

PRINCIPIOS DE GOBIERNO DE LA SEGURIDAD DE TI

GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN



Seguridad y Auditoría

M.A., Inga. Evelyn Lobos



AGENDA

1. ¿Cuál es entonces la importancia del Gobierno de la seguridad de la Información?
2. Incidentes de Seguridad
3. Como entendemos la Seguridad
4. Sistema de Gestión de la Seguridad de la Información
5. Cultura de Seguridad
6. Gobierno de Seguridad
7. Activos de Información
8. Análisis de Riesgos
9. Implementación de Controles
10. Implementación de Mejores prácticas en materia de Seguridad de la Información
11. Ejercicio Práctico.



REFERENCIAS

1. <http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx>
2. <https://www.pmg-ssi.com/2014/04/iso-27014-gobernanza-de-seguridad-de-la-informacion/>
3. <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>
4. <http://iso27000.es/iso27002.html>
5. <https://www.isotools.cl/isoiec-27004/>
6. <https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/>

¿Cuál es entonces la importancia de la Seguridad de la Información?

La creciente dependencia y los sistemas que procesan información, junto con los riesgos, beneficios y oportunidades que esos recursos representan, han transformado al gobierno de la seguridad de la información en una función vital en todo ámbito.




A close-up shot of Thanos, the purple-skinned Titan, looking directly at the camera with a stern expression. He is wearing his dark blue and gold armor. The background is a blurred, war-torn city with smoke and debris, suggesting a scene of destruction.

LOS ATACANTES SE
ACERCAN



Incidentes de Seguridad

Falsifican Sitio de Bi en Línea

 OCTOBER 6, 2009 - AUTHOR: GRAFFISK

Hoy empezó a circular un correo que busca alertar a los usuarios del sitio de BI en Línea del Banco Industrial. Debido que este ha sido clonado por jackers para hacer phishing.

Como medida de seguridad el banco ha enviado estos correos las imágenes adjuntas señalando las diferencias entre los sitios para que ningún usuario se confunda.

Sitio Real y Clonado de Bi en Línea



Hacer clic en imágenes para ver detalles de los sitios.

INCIDENTES DE SEGURIDAD



NOTICIAS

INSTITUCIONES BANCARIAS REPORTAN ALERTAS DE PHISING

El Observatorio Guatemalteco de Delitos Informáticos OGD, mantiene un monitoreo sobre las alertas de distintos tipos de cibercriminales que pueden estar sucediendo en el País, entre los, el tema del phishing, por lo cual hemos visto a varias instituciones bancarias que en sus web informan sobre no caer en la trampa de este delito informático, por lo cual, hay que tomar las medidas necesarias para no ser víctima de este flagelo:

Incidentes de Seguridad

Guatemala

Comunitario Justicia

Supuesto agresor sexual que contactaba por Facebook va a prisión

José Luis Osoy Hernández, de 22 años, detenido por violación con agravación de la pena y plagio o secuestro, fue ligado a proceso y enviado a prisión preventiva por un juez que conoce del caso.

Por JOSÉ MANUEL PATZÁN Y Joel Suncar

24 de febrero de 2016 a las 19:02h

Archivado en:

Facebook Policía Nacional Civil violador



José Luis Osoy Hernández, de 22 años, asiste a la audiencia de primera declaración. (Foto Prensa Libre: Erick Avila)

De acuerdo con la investigación del Ministerio Público, el detenido utilizaba perfiles de mujer en Facebook para captar a jóvenes entre 12 y 17 años para abusarlos sexualmente.



INCIDENTES DE SEGURIDAD

NÓMADA *n*

Redes sociales: una ventana a los delitos sexuales

Las denuncias por acoso y divulgación de fotos íntimas registran un considerable aumento en Guatemala, Honduras y El Salvador en los últimos años. El anonimato y el poder de divulgación atribuidos a los perfiles personales en internet posibilitan la alza.

