**

**Integrantes:**

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

**Índice**

[Objetivos Generales 3](#_Toc529542070)

[Objetivos Específicos de la Auditoria 3](#_Toc529542071)

[Clasificación de la auditoria 3](#_Toc529542072)

[Alcance 3](#_Toc529542073)

[Metodología de la auditoria 3](#_Toc529542074)

[Recursos Físicos y tecnológicos 3](#_Toc529542075)

[Objetivos de control 4](#_Toc529542076)

[Elaboración de informe 4](#_Toc529542077)

[vulnerabilidad de un sistema informático 4](#_Toc529542078)

[Hackers 4](#_Toc529542079)

[CRACKER 5](#_Toc529542080)

[PHREAKER 5](#_Toc529542081)

[INSIDERS 5](#_Toc529542082)

[OUTSIDERS 5](#_Toc529542083)

[Metodología de ataque 5](#_Toc529542084)

[Identificación 5](#_Toc529542085)

[Exploración 5](#_Toc529542086)

[Enumeración 6](#_Toc529542087)

[Obteniendo acceso 6](#_Toc529542088)

[Siniestro 6](#_Toc529542089)

[Siniestro Informático 6](#_Toc529542090)

[Importancia del Siniestro Informático 7](#_Toc529542091)

[Auditoria Forense 7](#_Toc529542092)

[Metodología de la Auditoria Informática Forense 7](#_Toc529542093)

[Normas relativas al informe de la Auditoria Informática 9](#_Toc529542094)

[UNIT-ISO/IEC 27000 9](#_Toc529542095)

[ISO 27001 11](#_Toc529542096)

[ISO 27002 12](#_Toc529542097)

[ISO 27003 14](#_Toc529542098)

[ISO 27004 14](#_Toc529542099)

[ISO 27005 16](#_Toc529542100)

[ISO 27006 17](#_Toc529542101)

[ISO 27007 18](#_Toc529542102)

[ISO 27008 18](#_Toc529542103)

[ISO 27010 19](#_Toc529542104)

[ISO 27011 19](#_Toc529542105)

## Objetivos Generales

Realizar la auditoría a la red de datos que soportan los sistemas de información en la organización GNC.

## Objetivos Específicos de la Auditoria

Objetivos Específicos de la Auditoria

* Identificar el estado actual de la seguridad de parte lógica y física de la red de datos, en la organización GNC para verificar la existencia de las vulnerabilidades y amenazas existentes en los activos informáticos y de información.
* Elaborar un informe de los resultados obtenidos en la Auditoria que contenga los hallazgos

## Clasificación de la auditoria

Auditoria interna: La auditoría será llevada a cabo por personal de la empresa.

La auditoría será sobre la seguridad Informática, Comunicaciones y Redes.

## Alcance

* Aplicación de instrumentos de recolección de la información
* Realización de un Análisis y Gestión de riesgos informáticos.

Para la aplicación de instrumentos de recolección de la información se tendrá en cuenta:

-Diseño y aplicación de cuestionarios.

-Diseño y aplicación de listas de chequeo

Para la realización del análisis y gestión de riesgos de los hallazgos se tendrá en cuenta:

-Análisis de riesgos de acuerdo a las vulnerabilidades encontradas

-Gestión de riesgos

## Metodología de la auditoria

Fase de recolección de información

Se revisará la documentación competente a todos los dispositivos utilizados en la red, así como los planos de la red. Además, también se deberá revisar la documentación respecto a la implementación de la red.

Fase de planeación

Posterior a recoger esa información se deberá identificar y seleccionar los métodos y procesos adecuados.

Fase de ejecución

Se aplicarán los métodos y procesos seleccionados, así como se realizará un análisis y gestión de riesgos sobre los hallazgos y vulnerabilidades encontrados con los métodos e instrumentos seleccionados.

Fase de auditoria o fase de resultados

Se examinará y recopilará la información, los resultados obtenidos en las pruebas y en la auditoria. Posteriormente se elaborará un informe el cual será presentado a la directiva de la Organización GNC.

## Recursos Físicos y tecnológicos

Para recursos relacionados con hardware, se utilizará:

•2 computadores portátiles.

•Dispositivos de almacenamiento.

•Papelería

Para recursos de software:

Software Libre para realizar pruebas de penetración y Ética Hacking, en este caso Kali Linux, el cual cuenta con:

-Herramientas para recolección de información.

-Herramientas para análisis de vulnerabilidades.

-Herramientas de explotación.

## Objetivos de control

Para la seguridad física:

•Control de áreas para los equipos de redes y comunicaciones, previniendo accesos inadecuados.

•Controles de utilización de los equipos de red y de comunicaciones, previniendo accesos inadecuados.

•Controles para la protección y tendido adecuado de cables y líneas de comunicaciones

Para la seguridad lógica

•Controles de contraseñas para limitar y detectar cualquier intento de acceso no autorizado a la red.

•Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

•Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.

•Controles de Seguridad en la Red.

## Elaboración de informe

Se le presentará un borrador de informe a los altos cargos de la empresa, con el máximo de detalle posible de todos los problemas y soluciones posibles recomendadas, este informe se pasará por correo electrónico.

