CRIPTOGRAFIA APLICADA

1

AGENDA

SEGURIDAD DE LA INFORMACIÓN

- Contexto y seguridad de la información

Definiciones

- Principales amenazas en seguridad de la información

ISO 27001

2

3

DEFINICIONES

¿QUE ENTENDEMOS ENTONCES POR SEGURIDAD?

4

1ª perspectiva: criptografía y códigos

2ª perspectiva: seguridad en redes

3ª perspectiva: gestión de la seguridad

4ª perspectiva: ciberseguridad

5

Seguridad

Tener confianza en algo o en alguien

"el estado de bienestar que percibe y disfruta el ser humano".

Ejemplo:

- seguridad sobre las personas: seguridad física
- seguridad sobre el ambiente: seguridad ambiental
- seguridad en ambiente laboral: seguridad e higiene

6

Son Aspectos de la seguridad que inciden directamente en los medios informáticos en los que la información se genera, se gestiona, se almacena o se destruye.

Seguridad Informática

VS

Seguridad de la Información

Se suman aspectos sistémicos de la gestión de esa seguridad, la orientación de esta seguridad hacia la continuidad del negocio, así como su adecuación al entorno legal y a las normativas internacionales

7

Ciberseguridad

Y

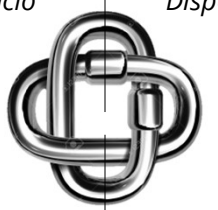
Ciberespacio

Condición de estar protegido en contra de las consecuencias físicas, sociales… que resultan del fallo, dañó… en el Ciberespacio que se pueda considerar no deseable.

Amenazas originadas en el ciberespacio que afectan a la organización

Entorno complejo que resulta de la interacción de personas , softwares y servicios en Internet por medio de dispositivos y redes de tecnología conectados a este

Dispositivos y redes conectados en forma virtual



8

Definiciones

- Ciberocupa
- Software engañoso
- Hackeo
- Hacktivismo
- Cibercrime
- Internet
- crimen de internet

9

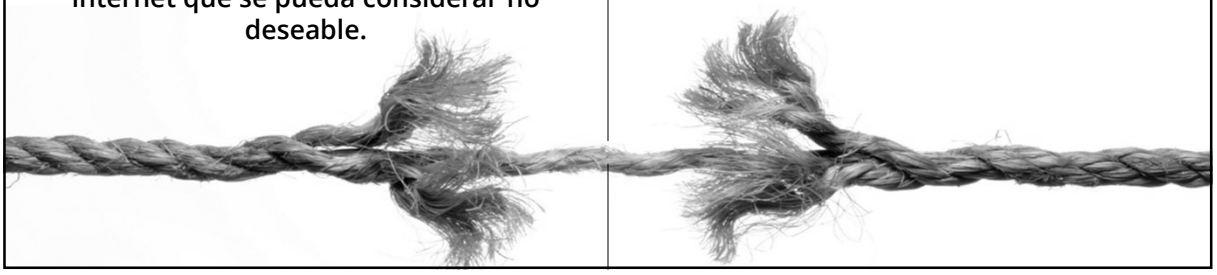
Seguridad de internet

Condición de estar protegido en contra de consecuencia físicas, sociales, espirituales, financieras, etc. que resultan del fallo, daño error, accidente perjuicio cualquier otro evento en internet que se pueda considerar no deseable.

O

Protección de internet

conservación de la confidencialidad, integridad y disponibilidad de la información que es accedida en internet