POR WILLIAN CARBALLO / 28 NOVIEMBRE, 2018

INCIDENTES DE SEGURIDAD

Buscar resultados

EL ROBO DE DATOS ES MÁS COMÚN DE LO QUE PIENSA

El robo o suplantación de identidad es uno de los principales crímenes cibernéticos que afectan al país, tanto a empresas como a usuarios.

Prensa Libre 2 sept. 2018 [+5 más](#) Por Pablo Juárez Andrino prjuarez@prensali-bre.com.gt

Cibercriminales utilizan el método de phishing para estafar a usuarios en páginas, correos y chats

“El sitio era exactamente igual, realmente no había ninguna diferencia con la página oficial del banco”, dijo Gloria —nombre ficticio—, quien recientemente fue víctima de un ataque cibernético

en el que fueron sustraídos Q54 mil de su cuenta bancaria.

Gloria es madre de familia y, al igual que muchas personas en el país, aprovecha la conveniencia de los servicios de banca en línea que ofrecen algunas entidades financieras; sin embargo, en marzo de este año cayó presa de un robo de datos que afectó la estabilidad



económica de su hogar.

“Todo lo manejaba por la app del celular, pero en una oportunidad tenía que hacer una

gestión que no podía llevar a cabo por ese medio. Llamé al call center del banco y se me indicó que debía hacerlo desde una computadora”, refiere

INCIDENTES DE SEGURIDAD

SEGURIDAD

Este es el aparato para clonar tarjetas en centros comerciales

• Por Soy502

26 de septiembre de 2017, 08:09



1/4

Esto localizó la PNC durante los allanamientos. (Foto: PNC)

1

Los allanamientos para desarticular a la estructura

Incidentes de Seguridad



ESP | [AME](#) | BRA | CAT | ENG

NEWSLETTER ✉

[SUSCRÍBETE](#)



≡ EL PAÍS

ESTADOS UNIDOS

[EUROPA](#) [EE UU](#) [MÉXICO](#) [AMÉRICA LATINA](#) [ORIENTE PRÓXIMO](#) [ASIA](#) [ÁFRICA](#) [FOTOS](#) [OPINIÓN](#) [BLOGS](#) [TITULARES »](#)

EE UU lanzó este jueves un ciberataque a Irán autorizado por Trump

La agresión contra sistemas militares y de inteligencia se produjo el mismo día en que el presidente abortó un ataque con misiles por su elevado coste humano



¿NUESTRAS TROPAS ESTAN PREPARADAS?