Posteriormente se elaborará el informe en donde se muestren los resultados a los responsables de la empresa, el informe presentado dará a conocer todos los puntos evaluados durante la auditoria. La conclusión tendrá como temas los resultados, errores, puntos críticos y observaciones de los auditores. Mientras que en el resumen se verán las posibles soluciones de esos puntos críticos y fallas, así como recomendaciones para el buen uso y también recomendaciones sobre la forma incorrecta de realizar algunos procedimientos.

Finalmente se presentará el informe a la directiva de la empresa.

### vulnerabilidad de un sistema informático

Es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseada, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.

### Hackers

La palabra hacker aplicada en la computación se refiere a las personas que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

### CRACKER

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

### PHREAKER

El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

### INSIDERS

Es la intrusión en las redes de las empresas proviene de ataques internos. Es decir, los mismos empleados hackean a su propia organización.

### OUTSIDERS

El outsider es la persona que conoce muy bien la instalación de una organización, pero no pertenece a ella. Son aquellos que ingresan a la red simplemente averiguando una contraseña autorizada.

El aprovechamiento ilícito de las vulnerabilidades da lugar al delito informático que pueden originar en muchos casos siniestros informáticos.

Los hackers, crackers, preakers, insiders, outsiders pueden cometer delitos comunes que atentan contra la seguridad informática de una organización o empresa,

### Metodología de ataque

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

El objetivo de la metodología de ataque es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (estos ataques a la confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde dónde), es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo.

### Identificación

#### Networks Scanners

Hacen un mapa de la red identificando: dominios, servidores, sistemas operativos.

Recogiendo información sin atacar y descubriendo: los servidores activos, servidores de correo, nombres de empleados, rango de direcciones IP.

### Exploración

#### Ports Scanners.

Scanean las máquinas para detectar puertos abiertos, a fin de identificar posibles exposiciones o vulnerabilidades a explotar.

Sistemas activos, servicios a la escucha, sistemas operativos

### Enumeración

Obtención de usuarios válidos o recursos compartidos mal protegidos

### Obteniendo acceso

#### Contraseñas Crakers

Se usan para detectar la confinación de usuarios y contraseñas válidos. Obteniendo la contraseña para los usuarios/servicios

#### Escalando privilegios

Obteniendo el Super Usuario, que es el usuario administrador, que permite realizar todas las operaciones posibles en el sitio y/o la red.

#### Robando accesos

Buscando otros accesos válidos o rutas que permitan obtener información de la organización.

#### Cubriendo las huellas

Buscando logs y borrando todas las pistas de Auditoría, de manera tal que salgan sin dejar rastro.

#### Creando entradas traseras

Crear cuentas de usuario, buscando los archivos deseados.

Los métodos de ataque descritos, están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una contraseña, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derecho de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

### Siniestro

***“El siniestro es un hecho violento, súbito, externo y ajeno a la intencionalidad del asegurado, cuyas consecuencias pueden estar cubiertas por alguna garantía del seguro. Constituye un solo y único accidente el conjunto de daños derivados de un mismo hecho.”***

### Siniestro Informático

“El siniestro informático implica actividades como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.”

### Importancia del Siniestro Informático

En el área informática se pueden producir ataques, y esos ataques van contra la información la que puede sufrir distintos tipos de intromisión para agredirla en su confidencialidad, disponibilidad e integridad.

Cuando el siniestro informático es descubierto por un empleado, debe asegurarse que hay la máxima información disponible este intacta, clara y que sea la correcta para que el auditor forense informático pueda realizar su trabajo correctamente.

Actualmente en las organizaciones, es importante que haya un auditor forense para evitar los siniestros informáticos y así evitar la destrucción, robo o alteraciones de información valiosa para el desarrollo económico y profesional de la empresa.

### Auditoria Forense

#### Objetivo de la Auditoria Forense

La Auditoria Forense proporciona recomendaciones para asegurar la salvaguarda de los activos de los sistemas de información, manteniendo la integridad de los datos y lograr los objetivos de la organización en forma eficiente y eficaz.

#### Auditoria Informática Forense

La Auditoria Informática Forense puede definirse, como la ciencia que se encarga de analizar sistemas informáticos en busca de evidencia que colabore a llevar adelante una causa judicial o una negociación extrajudicial.

Es la aplicación de técnicas y herramientas de hardware y software para determinar datos potenciales o relevantes. También puede servir para informar adecuadamente al cliente acerca de las posibilidades reales de la evidencia existente o supuesta.

### Metodología de la Auditoria Informática Forense

El auditor forense para poder iniciar su trabajo, determinando los hallazgos de irregularidades, fraude y corrupción en las empresas del sector comercial, debe de establecer una metodología que este, acorde con las irregularidades encontradas.

#### Evidencia

En la Auditoria Forense, todo ataque deja evidencia que permite identificar lo ocurrido, lo mismo ocurre con la evidencia computacional.

La evidencia computacional es única, cuando se la compara con otras formas de “evidencia documental”. A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto, es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistido por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías.

La IOCE (International Organization On Computer Evidence), define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.

2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.

3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.

4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.

5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además, definen que los principios desarrollados para la recuperación estandarizada de evidencia computarizada se deben gobernar por los siguientes atributos:

1. Consistencia con todos los sistemas legales.

2. Permitir el uso de un lenguaje común.

3. Durabilidad.

4. Capacidad de cruzar límites internacionales.

5. Capacidad de ofrecer confianza en la integridad de la evidencia.

6. Aplicabilidad a toda la evidencia forense.

#### Evidencia digital

Es un tipo de evidencia física. Está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

Evidencia Digital: Información de valor para el caso que es transmitida o guardada en formato digital.