10

Contexto y Seguridad de la Información

11

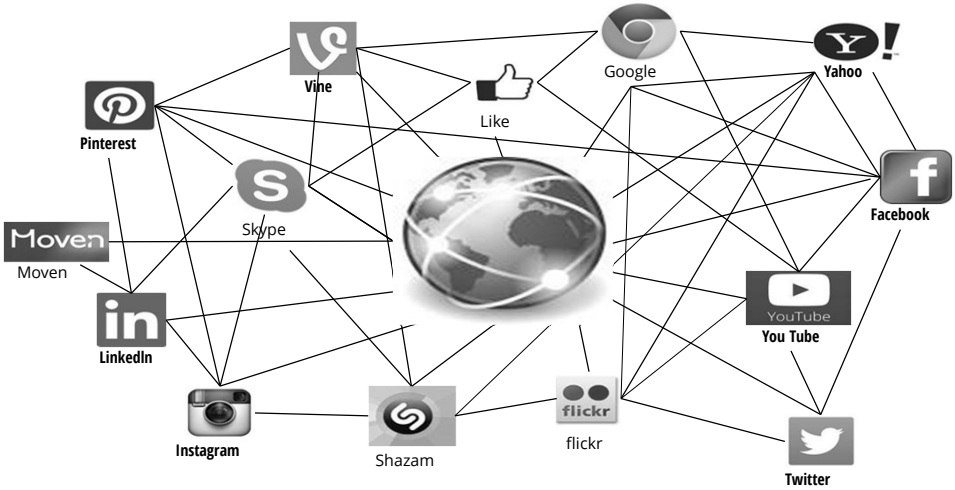
2005: Funeral del Papa Juan Pablo II

12

Elección del Papa Francisco

13

Contexto y Tendencias



14

Algunos hechos recientes

OPM

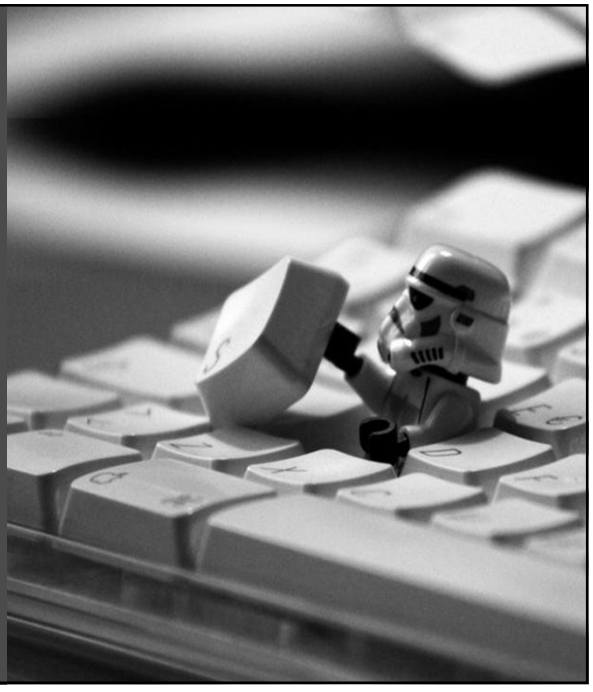
IRS

Apple Developer Tools
XcodeGhost

15

Amenazas Informáticas

1. **Ingeniería Social**
2. **Código malicioso**
   a. Virus
   b. Malware
3. **Amenazas Avanzadas**
   a. Ramsomware
   b. Amenazas Persistentes Avanzadas
4. **Amenazas Web / Mail**
   a. Spam
   b. Phishing



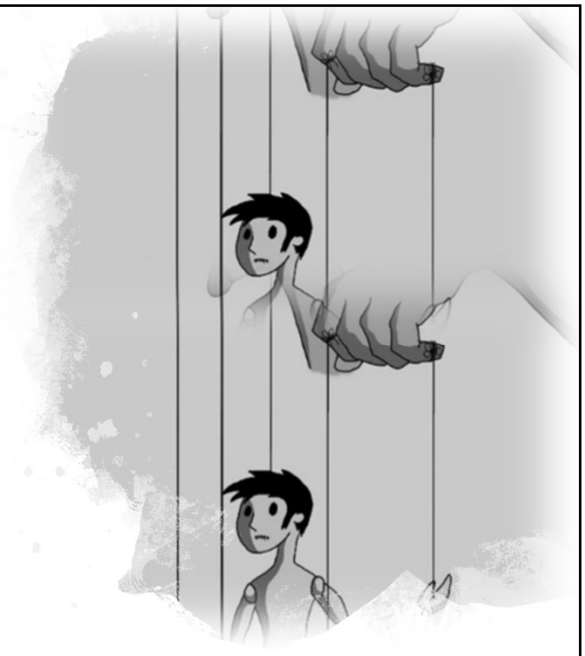
16

La ingeniería social

Es el término es utilizado para describir un método en el que un atacante, haciendo uso de la persuasión, y por lo general abusando de la ingenuidad o confianza de un usuario, busca obtener información confidencial.

Muchas veces, la información extraída a la víctima es utilizada para conseguir acceso no autorizado y comprometer la seguridad de un sistema.

Podríamos usar la analogía de que la ingeniería social se refiere al **hacking de la mente** humana.



17

Somos vulnerables porque somos muy confiados

El ser humano tiene la tendencia instintiva de confiar en cualquier persona que solicita ayuda.

- ✓ Todo lo que tiene que hacer un atacante es crear un escenario creíble para su víctima.
- ✓ El atacante buscará hacerse pasar por alguien conocido.
- ✓ En otros casos buscará engañar a alguien a quien sí conocemos para que sea esta persona quien nos solicite la información buscada.

Es por eso que factor humano es considerado el **eslabón más delgado** en la cadena de la seguridad de la información

18

19

Estar permanentemente alerta…

Ante cualquier solicitud de información, debemos siempre preguntarnos: ¿La persona con la que hablo,…

- ✓ …es en realidad quien dice ser?
- ✓ …es un empleado o alguien quien tiene algún tipo relación con la empresa?
- ✓ …está autorizada para recibir la información que está solicitando?
- ✓ …está autorizada para realizar gestiones en nombre de la empresa?

20

Código malicioso (Virus)

"El problema de los virus de computadora es temporal y estará resuelto en un par de años"

—John McAfee, ¡1988!
(fundador de McAfee, Inc., empresa fabricante de un conocido antimalware)

;-)

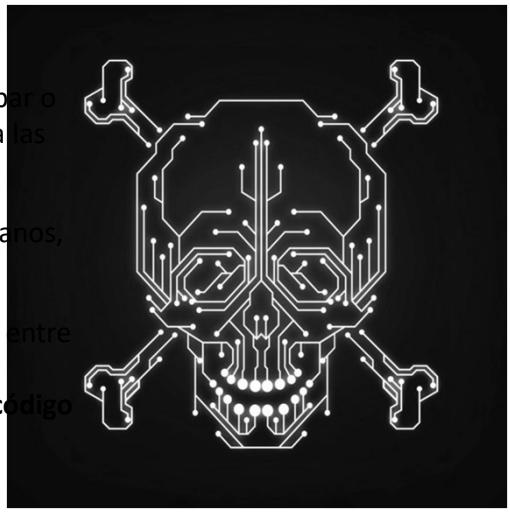
21

Código malicioso (malware)

Se trata de programas de software escritos específicamente para producir inconvenientes, robar o destruir información, o atacar de manera indirecta las redes y sistemas de otra organización.