Deténgase un minuto

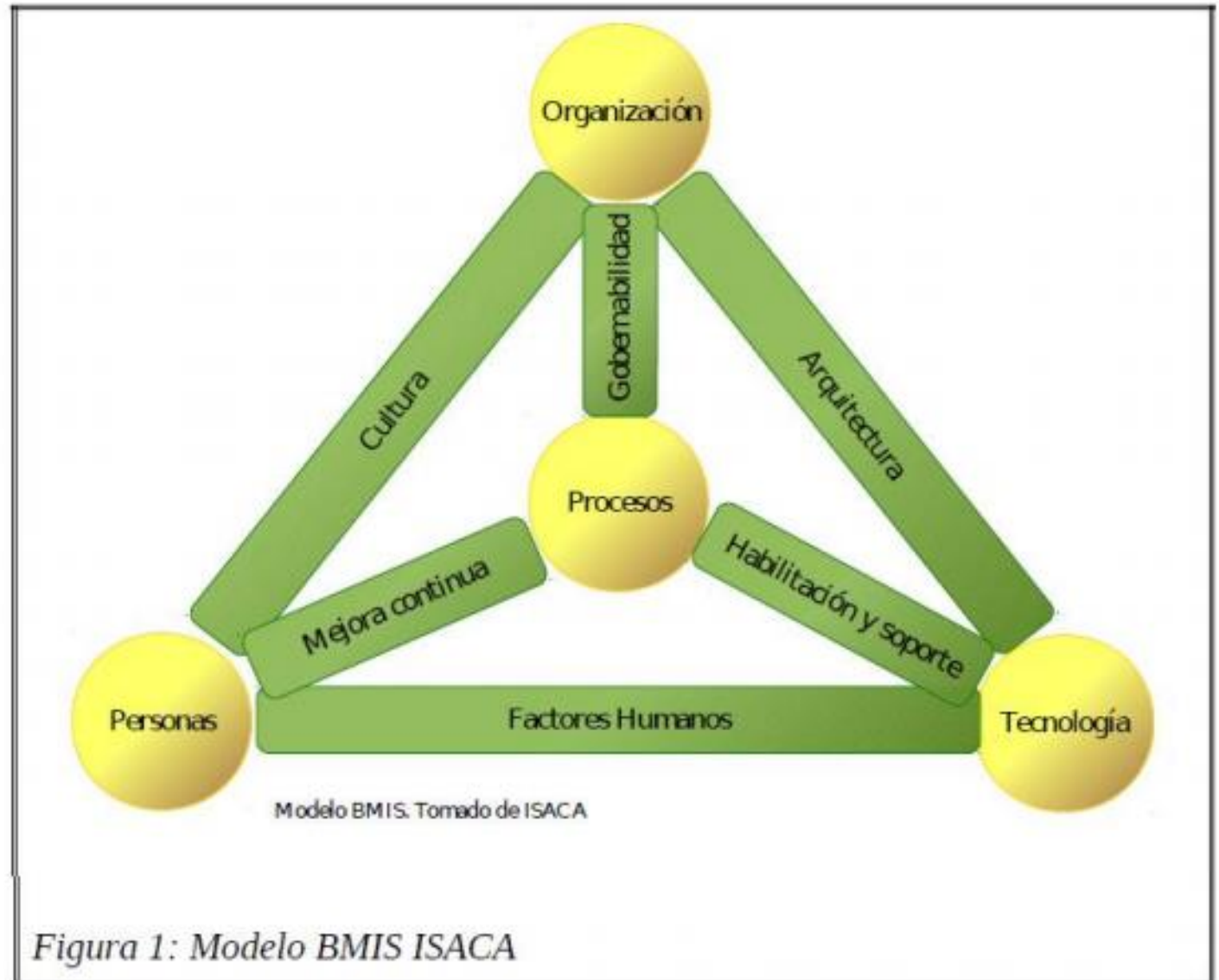
¿Cuál es nuestro aporte en el ecosistema de Seguridad de la información?

A cinematic still from the movie 'The Avengers' showing the main team standing in a modern, brightly lit hallway. From left to right, Iron Man (Robert Downey Jr.), Captain America (Chris Evans), Thor (Chris Hemsworth), Hulk (Mark Ruffalo), and Black Widow (Scarlett Johansson) are visible. Rocket Raccoon is also present, standing in front of Thor. The text '¿Estamos listos para comenzar?' is overlaid in the center of the image.

¿Estamos listos para
comenzar?

COMO ENTENDEMOS LA SEGURIDAD DE LA INFORMACIÓN

II. EL MODELO IBMS



Gobernar para la seguridad



Según conceptualiza Julia Allen, autora de la Guía de CERT (Computer Emergency Response Team), en su tratado “The cert guide to system and network security practices”:

“Gobernar para la seguridad de una empresa significa ver una seguridad adecuada como un requerimiento no negociable de permanecer en el negocio. Para lograr una capacidad sustentable, las organizaciones deben hacer que la seguridad de la empresa sea responsabilidad de los niveles directrices”.



¿CUAL ES EL GIRO DEL NEGOCIO DE LA ORGANIZACIÓN?

Video





COMPRA MAS CAJAS MAGICAS DE HARDWARE Y SOFTWARE, LAS NECESITAS!

Alcance del SGSI



Uno de los requisitos es que estén definidas las metas y la dirección de la organización en lo que respecta a la seguridad de la información.

Cabe destacar que no es suficiente con que la organización haya definido sus metas, sino que también debe considerar las políticas definidas en relación a la seguridad de la información, los requisitos contractuales y normativos y el marco legal en el cual está inmersa.

¿Cuál es nuestro estado actual?