* Evidencia digital original
* Evidencia digital duplicada

Objetos de datos: Información valiosa relacionada con el caso asociada a objetos físicos. Debemos procurar trabajar sobre imágenes de discos, esto es así para no trabajar a nivel de sistema de ficheros, pues podemos perder información valiosa.

Objetos físicos: Soporte físico sobre el que se guarda la información digital.

Ejemplos de evidencia digital:

* Email
* Images
* Chat rooms
* File contents
* System logs
* Network packets

#### Características del informe

El texto del informe sobre una investigación de auditoria forense debe reunir las siguientes características:

Debe presentarse por escrito. En él debe estar claramente:

* La descripción de los hechos, objeto del peritazgo y deben distinguirse de los pronósticos o conjeturas
* Las operaciones técnicas realizadas.
* Los principios científicos en que se fundamenta.
* Las conclusiones debidamente comprobadas y sustentadas que servirán al juez para valorar la prueba.

Si ciertos hechos parecen contradictorios, deben ser ampliamente discutidos. Un conjunto de hechos debe compararse con otro para llegar a una conclusión, y deben especificarse cuidadosamente las razones que se tengan para ignorar las implicaciones de cualquier hecho.

El informe debe excluir toda referencia a aquellas características de las cuentas que se presten a controversia, a menos que tengan relación con las conclusiones del informe.

### Normas relativas al informe de la Auditoria Informática

Contener observaciones o hallazgos, identificando causas y efectos de los mismos, conclusiones y recomendaciones correspondientes, con señalamiento expreso de que el trabajo ha sido realizado conforme a las Normas Generales de Auditoria.

Ser firmado por el nivel directivo o gerencial, competente para notificar los resultados.

Redactarse de manera objetiva, persuasiva y constructiva y en forma clara, precisa y concreta, insertarse los detalles necesarios que contribuyan a evitar equívocos y ambigüedades.

El informe debe ser presentado oportunamente, a objeto de que la información en él contenida tenga actualidad, utilidad y valor para que las autoridades a quienes corresponda, adopten las medidas inmediatas tendentes a corregir las deficiencias señaladas

En conclusión, las normas internas de auditoria, exigen que el trabajo realizado de auditoria, se establezcan normas mínimas para la ejecución del trabajo, ayuda a emitir una opinión razonable sobre el dictamen de dicho trabajo, evaluando el cumplimiento, leyes, reglamentos, y demás normativas aplicables a la organización a la cual se ha ejecutado una auditoria.

## UNIT-ISO/IEC 27000

#### Introducción / Presentación

La información es un activo que, como otros activos importantes del negocio, es esencial al negocio de una organización y requiere en consecuencia una protección adecuada. Esto es especialmente importante en ambientes de negocio cada vez más interconectados. Como consecuencia de esta creciente interconexión, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades.

#### Historia / Antecedentes

En 1995 el organismo británico de normalización (BSI - British Standards Institute) establece la norma BS 7799, con el objetivo de proporcionar a cualquier organización un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) fue una guía de buenas prácticas, para la que no se establecía un esquema de certificación. En 1998 fue publicada la segunda parte de la norma (BS 7799-2), en la que establecieron los requisitos de un sistema de seguridad de la información para ser certificable por una entidad independiente.

En el año 1999 las dos partes de la Norma BS 7799 se revisaron y la primera parte se adoptó por ISO e IEC, sin cambios sustanciales, como ISO/IEC 17799 en el año 2000.

En 2002, se revisó la segunda parte de la norma (BS 7799-2) para adecuarse a la filosofía de normas ISO/IEC de sistemas de gestión.

En el año 2005 la Norma BS 7799-2 se publicó por ISO e IEC, con algunos cambios, como norma ISO/IEC 27001.



#### Normalización internacional

Las normas internacionales para los sistemas de gestión proporcionan un modelo a seguir en la creación y operación de un sistema de gestión. Este modelo incorpora los elementos sobre los que expertos en la materia han llegado a un consenso internacional como estado del arte. El sub-comité ISO/IEC JTC 1 SC 27 reúne a los expertos dedicado a la elaboración de normas internacionales de sistemas de gestión para la seguridad de la información

UNIT es miembro pleno del Sub Comité 27 (ISO/IEC JTC1/SC 27) Técnicas de Seguridad, que cuenta con 136 Normas publicadas.

A nivel regional UNIT forma parte de del Comité CSM 28 “Comité Sectorial Mercosur de Seguridad de la Información” de la Asociación Mercosur de Normalización AMN.

#### ¿qué son las normas UNIT-ISO/IEC 27000?

La gestión eficaz de la seguridad de la información es un aspecto primordial para salvaguardar a las organizaciones de los riesgos que pueden dañar de forma importante sus sistemas de información.

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) han desarrollado una serie de normas internacionales de amplísima difusión a nivel mundial al respecto de esta problemática.

Quizás la de mayor trascendencia sea la ISO/IEC 27002 -en nuestro país adoptada como UNIT-ISO/IEC 27002-, Código de buenas prácticas para un Sistema de Gestión de la Seguridad de la Información(SGSI), la cual como lo indica en su título ofrece recomendaciones para la gestión de un SGSI. La norma está organizada en 14 dominios, los cuales contiene un total de 144 controles que abarcan desde los aspectos estratégicos de un SGSI hasta los más operativos.