Antes se clasificaban por tipo (virus, gusanos, troyanos, backdoors, spyware, keyloggers, etc.).

Hoy en día a veces es difícil distinguir la diferencia entre un tipo y otro, por lo que se denominan de forma común como ***malware*** (de *malicious software*) o **código malicioso** en español.



22

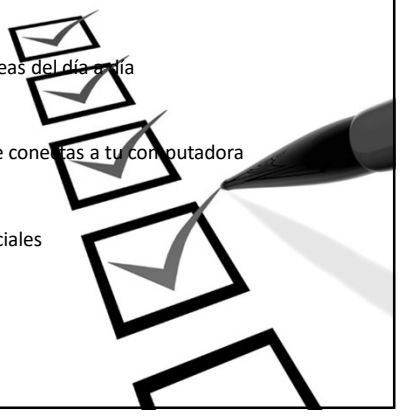
¿Qué cosas puede hacer el código malicioso?

- Borrar archivos del disco rígido para que la computadora se vuelva inoperable
- Infectar una computadora y usarla para atacar a otras
- Obtener información sobre vos, los sitios web que visitás y tus hábitos de uso de la computadora
- Capturar tus conversaciones activando el micrófono, o fotos y videos a través de la webcam
- Ejecutar comandos en la computadora, como si lo hubieras hecho vos
- Robar archivos del equipo (p.e., información personal, financiera, etc.)

23

¿Qué puedo hacer para prevenir una infección por código malicioso?

- ✓ Mantener al día el sistema operativo y programas de tu computadora con las actualizaciones y parches de seguridad más recientes
- ✓ Instalar y mantener actualizado un software antimalware
- ✓ Sólo instalar software nuevo desde fuentes confiables
- ✓ Evitar utilizar una cuenta con privilegios de administrador del sistema para las tareas del día a día
- ✓ Habilitar en tu equipo un firewall (cortafuegos) personal
- ✓ Tener mucho cuidado con los dispositivos de almacenamiento externos (USB) que conectas a tu computadora
- ✓ Evitar la descarga de archivos desde sitios no oficiales o confiables
- ✓ No descargar archivos adjuntos de mensajes de correo-e sospechosos o redes sociales
- ✓ Y finalmente… un poco de **sentido común**



24

Amenazas Persistentes Avanzadas

Las Advanced Persistent Threats (APT) conforman una clase de código malicioso sigiloso y de ejecución continua cuyo objetivo es vulnerar la seguridad y la operación regular de una organización o gobierno.

- Normalmente este tipo de ataques son orquestados por grupos de crimen organizado
- La actividad del APT es monitoreada y controlada de forma externa por el atacante
- Para lograr su cometido por lo general se requiere que la infección se mantenga durante un largo período de tiempo

25

26

Ransomware

- Código malicioso que ejecuta el secuestro parcial o total de los datos del usuario.
  - La información es cifrada con claves y algoritmos conocidos sólo por el atacante.
  - Se coacciona al usuario a pagar un “rescate” cambio de la clave para descifrar sus archivos.

- Para devolver el equipo a un estado operativo “normal”, el ransomware demanda que el usuario:
  - Pague una suma (mediana a considerable) de dinero
  - Algunos más excéntricos piden al usuario que completen encuestas

27

¿Qué hace el ransomware?

El Ransomware está diseñado para:

- Prevenir el acceso y uso regular del sistema operativo
- Cifrar los archivos para que no puedan ser utilizados
- Evitar que se ejecuten algunas aplicaciones

Para devolver el equipo a un estado operativo “normal”, el ransomware demanda que el usuario:

- Pague una suma (mediana a considerable) de dinero
- Algunos más excéntricos piden al usuario que completen encuestas

28

RANSOMWARE – en la vida real:

29

30

SPAM

- Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

- Los spammers utilizan diversas técnicas para armar largas listas de direcciones de correo a las cuales enviar este tipo de mensajes:

- Búsqueda de direcciones en paginas web y foros
- Captura de direcciones en cadenas de correo
- Suscripciones a listas de correo
- Compra de bases de datos de direcciones de correo
- Acceso no autorizado en servidores de correo

31

PHISHING

- Pueden recibirse correos electrónicos, supuestamente de empresas conocidas, solicitando información personal confidencial. Generalmente piden el envío de información, o contienen enlaces hac páginas falsificadas.

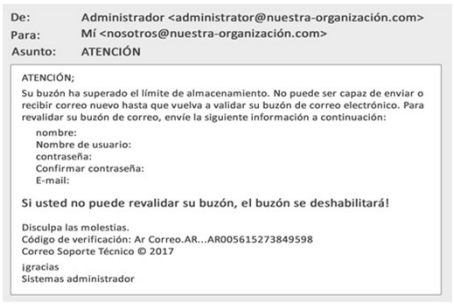
- Las técnicas más usadas son:

- Mensajes alarmistas para forzar al usuario a acceder al enlace web indicado en el mail.
- Pedidos de envío de datos en forma inmediata. Las páginas suelen tener poco tiempo de publicación.