Estado
actual

Estado
deseado

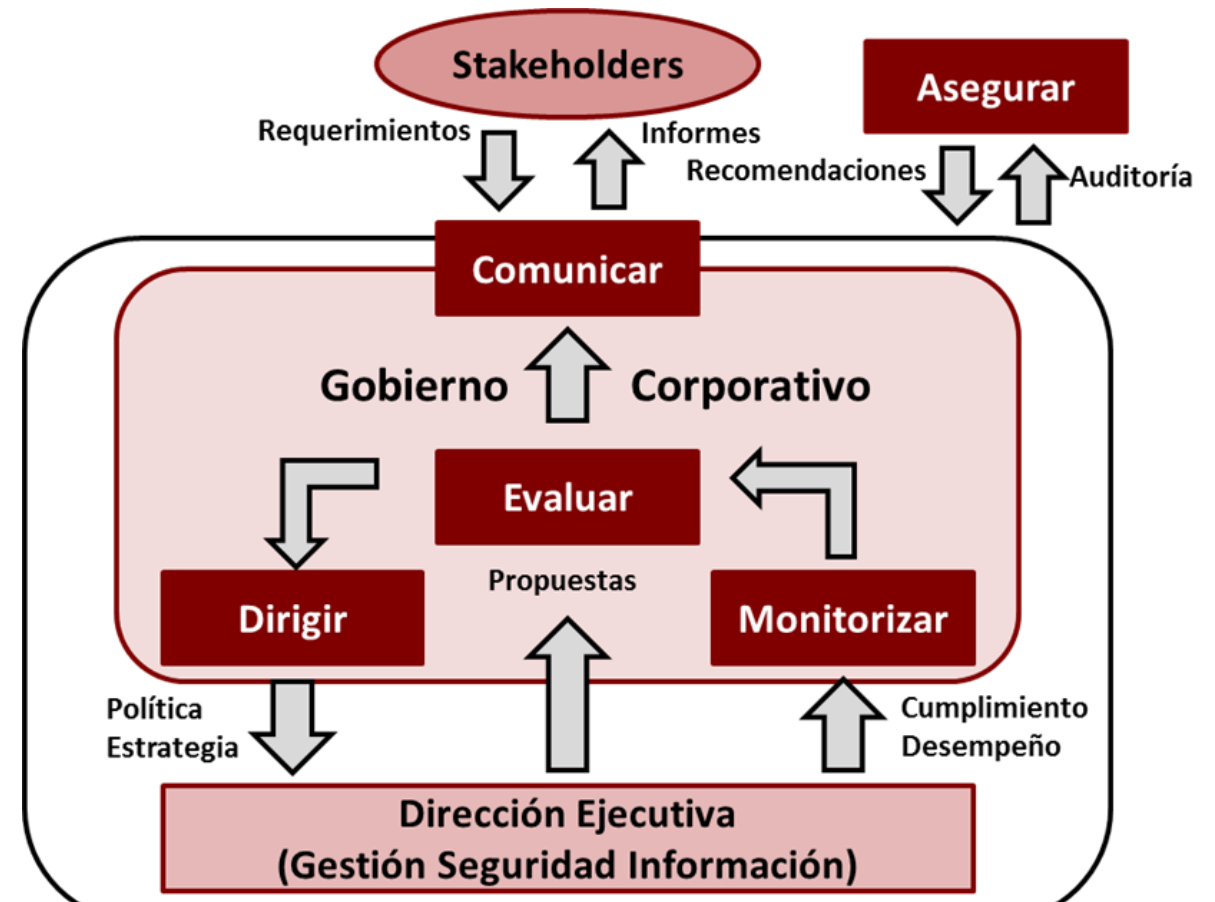
Estado
futuro

¿Cual es nuestra estrategia?

Defina su estrategia con la ayuda de estos seis principios

Referencia ISO 27014

1. Establecer responsabilidad con respecto a la seguridad de la información en toda la organización
2. Adoptar una aproximación basada en el riesgo
3. Establecer la dirección de las decisiones de inversión en seguridad de la información
4. Asegurar conformidad con los requerimientos internos y externos
5. Fomentar un entorno positivo respecto de la seguridad
6. Revisar el rendimiento en relación a los resultados de negocio.