Esta norma es en definitiva una herramienta muy útil para quienes sean los responsables de iniciar, implantar o mantener la seguridad de una organización. La ISO/IEC 27002 no es una norma de certificación, ni fue diseñada para ese propósito. La misma es seguida por la norma ISO/IEC 27001 (en nuestro país adoptada como UNIT-ISO 27001), Sistema de Gestión de la Seguridad de la Información-Requisitos publicada el 14 de octubre de 2005, la cual puede utilizarse para la certificación. Esta última implica declaraciones de conformidad con procesos y controles de seguridad.

Alrededor de 2000 organizaciones ya tienen su certificación para sus SGSI, y se espera que este número crezca.

UNIT, como representante exclusivo de ISO en Uruguay es el responsable de la Normalización Técnica en esta materia y también quién está promocionando en nuestro país la Capacitación en Gestión de Seguridad de la Información y la Certificación de los correspondientes Sistemas (UNIT-ISO/IEC 27001).

#### Familia de normas UNIT-ISO/IEC 27000

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información de manera similar a lo acontecido con las normas de gestión de la calidad, la serie ISO 9000.

|  |  |
| --- | --- |
| Identificación | Título |
| UNIT-ISO/IEC 27000:2014 | Visión General y Vocabulario |
| UNIT-ISO/IEC 27001:2013 | Sistemas de Gestión de la Seguridad de la Información - Requisitos |
| UNIT-ISO/IEC 27002:2013 | Código de buenas Prácticas para la Gestión de Seguridad de la Información |
| UNIT-ISO/IEC 27003:2010 | Directrices para la Implementación de un Sistema de Gestión de Seguridad de la Información. |
| UNIT-ISO/IEC 27004:2009 | Gestión de la Seguridad de la Información. Medición |
| UNIT-ISO/IEC 27005:2011 | Gestión del Riesgo de Seguridad de la Información |
| ISO/IEC 27006:2011 | Requisitos para los Organismos que Realizan Auditorías y Certificaciones de Sistemas de Gestión de Seguridad de la Información |
| UNIT-ISO/IEC 27007:2011 | Directrices para Auditar Sistemas de Gestión de Seguridad de la Información |
| UNIT-ISO/IEC 27008:2011 | Directrices para los Auditores sobre Controles de Seguridad de la Información |

### ****ISO 27001****

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

**Sección 0 – Introducción** – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

**Sección 1 – Alcance** – explica que esta norma es aplicable a cualquier tipo de organización.

**Sección 2 – Referencias normativas** – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

**Sección 3 – Términos y definiciones** – de nuevo, hace referencia a la norma ISO/IEC 27000.

**Sección 4 – Contexto de la organización** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

**Sección 5 – Liderazgo** – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

**Sección 6 – Planificación** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

**Sección 7 – Apoyo** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

**Sección 8 – Funcionamiento** – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

**Sección 9 – Evaluación del desempeño** – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

**Sección 10 – Mejora** – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

**Annexo A** – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

#### ****Otras normas relacionadas con seguridad de la información****

**ISO/IEC 27002** proporciona directrices para la implementación de los controles indicados en ISO 27001. ISO 27001 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1.

**ISO/IEC 27004** proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO 27001 ya que explica cómo determinar si el SGSI ha alcanzado los objetivos.

**ISO/IEC 27005** proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO 27001 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación.  ISO 27005 ha surgido de la norma británica BS 7799-3.

### ISO 27002

La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de la norma ISO 27002:2013.

La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad.

La norma ISO 27002 se encuentra enfocada a todo tipo de empresas, independientemente del tamaño, tipo o naturaleza.

La norma ISO 27002 se encuentra estructurada en 14 capítulos que describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone. El documento recomienda un total de 114 controles, si bien no hace falta cumplirlos todos, sí que hay que tenerlos en cuenta y considerar su posible aplicación, además del grado de la misma.

Queremos realizar una revisión muy breve de cada uno de los 14 capítulos.

#### 1 Políticas de Seguridad de la Información

Dentro de este capítulo se hace hincapié en la importancia que ocupa la disposición de una adecuada política de seguridad, aprobada por la dirección, comunicada a todo el personal, revisada de forma periódica y actualizada con los cambios que se producen en el interior y en el exterior.

#### 2 Organización de la Seguridad de la Información

Los controles indicados en este capítulo buscan estructurar un marco de seguridad eficiente tanto mediante los roles, tareas, seguridad, etc. como en los dispositivos móviles.

Tenemos que tener presente que cada vez es mayor el peso que está ocupando el teletrabajo dentro de las empresas, y por ello, se deben tener en cuenta todas sus características especiales para que ningún momento la seguridad de la información de la que se dispone se vea afectada.

#### 3 Seguridad relativa a los recursos humanos

Si analizamos los incidentes de seguridad que se producen en una organización nos daremos cuenta de que la gran mayoría de estos tienen su origen en un error humano. Se debe concienciar y formar al personal de los términos de empleo de la información en el desarrollo de sus actividades y la importancia que tiene la información en el desarrollo de sus actividades, además de la importancia que tiene promover, mantener y mejorar el nivel de seguridad adecuándolo a las características de los datos y la información que maneja es clave y uno de los objetivos que se debe perseguir.