32

Phishing - Un delito en crecimiento

- ✓ Los ciberdelincuentes roban nuestra información privada, engañándonos para que nosotros mismos se la proporcionemos.
- ✓ Este nombre, viene del inglés “Pescar”, y la relación está en que los ciberdelincuentes nos hacen “morder un anzuelo” cuando nos engañan nosotros terminamos brindándoles nuestra información
- ✓ NO ES SÓLO EMAIL, TAMBIEN SMS, WhatsApp, SITIOS FALSOS, PUBLICIDAD , ETC



De: Administrador <administrator@nuestra-organización.com>
Para: Mí <nosotros@nuestra-organización.com>
Asunto: ATENCIÓN

ATENCIÓN;
Su buzón ha superado el límite de almacenamiento. No puede ser capaz de enviar o recibir correo nuevo hasta que vuelva a validar su buzón de correo electrónico. Para revalidar su buzón de correo, envíe la siguiente información a continuación:
nombre:
Nombre de usuario:
contraseña:
Confirmar contraseña:
E-mail:

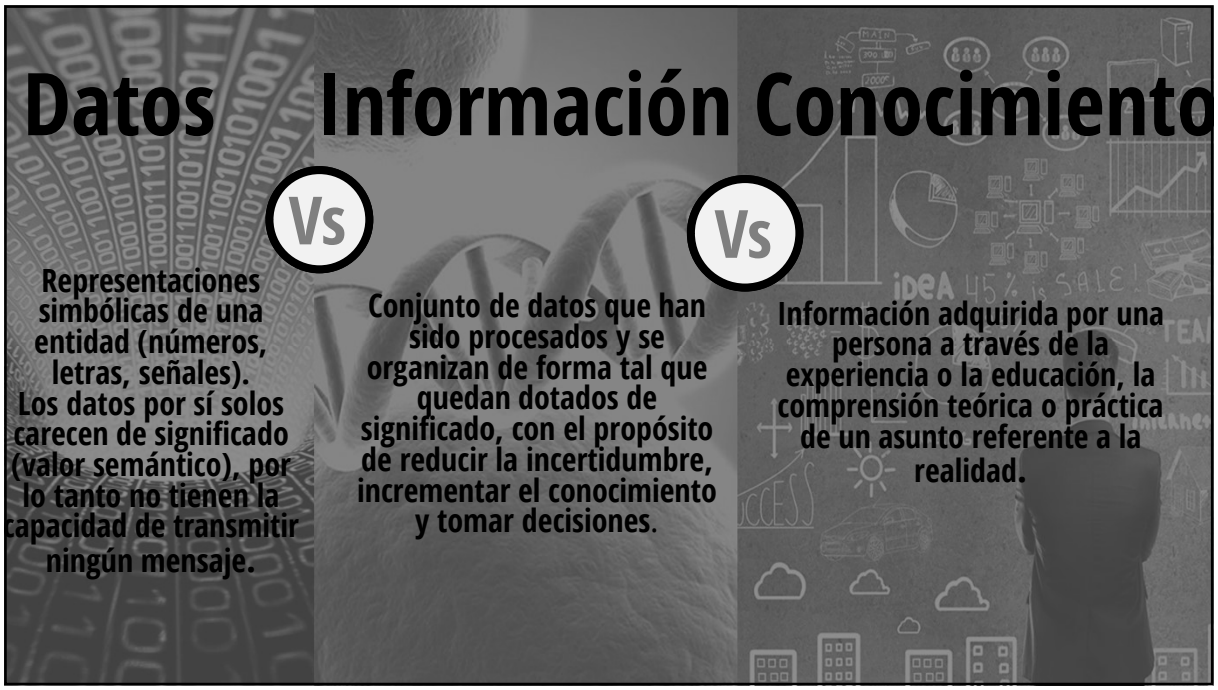
Si usted no puede revalidar su buzón, el buzón se deshabilitará!

Disculpa las molestias.
Código de verificación: Ar Correo.AR...AR005615273849598
Correo Soporte Técnico © 2017
igracias
Sistemas administrador

33

Norma IRAM-ISO/IEC 27001

34


Datos
Vs
Representaciones simbólicas de una entidad (números, letras, señales). Los datos por sí solos carecen de significado (valor semántico), por lo tanto no tienen la capacidad de transmitir ningún mensaje.
Información
Vs
Conjunto de datos que han sido procesados y se organizan de forma tal que quedan dotados de significado, con el propósito de reducir la incertidumbre, incrementar el conocimiento y tomar decisiones.
Conocimiento
Información adquirida por una persona a través de la experiencia o la educación, la comprensión teórica o práctica de un asunto referente a la realidad.

35


Definiciones de tipos de Activos
Activo
Información
Virtual
Físico

36

Qué es ISO/IEC 27001?

Standard Auditable.

Marco para administrar un Programa de Seguridad de la Información.

Permite considerar aspectos legales, reglamentarios y requisitos contractuales.

Mejora Continua (Ciclo PDCA).