CREE LA CULTURA DE SEGURIDAD

La cultura de seguridad de la información es el factor principal de éxito y el mas complejo, las personas deben ser su foco

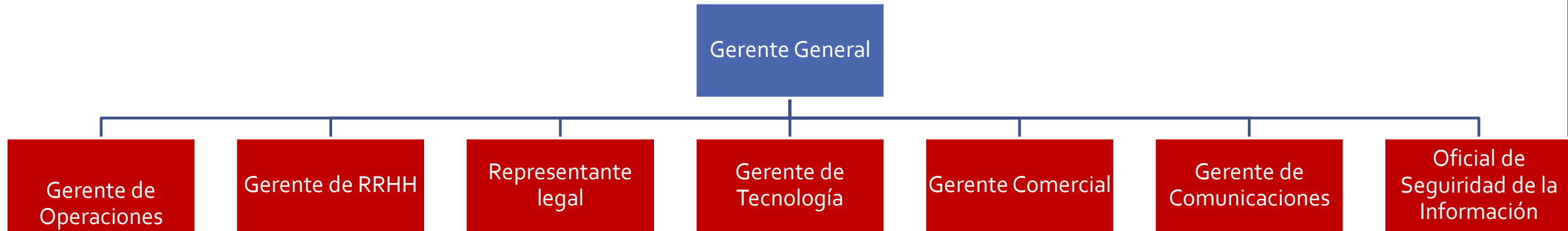


EDUCACIÓN

La cultura de Seguridad de la Información es el factor principal de éxito y el mas complejo, las personas deben ser su foco.



COMITÉ DE LA ORGANIZACIÓN



Objetivo: Alinear la estrategia de Seguridad de la información con los objetivos de negocio

COMITÉ TÉCNICO DE SEGURIDAD



Objetivo: Implementar las medidas necesarias para el fiel cumplimiento del programa de seguridad de la información.

Reflexiona las siguientes preguntas:



¿Identifico qué información sensible debo proteger?

Gobierno de la Seguridad de la Información

El conjunto de responsabilidades y prácticas ejercidas por la junta directiva y la dirección ejecutiva, con la finalidad de brindar una dirección estratégica, garantizar que se logren los objetivos, determinar que los riesgos se administren en forma apropiada y verificar que los recursos de la empresa se utilicen con responsabilidad.

El diagrama muestra tres niveles de gobierno corporativo representados como rectángulos concéntricos. El nivel más externo es un rectángulo rojo con el texto 'Gobierno Corporativo'. Dentro de él está un rectángulo verde con el texto 'Gobierno de TI'. Dentro de este último está un rectángulo blanco con el texto 'Gobierno de Seguridad de la Información'.

Gobierno Corporativo

Gobierno de TI

Gobierno de Seguridad de la
Información

Referencia www.isaca.org/knowledge-center



¿Cuál es entonces la importancia de este gobierno?

Tener en cuenta que las tecnologías de la información mejoran sensiblemente las posibilidades de negocio, con lo cual su seguridad añade un valor significativo al momento de minimizar riesgos y, consecuentemente, disminuir pérdidas derivadas de eventos relacionados a la seguridad.

¿Cuál es entonces la importancia de este gobierno?



No es suficiente con transmitir a los empleados de las organizaciones los objetivos, misiones y visiones y pautar las condiciones que conllevan al éxito, sino que además se debe comunicar cómo se va a proteger la propia existencia de su negocio.

Gobierno de la Seguridad de la Información



El gobierno de la seguridad de los activos de información (en adelante gobierno de la seguridad de la información) debe ser una parte integrante y transparente del gobierno global de las empresas u organizaciones, con el fin de tener continuidad en sus negocios.

INFORMACIÓN



La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada.