#### 4 Gestión de activos

Se centra en la atención en la información como activo y en cómo se deben establecer las medidas adecuadas para guardarlos de las incidencias, quiebras en la seguridad y en la alteración no deseada.

#### 5 Control de acceso

Controlar quien accede a la información dentro de un aspecto relevante. Al fin y al cabo, no todas las personas de una organización necesitan acceder para realizar su actividad diarias a todos los datos, sino que tendremos roles que necesitan un mayor acceso y otros con un acceso mucho más limitado. Para poder marcar las diferencias, se deben establecer todos los controles como registro de los usuarios, gestión de los privilegios de acceso, etc. siendo algunos de los controles que se incluyen en este apartado.

#### 6 Criptografía

En el caso de que estemos tratando la información sensible o crítica puede ser interesante utilizar diferentes técnicas criptográficas para proteger y garantizar su autenticidad, confidencialidad e integridad.

#### 7 Seguridad física y del entorno

La seguridad no es solo a nivel tecnológico sino también físico, es decir, una simple labor de no dejar las pantallas e impresoras en zonas que sean fácilmente accesibles, por parte del personal externo los documentos con los que se están trabajando no sólo nos permitirán gestionar de forma adecuada la seguridad, sino que se acabarán convirtiendo en hábitos que nos aportan eficiencia en la gestión.

#### 8 Seguridad de las operaciones

Tiene un marcado componente técnico entrado en todos los **aspectos disponibles como la protección**del software malicioso, copias de seguridad, control de software en explotación, gestión de vulnerabilidad, etc.

#### 9 Seguridad de las comunicaciones

Partiendo de la base de que la gran mayoría de los intercambios de información y de datos en distintas escalas **se llevan a cabo mediante las redes sociales**, garantizar la seguridad y proteger de forma adecuada los medios de transmisión de estos datos clave.

#### 10 Adquisiciones, desarrollo y mantenimiento de los sistemas de información

La seguridad no es un aspecto de un área en concreto, ni de un determinado proceso, no que es general, **abarca toda la organización** y tiene que estar presente como elemento transversal clave dentro del ciclo de vida del sistema de gestión.

#### 11 Relación de proveedores

Cuando se establecen las relaciones con terceras partes, como puede ser proveedores, se deben **establecer medidas de seguridad** pudiendo ser muy recomendable e incluso necesario en determinados casos.

#### 12 Gestión de incidentes de seguridad de la información

No podemos hablar de **controles de seguridad** sin mencionar un elemento clave, los incidentes en seguridad. Y es que, estar preparados para cuando estos incidentes ocurran, dando **una respuesta rápida y eficiente** siendo la calve para prevenirlos en el futuro.

#### 13 Aspectos de seguridad de la información para la gestión de la continuidad de negocio

No sabemos lo que necesitábamos un dato hasta que lo hemos perdido. Sufrir una pérdida de **información relevante y no poder recuperarla** de laguna forma puede poner en peligro la continuidad de negocio de la organización.

#### 14 Cumplimiento

No podemos hablar de seguridad de la información, sin hablar de legislación, normas y políticas aplicables que **se encuentre relacionadas con este campo** y con las que conviven en las organizaciones. Debemos tener presente que ocupan un enorme lugar en cualquier sistema de gestión y deben **garantizar que se cumple** y que están actualizados con los últimos cambios siendo esencial para no llevarnos sorpresas desagradables.

### ISO 27003

Es un estándar internacional que constituye una guía para la implantación de un SGSI.

Se trata de una norma adaptada tanto para los que quieren lanzarse a implantar un SGSI como para los consultores en su trabajo diario, debido a que resuelve ciertas cuestiones que venían careciendo de un criterio normalizado.

Focaliza su atención en los aspectos requeridos para un diseño exitoso y una buena implementación del Sistema de Gestión de Seguridad de la Información – SGSI – según el estándar ISO 27001.

Contiene una descripción del proceso de delimitación del SGSI, y además el diseño y ejecución de distintos planes de implementación.

Especifica el proceso de conseguir una aprobación para la implementación de un SGSI, define el proyecto para dicho acometido, el cual es llamado en la norma**ISO 27003** proyecto de SGSI, y da instrucciones sobre cómo abordar la planificación de la gestión para implementar el SGSI.

La norma tiene el siguiente contenido:

* Alcance.
* Referencias Normativas.
* Términos y Definiciones.
* Estructura de esta Norma.
* Obtención de la aprobación de la alta dirección para iniciar un SGSI.
* Definición del alcance del SGSI, límites y políticas.
* Evaluación de requerimientos de seguridad de la información.
* Evaluación de Riesgos y Plan de tratamiento de riesgos.
* Diseño del SGSI.
* Anexo A: lista de chequeo para la implementación de un SGSI.
* Anexo B: Roles y responsabilidades en seguridad de la información
* Anexo C: Información sobre auditorías internas.
* Anexo D: Estructura de las políticas de seguridad.
* Anexo E: Monitoreo y seguimiento del SGSI.



### ISO 27004

Facilita una serie de mejores prácticas para poder medir el resultado de un SGSI basado en ISO 27001.

El estándar concreto cómo configurar el programa de medición, qué parámetros medir, cuñando y cómo medirlos, y ayuda a las empresas a crear objetivos de rendimiento y criterios de éxito.

La medición de la seguridad aporta protección a los sistemas de la organización y da respuesta a las amenazas de la misma.