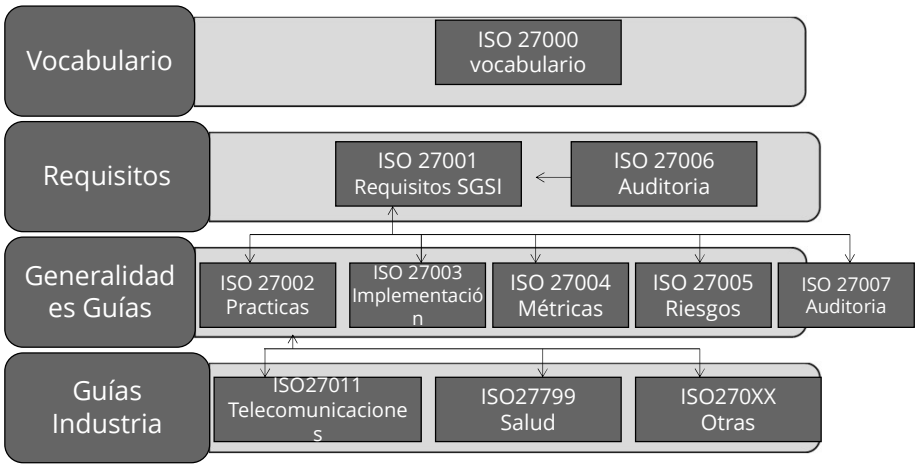
La ISO 27001 define como componentes básicos:

- Confidencialidad
- Integridad
- Disponibilidad

"La información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y requiere ser protegida."

37

La familia ISO 27000



Resultante de reflexiones de grupos de trabajo internacionales dedicados al ámbito de la seguridad de la información, la familia ISO 27000 se esta publicando gradualmente desde el año 2005. ISO27001:2005 es la única norma certificable de la familia ISO 27000. Las demás normas son directrices.

38

La información como Activo

Seguridad de la información es determinar que requiere ser protegido y por que, de que debe ser protegido y como protegerlo.

Las Organizaciones tienen que desarrollar mecanismos que les permitan asegurar la

Disponibilidad

Integridad

Confidencialidad

en el manejo de la información.

Debido a que la información esta sujeta a muchas amenazas, tanto Internas como externas

La información es un activo, que tal como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente

Términos y definiciones

- **Evento de seguridad**: cualquier ocurrencia que indique la posibilidad de que se haya violado la política de seguridad, haya fallado algún control o situación previamente desconocida que pueda ser relevante desde la seguridad.
- **Incidente de seguridad**: uno o varios eventos de seguridad, inesperados o no deseados que tienen una probabilidad cierta y significante de comprometer la operación del negocio o amenazar la seguridad de la información.

¿Que se busca proteger?

- La Seguridad de la Información busca garantizar:

CONFIDENCIALIDAD

La información sólo debe ser accedida por personas o sistemas autorizados

¿Que niveles de clasificación tenemos ?

INTEGRIDAD

La información debe mantenerse libre de modificaciones no autorizadas

¿Que hacemos para asegurarnos que se mantienen Íntegros?

DISPONIBILIDAD

La información debe encontrarse a disposición de quienes están autorizados a accederla, en el momento en que así lo requieran

¿ Hacemos un buen uso de las Tecnología?

41

CONFIDENCIALIDAD

Nivel de Confidencialidad	Nombre	Descripción
0	Nivel de confidencialidad muy bajo.	La información se puede hacer público
1	Nivel de confidencialidad bajo.	Hacerlo público supone una pérdida leve de confianza de la opinión pública
2	Nivel de confidencialidad medio	Hacerlo se ven comprometidas ventajas competitivas o un atacante puede utilizarla para comprometer activos relevantes de la organización
3	Nivel de confidencialidad alto.	Hacerlo público dañaría la imagen y se sufriría una pérdida de confianza. información muy relevante para el proceso
4	Nivel de confidencialidad crítico.	Hacerlo público supone una falta total de confianza y la pérdida de negocio. Pérdida de clientes y acciones legales

- ✓ **La información debe estar dirigida solamente a las personas autorizadas**
- ✓ **La confidencialidad es una propiedad de difícil recuperación**
- ✓ **No hacerlo da lugar darse fugas y filtraciones de información, incumplimiento de leyes y compromisos contractuales.**

42

INTEGRIDAD

- ✓ La información debe mantener sus características de completitud y corrección para que sea confiable
- ✓ La información puede aparecer manipulada, corrupta o incompleta
- ✓ No hacerlo afecta directamente al correcto desempeño de las funciones de una Organización.

Nivel de Integridad	Nombre	Descripción
0	Nivel de integridad muy bajo.	El proceso de negocio no se ve afectado
1	Nivel de integridad bajo.	La falla puede afectar a procesos de soporte
2	Nivel de integridad medio	Se producen errores que afecta al proceso de negocio ligeramente, ocurren errores en el proceso y se requiere re trabajo
3	Nivel de integridad alto.	Se produce ralentización de actividades, mal funcionamiento del servicio se ve afectado severamente al proceso de negocio, podrían ver errores graves en la entrega del servicio
4	Nivel de integridad crítico.	El servicio no puede funcionar o el servicio no puede ser entregado. La imagen de la empresa se ve afectada, se pierden clientes por la mala calidad del servicio.

43

DISPONIBILIDAD

Nivel de Disponibilidad	Nombre	Descripción
0	Nivel de disponibilidad muy bajo.	El proceso de negocio no se ve afectado
1	Nivel de disponibilidad bajo.	La falla afectar a uno o muy pocos clientes. (El proceso de negocio no está disponible el 10% del tiempo)
2	Nivel de disponibilidad medio.	La falla afectar a algunos clientes que ven el servicio interrumpido. (El proceso de negocio no está disponible el 30% del tiempo)
3	Nivel de disponibilidad alto.	La falla afectar a la mitad de los clientes (El proceso de negocio no está disponible el 50% del tiempo)
4	Nivel de disponibilidad crítico.	El servicio no puede funcionar o el servicio no puede ser entregado. La imagen de la empresa se ve afectada, se pierden clientes por la mala calidad del servicio.