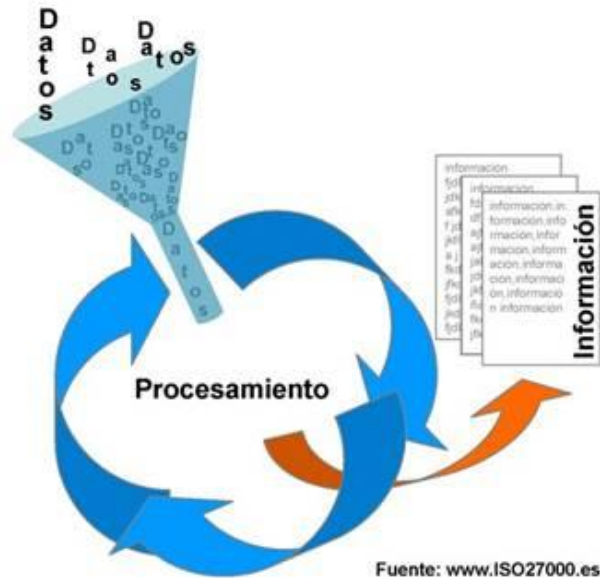
La información puede estar:

1. Impresa o escrita en papel.
2. Almacenada electrónicamente.
3. Transmitida por correo o medios electrónicos
4. Mostrada en filmes.
5. Hablada en conversación.

Debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparte o almacene.

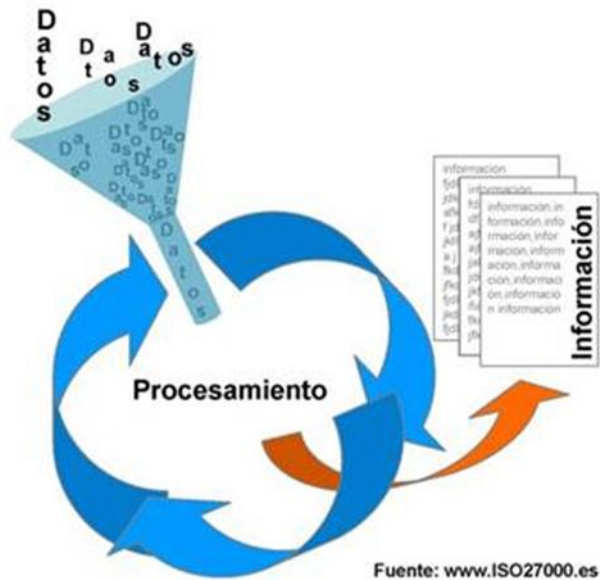
Clasificación de los activos de Información 1/3

❑ Si suponemos que la información relevante que existe en la organización no está debidamente identificada y catalogada, entonces no queda mejor alternativa que clasificarla.



❑ Esto se hará en función a su sensibilidad y criticidad. Se considera que una información es sensible cuando su divulgación no autorizada pueda ocasionar un severo impacto en la organización

Clasificación de los Activos de Información 2/3



En las grandes organizaciones clasificar los activos de información significa una tarea de enormes proporciones y un esfuerzo sustancial de muchos recursos. De no hacerlo, los costos asociados a la protección de esos activos crecerán de manera exponencial, al tiempo que aumentará la dependencia de la información. Por lo tanto, no hay mejor estrategia que realizar una clasificación.

Clasificación de Activos de Información 3/3



En ciertos casos, las organizaciones definen los activos pero no se identifican las amenazas a éstos, ni las debilidades que pudieran ser aprovechadas por dichas amenazas.