Expone que el tipo de medidas requeridas dependerá del tamaño y complejidad de la organización, de la relación coste beneficio y del nivel de integración de la seguridad de la información en los procesos de la propia organización.

La norma ISO27004 establece cómo se deben constituir estas medidas y cómo se deben documentar e integrar los datos obtenidos en el SGSI.

Las etapas propuestas por **ISO 27004** con el objetivo de medir la eficacia de la seguridad de la información son:

* Selección procesos y objetos de medición.

Las empresas deben definir lo que hay que medir y el alcance de la medida. Sólo se consideran en la medición los procesos bien documentados que son consistentes y repetibles. Objetos de medición puede ser el rendimiento de los controles o de procedimientos, el comportamiento del personal.

* Definición de las líneas base.

Los valores base que muestran el punto de referencia deben definirse para cada objeto que se está midiendo.

* Recopilación de datos.

Los datos deben ser dimensionales precisos y oportunos. Se pueden emplear técnicas automatizadas de recogida de datos para lograr una recolección estandarizada y presentar informes.

* Desarrollo de un método de medición.

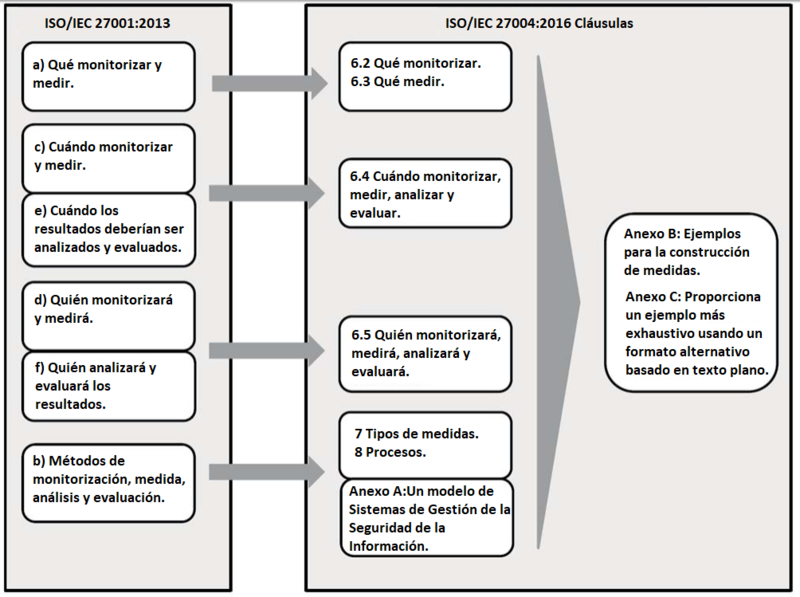
Según**ISO 27004**, la secuencia lógica de operaciones se aplica en diversos atributos del objeto seleccionado para la medición. Se usan indicadores como fuentes de datos para mejorar el rendimiento de los programas de seguridad de la información.

* Interpretación de los valores medidos.

Mediante procesos y la tecnología para el análisis y la interpretación de los valores se deben identificar las brechas entre el valor inicial y el valor de medición real.

* Comunicación de los valores de medición.

Los resultados de medición del SGSI se comunicarán a las partes interesadas. Se puede hacer en forma de gráficos, cuadros de mando operacionales, informes o boletines de noticias.



### ISO 27005

La norma ISO 27005 contiene **diferentes recomendaciones y directrices** generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.

Es compatible con los conceptos generales especificados en la norma ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo.

La **norma ISO 27005 reemplaza a la norma ISO 13335-2** “Gestión de Seguridad de la Información y la tecnología de las comunicaciones”.

El riesgo se define como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daños. **El riesgo se encuentra relacionado con el uso**, propiedad, operación, distribución y la adopción de las tecnologías de la información de la empresa. Aunque no existe un método concreto de cómo gestionar riesgos, se recomienda utilizar un proceso estructurado, **sistemático y riguroso de análisis de riesgos** para la creación del plan de tratamiento de riesgos.

Los **indicadores de riesgo muestran si la empresa se encuentra sujeta** o tiene alta probabilidad de ser sometida a un riesgo que excede el riesgo permitido.

La gestión del riesgo es una actividad recurrente que se refiere al análisis, a la planificación, la ejecución, el **control y el seguimiento de todas las medidas implantadas** y la política de seguridad que ha sido impuesta.

La actualización del establecimiento, mantenimiento y mejora continua de un SGSI ofrecen una clara indicación de que **una organización está utilizando un enfoque sistemático** para la identificación, evaluación y gestión de riesgos de seguridad de la información.

#### Identificación de riegos

Un evento solo es un riesgo si existe un grado de incertidumbre. El valor de un activo puede **cambiar su valor durante la ejecución de un proyecto**, por experiencia esto es cierto, pero ¿Cuánto puede cambiar? No lo sabemos. Por lo tanto, es un riesgo que debemos evitar en un proyecto pequeño. Debemos estar seguros de identificar el riesgo en realidad y no sus causas o efectos.

#### Evaluación de los riesgos

Es necesario **establecer un vínculo entre los escenarios de riesgos IT** y el impacto empresarial que estaos generarían, para así comprender el efecto de los **eventos adversos** que se pueden desencadenar.