- ✓ La información provista por los servicios debe estar disponible (ser usada) cuando sea necesario o se lo requiera
- ✓ La carencia de disponibilidad supone una interrupción del servicio
- ✓ No brindarlo afecta directamente a la productividad

44

IMPORTANCIA

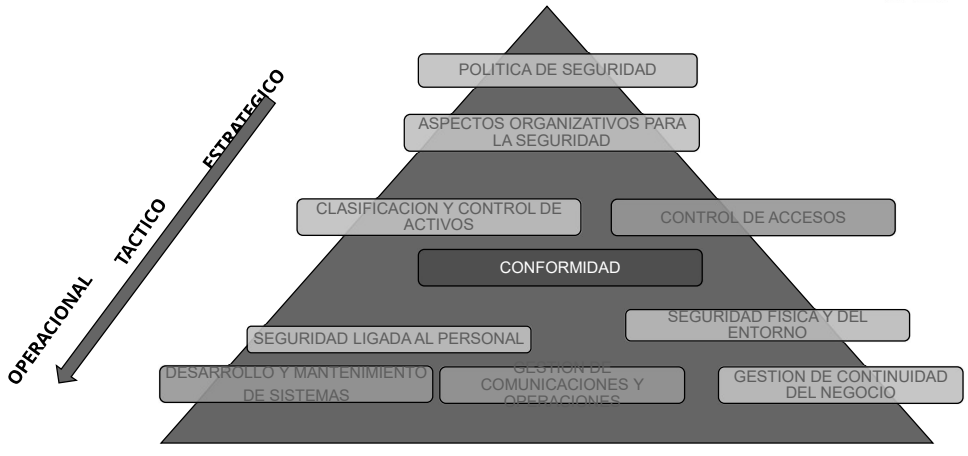
✓ **Cada activo se lo evalúa y se obtiene un valore de referencia**

VALOR de IMPORTANCIA = DISPONIBILIDAD + INTEGRIDAD + CONFIDENCIALIDAD

Valor de Importancia	Nivel de criticidad del activo
0 -3	Nivel de criticidad baja.
4-6	Nivel de criticidad medio
7-9	Nivel de criticidad alto.
10- 12	Nivel de criticidad crítico.