Gobierno de la Seguridad de la Información

Activos de Información

Datos Digitales: Base de datos copias de Seguridad, claves, Información en office

Activos tangibles: correo, fax, llaves, libros

Activos Intangible: Patentes, conocimientos, relaciones

Software

Activos Físicos

Infraestructura de TI, edificios, oficinas, armarios

Hardware de TI: Estaciones de trabajo, portátiles

Activos de servicios de TI

Servicios de autenticación, servicios de red

Activos Humanos

Empleados

Proveedores

Activos

Primarios

De soporte

Datos o información que se manipula dentro de la organización

Servicios



Software



Hardware



Redes de comunicaciones



Recurso humano



Sitios



Procesos que soportan la organización

Soportes de información



Equipamiento auxiliar



Instalaciones o infraestructura física



Bienes intangibles



Para gestionar correctamente los activos de información



- ☐ Un buen gobierno de SI realiza evaluaciones por lo menos anuales de la seguridad que los protege.
- ☐ Realizarse periódicos análisis de riesgos y existir políticas que sean revisadas periódicamente.
- ☐ Los procesos y procedimientos deben estar basados en esas evaluaciones de riesgos.
- ☐ La seguridad de los activos de información forma parte integral del ciclo de vida de los sistemas, probar los sistemas de control y protección de esos activos, y prevenir para asegurar una continuidad de las operaciones y, por ende, la continuidad de la organización en el negocio

Lo que hay que proteger son los activos de información.

1. Los activos de información deben conocerse con un alto grado de precisión, y esto comúnmente no ocurre en la mayoría de las organizaciones.
1. Que significa proteger un activo de información; dado que este concepto es entendido por cada persona en términos generales, se torna mucho más complejo cuantificar qué activos requieren protección, cuánta y contra qué.



Reflexiona las siguientes preguntas:



2. ¿Conozco las consecuencias de la pérdida de datos sensibles?

Gestión de Riesgos



Tipos de amenazas

Amenazas Operacionales

Amenazas Humanas

Amenazas a Instalaciones

Amenazas Sociales

Amenazas Tecnológicas

Amenazas Naturales



Análisis de riesgo

Al realizar el análisis de riesgo se cuenta con una gran cantidad de información que con frecuencia no es bien interpretada, de allí la importancia de la herramienta a usar. Para que el proceso de tratamiento de los riesgos sea efectivo, es preciso que esté basado en un completo análisis de riesgo.

La información permitirá decidir cuál es el nivel de riesgo que se aceptará, qué riesgos serán tratados y cuál será el tratamiento para esos riesgos.



Análisis de riesgos

Esto implica la necesidad de definir un paquete de medidas que hagan posible controlar y tratar los riesgos.



La norma ISO/IEC 27001 en su anexo A define objetivos de control y controles para el tratamiento de los riesgos.

Estos controles no serán suficientes si no cubren todos los requisitos de seguridad de la información que definió la organización, por lo tanto es responsabilidad de la organización verificar si debe definir controles adicionales.

¿Por qué debemos identificar riesgos y medir su impacto?



