
## CAPITULO I

# La norma ISO 27000

Buenas practicas, términos y definiciones

**SIS-254 SEGURIDAD DE LA INFORMACION**

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

*2/2021*

FAMILIA ISO 27000

ISO International Organization for Standardization

UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER CHUQUISACA FUNDADA EN 27 DE MARZO DE 1624

# Todos los días tenemos riegos que atentan contra la seguridad de la información:

| Usuario internos | Usuarios externos | Desastres naturales |
|---|---|---|


UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

*2021*

ISO 27000

FAMILIA ISO 27000

## ¿Qué podemos hacer para proteger datos e información en un entorno como este?

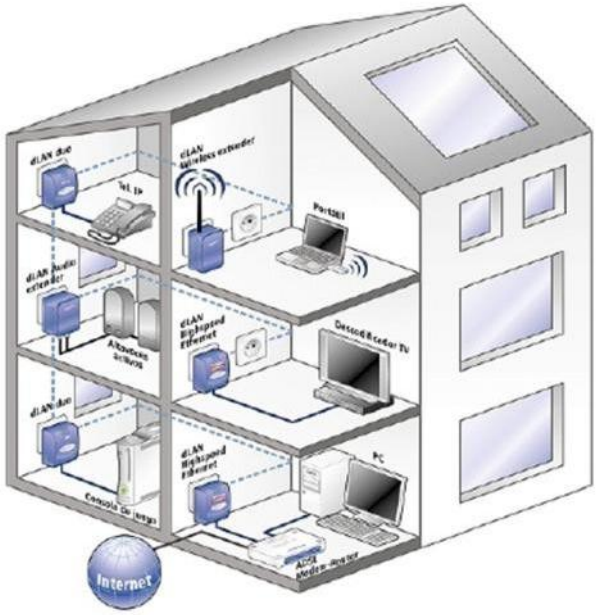

- La respuesta es simple:
  - Se puede implementar un sistema de gestión de seguridad de la información.
- ¿Para qué sirve?
  - Conocer
  - Gestionar
  - Minimizar
    - Los riesgos que atentan contra la seguridad de la información

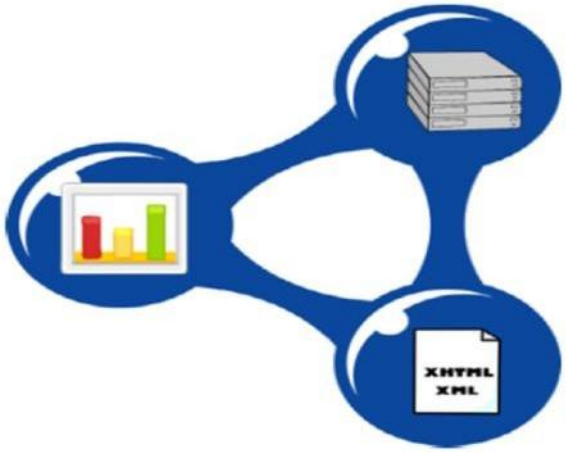
UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

ISO 27000

# ¿Seguridad informática es lo mismo que seguridad de la información?


*Los activos de información provienen de distintas fuentes y se almacenan en diversos soportes, como BD e inclusiv impresos.

*Prof: Ing. D. Roca*

ISO 27000

FAMILIA ISO 27000

# TERMINOS Y DEFINICIONES

**Activo.** En general, activo es todo aquello que tiene valor para la entidad o institución pública.

**Activo de información.** Conocimientos, datos o informacion que tienen valor para la organización.

**Acuerdo de confidencialidad.** Documento en el cual el servidor público y/o terceros se comprometen a respetar la confidencialidad de la información y a usarla solo para el fin que se estipule.

Términos y Definiciones NB/ISO/IEC 27000:2010.

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

ISO 27000

**Apetito del riesgo.** Nivel máximo de riesgo que una entidad o institución está dispuesta a aceptar o soportar.

**Amenaza:** (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.


**Aceptación del riesgo:** Decisión de asumir un riesgo, la aceptación del riesgo puede ocurrir sin tratamiento, durante o al final del proceso de tratamiento del riesgo.

**Ataque:** Intentar destruir, exponer, alterar, inutilizar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo

**Análisis de riego:** Uso sistemático de la información para identificar fuentes y estimar riesgos.

**Activos Informáticos**: Son aquellos recursos (hardware y software) con los que cuenta una institución. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.

https://es.scribd.com/document/282558227/Activos-Informaticos

**Base de datos:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Almacenes/Deposito:** locales donde se guarda material informático y de telecomunicaciones y/o copias de seguridad.

**Comité de Seguridad de la Información (CSI).** Equipo de trabajo conformado para gestionar, promover e impulsar iniciativas en seguridad de la información.