45

Dominios de la Norma ISO 27001



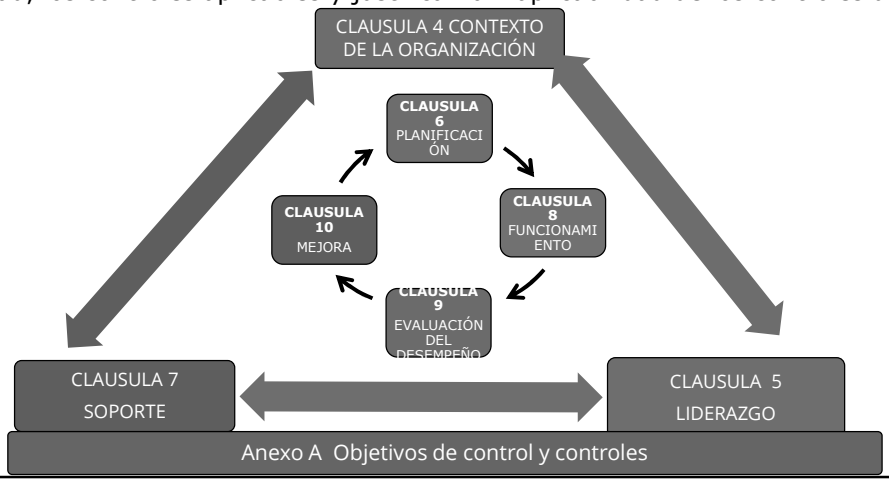
SEGURIDAD ORGANIZATIVA
SEGURIDAD LOGICA
SEGURIDAD FÍSICA
SEGURIDAD LEGAL

DOMINIOS DE LA NORMA ISO 27001

46

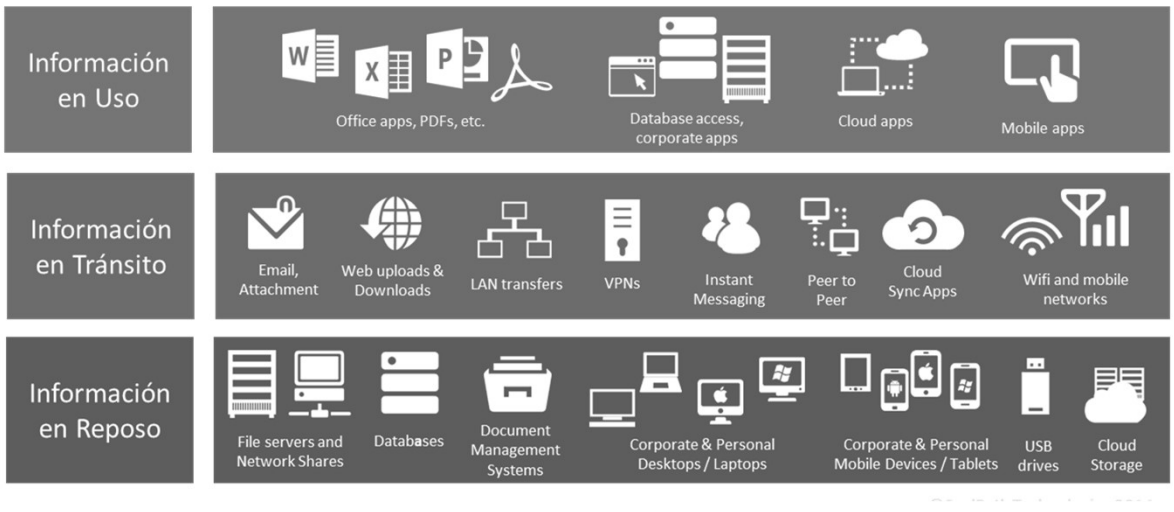
Estructura de la norma ISO 27001

Una organización que busca la certificación ISO 27001 debe cumplir con todos los términos definidos en las cláusulas 4 a 10 de la norma, definir, en la declaración de aplicabilidad, los controles aplicables y justificar la inaplicabilidad de los controles del Anexo A



47

Estados de la información



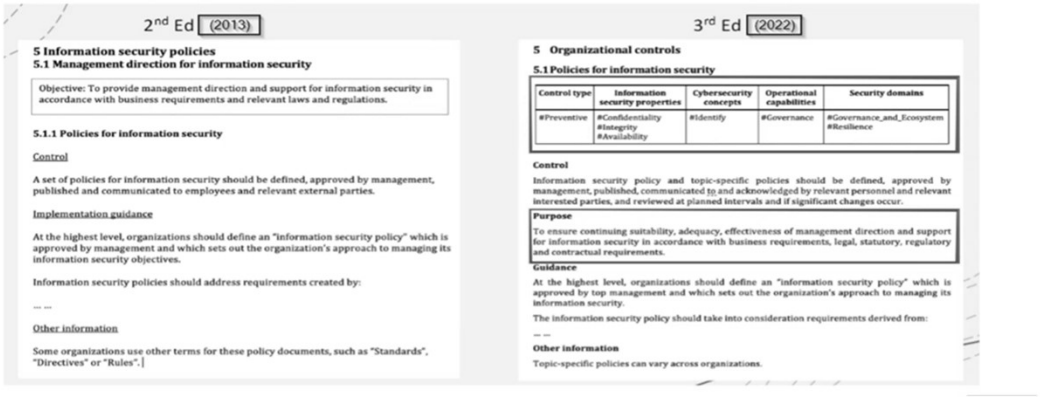
48

NUEVA VERSION DE ISO 27002

49

Principales cambios en la nueva versión ISO 27002:2022

- Cambios clave en ISO/IEC 27002:2022 en comparación con la edición de 2013 - Cambios en la estructura de cada Control



2nd Ed (2013)

5 Information security policies
5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.

Implementation guidance

At the highest level, organizations should define an "information security policy" which is approved by management and which sets out the organization's approach to managing its information security objectives.

Information security policies should address requirements created by:

-- --

Other information

Some organizations use other terms for these policy documents, such as "Standards", "Directives" or "Rules".

3rd Ed (2022)

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business requirements, legal, statutory, regulatory and contractual requirements.

Guidance

At the highest level, organizations should define an "information security policy" which is approved by top management and which sets out the organization's approach to managing its information security.

The information security policy should take into consideration requirements derived from:

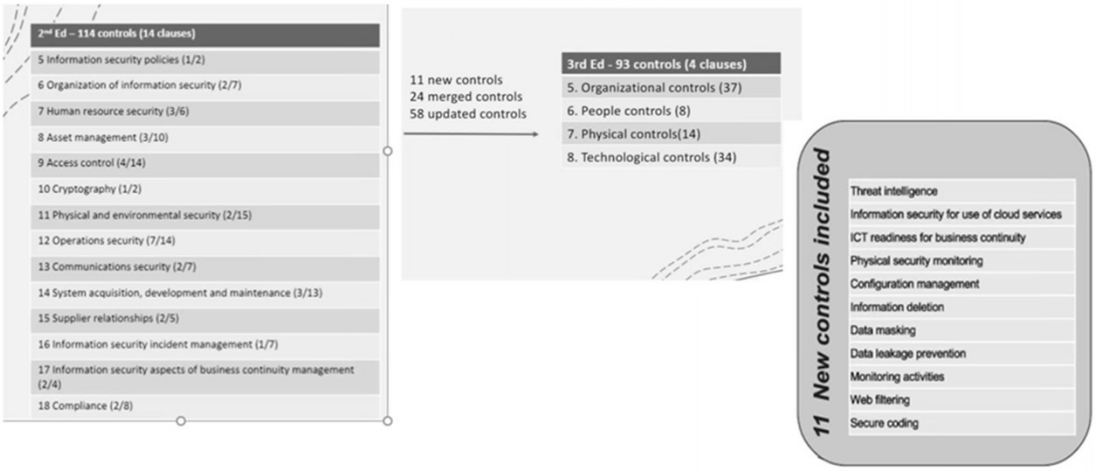
-- --

Other information

Topic-specific policies can vary across organizations.

50

Principales cambios en la nueva versión ISO 27001:2022



51

Principales cambios en la nueva versión ISO 27001:2022

5.25 Assessment and decision on information security events

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose

To ensure effective categorization and prioritization of information security events.