La evaluación de riesgos se ejecuta en los puntos discretos de tiempo y hasta que el rendimiento de la **próxima evaluación proporciona una visión temporal** de los riesgos evaluados.  
La evaluación de riesgos se realiza a menudo en más de una interación, la primera es una evaluación de **alto nivel para identificar los riesgos altos**, mientras que las interacciones posteriores detallan el análisis de los riesgos principales y tolerables. Varios factores ayudan a **seleccionar eventos con cierto grado de riesgo**:

* Probabilidad
* Consecuencias
* Ocurrencia
* Urgencia
* Maleabilidad
* Dependencia
* Proximidad

La evaluación de riesgos **requiere de los siguientes puntos**:

* Un **estudio de la vulnerabilidad**, amenazas, probabilidad, pérdidas y la eficacia de las medidas de seguridad. Los directivos de la empresa utilizan los resultados de la evaluación del riesgo para desarrollar los requisitos de seguridad y sus especificaciones.
* El **proceso de evaluación de amenazas y vulnerabilidades**, para estimar el efecto producido en caso de pérdidas y establecer el grado de aceptación y aplicabilidad de las operaciones del negocio.
* **Identificar los activos y las facilidades** que pueden ser afectadas por las amenazas y vulnerabilidades.
* **Análisis de los activos del sistema** y las vulnerabilidades para establecer un estimado de pérdida esperada en caso de que ocurra ciertos eventos y la probabilidad estimada cuando ocurra. El propósito de una evaluación del riesgo es determinar si las contramedidas son adecuadas para reducir la probabilidad de la pérdida o impacto de la pérdida dentro del nivel aceptable.

Es una **herramienta de gestión**que proporciona un enfoque sistemático que determine el valor relativo a: la sensibilidad al instalar activos informáticos, la evaluación de vulnerabilidades, la evaluación de la expectativa de pérdidas, la percepción de los niveles de exposición al riesgo, la evaluación de las características de protección existentes, las alternativas adicionales de protección, la aceptación de riesgos y la documentación de las decisiones de gestión.

### ISO 27006

Tiene como título oficial “Tecnología de la información -. Técnicas de seguridad Requisitos para los organismos que realizan la auditoría y certificación de sistemas de información de gestión de la seguridad”, se compone de 10 capítulos y 4 anexos.

El estándar**ISO 27006** responde a una guía para los organismos de certificación en los procesos formales que hay que seguir al auditar SGSI. Los procedimientos descritos en dicha norma dan la garantía de que el certificado emitido de acuerdo a ISO 27001 es válido.

**ISO-27006** está pensada para apoyar la acreditación de organismos de certificación que ofrecen la certificación del Sistema de Gestión de Seguridad de la Información. Se encarga de especificar los requisitos y suministrar una guía para la auditoría y la certificación del sistema.

Cualquier organización certificada en ISO27001 debe cumplir también con los requisitos de la norma **ISO27006**.

El proceso de certificación consiste en auditar el SGSI para el cumplimiento de ISO 27001. Los auditores de certificación solo tienen interés pasajero en los controles reales de seguridad de información que están siendo administrados por el sistema de gestión. Se supone que cualquier empresa con una queja del SGSI es, ha de gestionar sus riesgos de seguridad de información con diligencia.

Esta norma se publicó en 2007 y se revisó en 2011.

La próxima versión es probable que sea diferente debido a los cambios relevantes en las normas en las que se basa.

Los requisitos generales a los que hace referencia son:

* Orientación específica del SGSI en relación con la imparcialidad.
* Listado del trabajo que pudiera estar en conflicto.
* Inclusión de una lista de todas las actividades que se pueden realizar fuera.

### ISO 27007

Forma parte de la familia de normas del Sistema de Gestión de Seguridad de la Información – SGSI –.

La norma suministra una guía para las entidades acreditadas de certificación para auditar SGSI.

**ISO-27007** refleja en gran parte a la norma ISO 19001 (estándar de auditoría para sistemas de gestión de la calidad y medioambiental). Se encarga de aportar orientación adicional al SGSI.

Por otro lado, también se basa en **ISO 17021**, Evaluación de la conformidad.

El estándar acoge:

* La gestión del programa de auditoría del SGSI: establecer qué, cuándo y cómo se debe auditar, asignar auditores apropiados, gestionar los riesgos de auditoría, mantenimiento de los registros de la misma, mejora continua del proceso…
* Ejecución de la auditoría relativa al SGSI, ésta incluye el proceso de auditoría, la planificación, la realización de actividades clave, trabajo de campo, análisis, presentación de informes y seguimiento.
* Gestión de los auditores del SGSI: competencias, atributos, habilidades, evaluación…

Esta guía tiene los siguientes fines:

* Confirmar que los controles de seguridad de la información mitigan de forma correcta los riesgos de la organización.
* Verificar que los controles de seguridad en relación con la contabilidad general o de los sistemas y procesos de contratación son correctas para que los auditores corroboren los datos.
* Ratificar que las obligaciones contractuales de los proveedores son satisfactorias en relación a la seguridad de la información.
* Revisar por la dirección, sin olvidar las operaciones rutinarias que forman parte del SGSI de una organización, para asegurarnos que todo está en orden.
* Auditar tras incidentes de seguridad de la información como parte del análisis y generar acciones correctivas.

### ISO 27008

Es un estándar que suministra orientación acerca de la implementación y operación de los controles, es aplicable a cualquier tipo y tamaño de empresa, tanto pública como privada que lleve a cabo revisiones relativas a la seguridad de la información y los controles de seguridad de la información.