**Confidencialidad.** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.[1]

**Custodia del activo de información.** Servidor público encargado de administrar y hacer efectivo los controles de seguridad definidos por el responsable del activo de información. **Disponibilidad.** Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

1 Términos y Definiciones NB/ISO/IEC 27000:2010


**CIA:** Acrónimo inglés de confidentiality, integrity y availability, las dimensiones básicas de la seguridad de la información.

**CID:** Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

**CobiT:** Control Objectives for Information and related Technology. Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacional y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

**CISA:** Certified Information Systems Auditor. Es una acreditación ofrecida por ISACA.

**CISM:** Certified Information Security Manager. Es una acreditación ofrecida por ISACA.


**CISSP:** Certified Information Systems Security Professional. Es una acreditación ofrecida por ISC2.

**Checklist:** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Control correctivo:** (Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

**Control detectivo:** (Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.


**Control disuasorio:** (Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

**Control preventivo:** (Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

**Control selection:** Selección de controles.

**Corrección:** (Inglés: Correction). Acción para eliminar una no conformidad detectada.


**Custodia del activo de información:** Servidor público encargado de administrar y hacer efectivo los controles de seguridad definidos por el responsable del activo de información. Disponibilidad. Propiedad de acceso y uso de información a entidades autorizadas cuando estas lo requieran.

**Cifrar:** Técnicas bajo las cuales se transforma la información (de texto claro a texto secreto) y que solo puede ser accedida si se cuenta con las llaves o contraseñas.


**Centros de Proceso de Datos (en adelante CPDs):** Salas de equipamiento TIC en las que se ubican los Sistemas de Información de la institucion. Requieren unas características técnicas particulares, infraestructura específica, medidas concretas de seguridad y mantenimiento continuo para su correcto funcionamiento.

**Cuartos Técnicos de Telecomunicaciones:** locales donde se ubican los racks de telecomunicaciones del edificio, equipo activo, infraestructura de RED y/o la central telefónica del edificio.


**Declaración de aplicabilidad:** (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, *así como la justificación de las exclusiones de controles del anexo A de ISO 27001*.

**Desastre:** (Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

**Directiva o directriz:** (Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

**Disponibilidad:** (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

**DRII:** Instituto Internacional de Recuperación de Desastres.

**Entregables.-** Son los productos intermedios que generan las fases. Los entregables permiten evaluar la marcha del proyecto mediante comprobaciones de su adecuación o no a los requisitos funcionales y de condiciones de realización previamente establecidos.


**Entidad de acreditación:** (Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

**Entidad de certificación:** (Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.


**Entidad de normalización:** (Inglés: Standards body). Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), IBNORCA Bolivia, etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

**Estimación de riesgos:** (Inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable

**Evaluación de riesgos:** (Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

**Evidencia objetiva:** (Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

**Eventos de seguridad de la información:** Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.


**Fase 1 de auditoría:** (Inglés: Stage 1 Audit). Etapa de la auditoría de primera certificación en la que, fundamentalmente a través de la revisión de documentación, se analiza en SGSI en el contexto de la política de seguridad de la organización, sus objetivos, el alcance, la evaluación de riesgos, la declaración de aplicabilidad y los documentos principales, estableciendo un marco para planificar la fase 2.

**Fase 2 de auditoría:** (Inglés: Stage 2 Audit). Etapa de la auditoría de primera certificación en la que se comprueba que la organización se ajusta a sus propias políticas, objetivos y procedimientos, que el SGSI cumple con los requisitos de ISO 27001 y que está siendo eficaz.

**Gestión de claves:** (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.


**Gestión de incidentes de seguridad de la información:** (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

**Gestión de riesgos:** (Inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

FAMILIA ISO 27000

ISO International Organization for Standardization

UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER CHVQUISACA FUNDADA EN 27 DE MARZO DE 1624


**Gobernanza de la seguridad de información:** sistema por el cual las actividades de seguridad de información de una organización son dirigidas y controladas

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

ISO 27000


**Incidente de seguridad:** uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

**Integridad:** Propiedad de salvaguardar la precisión y completitud de los recursos.

**Identificación de riesgos:** (Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

**IEC:** International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

**IIA:** Instituto de Auditores Internos.

**Impacto**: (Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.

**Incidente de seguridad de la información:** (Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.


**Inventario de activos:** (Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**IRCA:** International Register of Certified Auditors. Acredita a los auditores de diversas normas, entre ellas ISO 27001.

**ISACA:** Information Systems Audit and Control Association. Publica CobiT y gestiona diversas acreditaciones personales en el ámbito de la auditoría de sistemas y la seguridad de la información.