Guidance

A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each information security event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

52

Principales cambios en la nueva versión ISO 27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Inteligencia de amenazas (5.7)	La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas.	Proporcionar conciencia sobre el entorno de amenazas para que se puedan tomar las medidas apropiadas.
Seguridad de la información para uso de servicios en la nube (5.23)	El proceso de adquisición, uso, gestión y salida del servicio en la nube debe establecerse de acuerdo con los requisitos de seguridad de la información de la organización.	Especificar y administrar la seguridad de la información para el uso de servicios en la nube
Preparación de las TIC para la continuidad del negocio (5.30)	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	Para garantizar la disponibilidad de la información de la organización y otros activos asociados durante la interrupción
Vigilancia de la seguridad física (7.4)	Las instalaciones deben monitorearse continuamente para detectar accesos físicos no autorizados.	Para detectar y disuadir el acceso físico no autorizado.

53

Principales cambios en la nueva versión ISO 27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Gestión de la configuración (8.9)	La configuración, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes debe establecerse, documentarse, implementarse, monitorearse y revisarse.	Para garantizar que el hardware, el software, los servicios y las redes funcionen correctamente con la configuración de seguridad requerida, y que la configuración no se altere por cambios no autorizados o incorrectos.
Eliminación de información (8.10)	La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.	Para evitar la exposición innecesaria de información confidencial y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales para la eliminación de información.
Enmascaramiento de datos (8.11)	El enmascaramiento de datos debe usarse de acuerdo con la política específica del tema de la organización sobre el control de acceso y los requisitos comerciales, teniendo en cuenta los requisitos de la legislación aplicable.	Limitar la exposición de datos confidenciales, incluida la PII, y cumplir con los requisitos legales, estatutarios, reglamentarios y contractuales.

54

Principales cambios en la nueva versión ISO 27001:2022

Descripción general de los nuevos controles

Título del control	Control	Propósito
Prevención de fuga de datos (8.12)	Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y dispositivos finales que procesan, almacenan o transmiten información confidencial.	Para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.
Actividades de seguimiento (8.16)	Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y deben tomarse las medidas apropiadas para evaluar posibles incidentes de seguridad de la información.	Para detectar comportamientos anómalos y posibles incidentes de seguridad de la información.
Filtrado web (8.23)	El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso	Para proteger los sistemas contra el malware y evitar el acceso a recursos web no autorizados.
Codificación segura (8.28)	Los principios de codificación segura deben aplicarse al desarrollo de software.	Garantizar que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información en el software.

55

Ejemplos

56

Clasificación de activos (Ejemplo)

ACTIVOS DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
- Software periplo	2	5	5	4
- BD (Aho-peripl)	5	5	4	5
- Equipo de cómputo	1	1	4	2
- Línea dedicada	2	2	5	3
- Internet	2	1	3	2
- Servidor de archivos	5	5	4	5
- Servidor de BD	5	5	5	5
- Copias de respaldo	5	5	3	4
- Switchers	1	1	5	2
- Router's	1	1	5	2
- Modem	1	1	5	2
- Líneas telefónicas	4	2	3	3
- Central telefónica	4	2	3	3
- Disco duro y grab. (vid)	5	5	3	4
- Cámaras	1	1	5	2
- Teléfonos	4	1	3	3

Análisis y evaluación de riesgos (Ejemplo)

ACTIVOS DE INFORMACIÓN	AMENAZAS	POSIBILIDAD OCURRENCIA	VULNERABILIDADES	POSIBILIDAD QUE AMENAZA PENETRE VULNERABILIDAD	VALOR DE ACTIVOS DE RIESGOS	POSIBILIDAD DE OCURRENCIA DE AMENAZA	TOTAL	CRITICIDAD	OBJETIVOS DE CONTROL	CONTROLES	INDICADOR EFECTIVIDAD CONTROLES
1. BCD DE AHO-CLI	- Virus - Daño físico en el DD	3 5	- Falta de antivirus - Falla técnica	3 4	5	4	20	C	A.3.1 Promocionar dirección gerencial y apoyo a la S.I. A.7.2 Seguridad del equipo: evitar la pérdida, daño o compromiso de los activos y la interrupción de las actividades comerciales. A.8.3 Proteger la integridad del software y la información del daño de software malicioso. A.8.4 Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.	A.3.1.1 A.3.1.2 A.7.2.4 A.8.3.1 A.8.4.1 A.8.4.3	Nº veces/interrupción Nº veces/eventos de seguridad Nº veces/incidentes seguridad
2. Serv. de BDD	- Daño físico en las partes - Virus	3 3	- Falla técnica - Software desactualizado	4 3	5	4	20	C	A.8.3 Proteger la integridad del software y la información del daño de software malicioso.	A.8.3.1	Nº veces/ intentos hacking Nº veces/software dañado
3. Vitales Aho-cli	- Errores de programación/validación/prueba	3	- Mala programación - Mala validación y pruebas	3 4	4	4		C	A.8.2 Minimizar el riesgo de fallas en los sistemas. A.10.1 Asegurar que se incorpore seguridad en los sistemas de información. A.10.2 Evitar la pérdida, modificación o mal uso de la data del usuario en los sistemas de información. A.10.4 Asegurar que los proyectos T.I. y las actividades de apoyo se reducen de manera segura.	A.8.2.1 A.8.2.2 A.10.1.1 A.10.2.1 A.10.2.2 A.10.2.3 A.10.4.1 A.10.4.3	Nº veces/ fallas en sistemas Nº veces/pérdida datos usuario

¡Gracias!

59