Es compatible con otras normas como ISO 27001 o ISO 27002, y sirve como plataforma estratégica para garantizar la seguridad de la información.

**ISO 27008** soporta tanto la planificación como la ejecución del SGSI y el proceso de gestión del riesgo del sistema de la organización.

Por otro lado, supone un valor añadido y una mejora de la calidad de las normas de la serie ISO 27000.

Mejora las auditorias del SGSI a través de la optimización de la relación entre los procesos del Sistema de Gestión de Seguridad de la Información y los controles necesarios para los mismos. Además, garantiza un uso eficiente y efectivo de los recursos de la auditoría.

Mientras que ISO 27007 se focaliza en la auditoría de todos los elementos del SGSI, según lo describe ISO 27001,**ISO-27008** se dirige a la comprobación de los controles de seguridad de la información.

La norma incluye la comprobación de la conformidad técnica frente a un estándar de implementación de seguridad de la información establecido en la empresa. No busca suministrar orientaciones específicas sobre la verificación del cumplimiento relativo a la medición, evaluación del riesgo o auditoría del SGSI.

Los controles técnicos de los que hablamos no se definen explícitamente en la norma, son los conocidos como controles de seguridad de TI, que no son sino un subconjunto de los controles de seguridad de la información descritos en la norma ISO 27001 e ISO 27002.

Estos controles que trae **ISO 27008** ayudarán a la organización a:

* Comprender el alcance de los problemas o deficiencias en la aplicación y puesta en marcha de los controles de seguridad de la información, normas de seguridad de la información y controles de la información técnica.
* Identificar los posibles impactos en la empresa de las amenazas y vulnerabilidades de seguridad de la información.
* Planificar actividades de mitigación de riesgos de seguridad de la información.
* Confirmar que las deficiencias de seguridad de información emergentes se han abordado de forma adecuad.

### ISO 27010

**ISO 27010** suministra orientación relacionada con el intercambio de información relativa a los riesgos de seguridad de la información, controles, problemas e incidencias que puedan ocurrir en las organizaciones.

Más concretamente **ISO-27010** aporta orientación sobre del funcionamiento interno de la empresa, seguridad y comunicación entre el propio sector, entre sectores y con los gobiernos. Con esto se consigue proteger la infraestructura crítica, reconocer las circunstancias normales para satisfacer los requisitos jurídicos, reglamentarios y otras obligaciones contractuales.

Puede ser necesario compartir información confidencial de amenazas sobre la seguridad de la información, vulnerabilidades e incidentes de una organización.

Un ejemplo puede ser la colaboración de empresas privadas, gobiernos, policía… en una misma investigación, evaluación y/o resolución de conflictos internacionales.

La información es algo muy valioso y sensible, suele estar restringida a determinados individuos dentro de una organización. Por esto la fuente informativa ha de estar amparada y permanecer en el anonimato.

Los intercambios de información se dan en ambientes estresantes, sometidos a presiones intensas, conduciendo a la probabilidad de que aparezcan problemas sobre los controles de seguridad de la información. **ISO27010** ayudar a que esto no ocurra, estableciendo reglas comunes para la seguridad.

El estándar **ISO 27010** aporta una guía sobre los métodos, modelos, procesos, controles y demás mecanismos para realizar el intercambio de información de una manera segura, garantizando la confianza y el entendimiento, respetando los principios de seguridad de la información.

### ISO 27011

**ISO 27011** aborda las directrices de gestión de seguridad para las organizaciones de telecomunicaciones basadas en la norma ISO 27002.

La norma facilita modernos controles, además de una orientación para la implementación en las empresas de telecomunicaciones. Consolida la privacidad, disponibilidad e integridad de las infraestructuras y servicios de estas empresas.

La información para las organizaciones de telecomunicaciones es un activo esencial y por ello le resuelta necesario conservarlo debido a que es también objeto de muchas amenazas.

Por todo ello, los objetivos que proporciona está norma son:

* Seguridad de la información a través de prácticas que den confianza en las actividades realizadas por las organizaciones.
* Retos globales de la seguridad de la información acondicionados exclusivamente para estas empresas.

La norma **ISO27011** nos garantiza la seguridad de la información de las empresas a través de unos controles apropiados. Estos controles han de ser implementados, controlados, especificados y deben de ir evolucionando a lo largo del tiempo para que se lleve a cabo el cumplimento de los objetivos de seguridad fijados previamente por estas entidades.

Previo a la selección de controles, las organizaciones de telecomunicaciones deben identificar los requisitos y la evaluación continua de los posibles riesgos de seguridad.

La elección de estos controles va a depender de la aceptación del riesgo que tenga esta organización con el requisito, además, de estar sujetas a la normativa legales internacionales o no pertinentes.

Con la implementación de la norma **ISO-27011**, las organizaciones dedicadas a las telecomunicaciones tendrán que llevar a cabo las siguientes pautas:

* Proteger la integridad, confidencialidad y disponibilidad de las infraestructuras y servicios.
* Asegurar la disminución de los riesgos de los servicios que las empresas de telecomunicaciones prestan mediante procesos de cooperación fiables.
* Han de saber reordenar los recursos para que las actividades llevadas a cabo sean más eficientes.
* Acoger un principio global relacionado con la seguridad de la información.
* Tener la capacidad de hacer que la moralidad de las personas y la confianza de las mismas mejoren.