FAMILIA ISO 27000


**ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

**ITIL:** IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información.

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

ISO 27000

**Método.-** Un método se compone de diversos aspectos que nos permitirán conseguir una meta o lograr un objetivo. Se define más claramente como un conjunto de herramientas, las cuales, utilizadas mediante las técnicas correctas, permiten la ejecución de procesos que nos llevarán a cumplir los objetivos que buscamos

**Metodología.-** Hace referencia al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la metodología como el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto.

FAMILIA ISO 27000

**Metodología de Desarrollo de Software. -** Es un marco de trabajo usado para estructurar, planificar y controlar el proceso de desarrollo en sistemas de información. En un proyecto de desarrollo de software la metodología ayuda a definir: *Quién* debe hacer *Qué Cuándo* y *Cómo* debe hacerlo.

La metodología para el desarrollo de software es un modo sistemático de realizar, gestionar y administrar un proyecto para llevarlo a cabo con altas posibilidades de éxito. Una metodología para el desarrollo de software comprende actividades a seguir para idear, implementar y mantener un producto de software desde que surge la necesidad del producto hasta que se cumple el objetivo por el cual fue creado.

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*

ISO 27000


**Módulo Informático. -** Es una porción de software que realiza tareas específicas.

**Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad para determinar el estado puede haber una necesidad de revisar, supervisar o críticamente observar.


**No conformidad:** Incumplimiento de un requisito.

**No repudio:** Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.

Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).


**Objetivo:** (Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

**Objetivo de control:** Declaración que describe lo que se quiere lograr como resultado de los controles de aplicación.

**Proyecto:** Según la definición que nos proporciona PMI en su guía PMBOOK, un proyecto se podría definir como “un servicio temporal que se lleva a cabo para crear un producto, servicio o resultado único”. Podemos decir entonces que un proyecto tiene un inicio y un fin, este fin se tiene que alcanzar dentro de un tiempo fijado.


**Política de Seguridad de la Información (PSI).** Acciones o directrices que establecen la postura institucional en relación a la seguridad de la información, incluidas dentro del Plan Institucional de Seguridad de la Información.

**Plan Institucional de Seguridad de la Información (PISI).** Documento que establece las actividades relativas a la organización y gestión de la seguridad de la información en la entidad o institución pública.

**Parte interesada:** (Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**PDCA:** Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

**Plan de continuidad del negocio:** (Inglés: Bussines Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

**Plan de tratamiento de riesgos:** (Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

**Política de escritorio despejado:** (Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

**Proceso:** (Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

**Propietario del riesgo:** (Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.


**Riesgo:** (Inglés: Risk). *Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información*. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**Riesgo residual:** (Inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo, también puede ser conocido como "riesgo retenido".

**Responsable del activo de información:** Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer los requisitos de seguridad y la clasificación de la información vinculada al activo enmarcado al proceso del cual es responsable.

**Responsable de procesos:** Servidor público de nivel jerárquico que tiene la responsabilidad y atribución de establecer las actividades, roles y responsabilidades de los procesos. Responsable de Seguridad de la Información (RSI). Servidor público responsable de gestionar, planificar, desarrollar e implementar el Plan Institucional de Seguridad de la Información.


**Seguridad de la información.** La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, trazabilidad(*Accountability*), no repudio y confiabilidad.

**Seguridad informática.** Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

**Servidor público.** Persona individual, que independientemente de su jerarquía y calidad, presta servicios en relación de dependencia a una entidad, u otras personas que presten servicios en relación de dependencia, cualquiera sea la fuente de su remuneración.

Artículo 4, Ley 2027 del Estatuto del Funcionario Público.

**Software institucional:** Software con licenciamiento de uso y/o propietario que puede ser instalado y utilizado por los usuarios para el desempeño de sus actividades o funciones, o para la gestión de un servicio informático otorgado por la institución.

FAMILIA ISO 27000

**Software libre:** También conocido como freeware, shareware, software demo. Software gratuito proveniente de internet o cualquier otro medio que no requiere la compra de una licencia para su uso.

**Sistema de gestión de la seguridad de la información SGSI:** Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

NOTA El sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos.

UMRPSFXCH FACULTAD TECNOLOGÍA

*Prof: Ing. D. Roca*


**Sistema de información:** aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.

**Sistema de información:** Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información


**Tratamiento de riesgos:** (Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

**Trazabilidad:** (Inglés: Accountability). Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

**TIC:** Tecnologías de Información y Comunicación.


**Vulnerabilidad:** (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

**Validacion:** Confirmación, a través de la aportación de evidencia objetiva, de que se han cumplido los requisitos para un uso específico previsto o aplicación [FUENTE: ISO 9000: 2005].

**Verificación:** confirmación, a través de la presentación de pruebas objetivas, que especifica los requisitos se han cumplido [FUENTE: ISO 9000: 2005]. Esto también podría ser llamado prueba de conformidad.