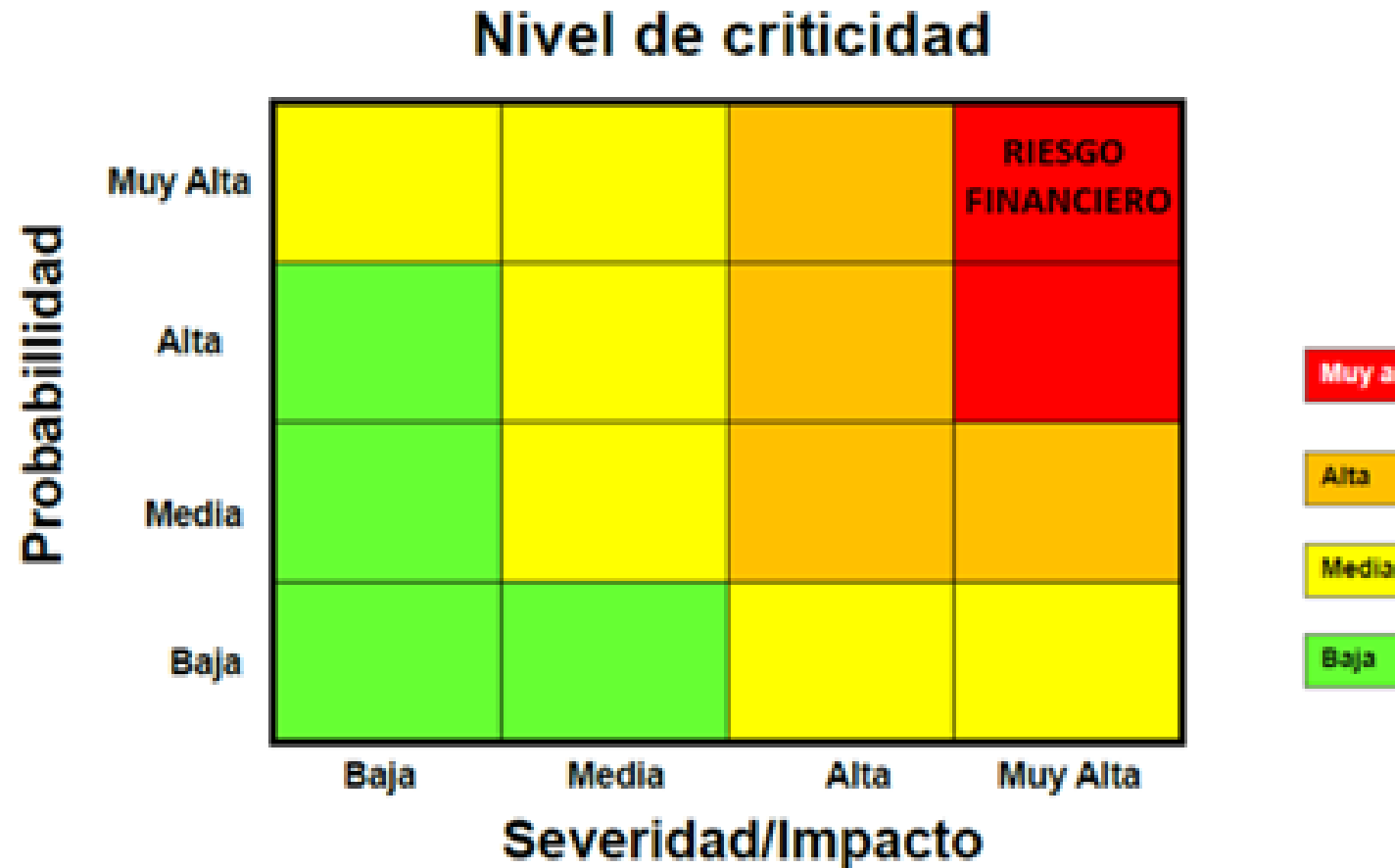
Dentro de una organización, el tema de la seguridad de la información es un punto importante tal que es necesario dedicar tiempo y recursos. Por esta razón, una organización debe crear un Sistema de Gestión de la Seguridad de la Información (SGSI), con el objetivo de salvaguardar la información, una vez identificados los “activos de información” que deben ser protegidos y en qué grado.

¿Por qué debemos identificar riesgos y medir su impacto?



- La seguridad es un proceso que nunca termina, ya que los riesgos no se eliminan completamente. Por ello es necesaria una adecuada gestión de la seguridad de la información, para contribuir a disminuir los riesgos que la institución soporta, y a minimizar los daños en los activos de información, en caso de que los riesgos lleguen a materializarse.
- Por tal motivo, es importante que la institución implemente el SGSI, ciclo repetitivo de cuatro niveles: Planificar, Hacer, Verificar y Actuar.

Nivel de criticidad



Oficial de la Seguridad de la Información

Se espera que sean de dominio del oficial de la seguridad de la información para que éste pueda implementar un gobierno efectivo y contemple el conjunto de las funciones que se requieren.

Entre los principales conceptos que debe conocer y manejar un gerente de seguridad de la información, se hallan los siguientes:



Seguridad de la Información



❑ **Confidencialidad:** preservación de la información dentro de los ámbitos de conocimientos definidos y autorizados.

❑ **Integridad:** permite asegurar que la información no es modificada sin autorización.

❑ **Disponibilidad:** tan importante como cuidar de su confidencialidad e integridad. Contar con la información en forma oportuna puede llegar a transformarse en la diferencia entre la continuidad y discontinuidad del negocio.

Objetivos del programa de seguridad de la información

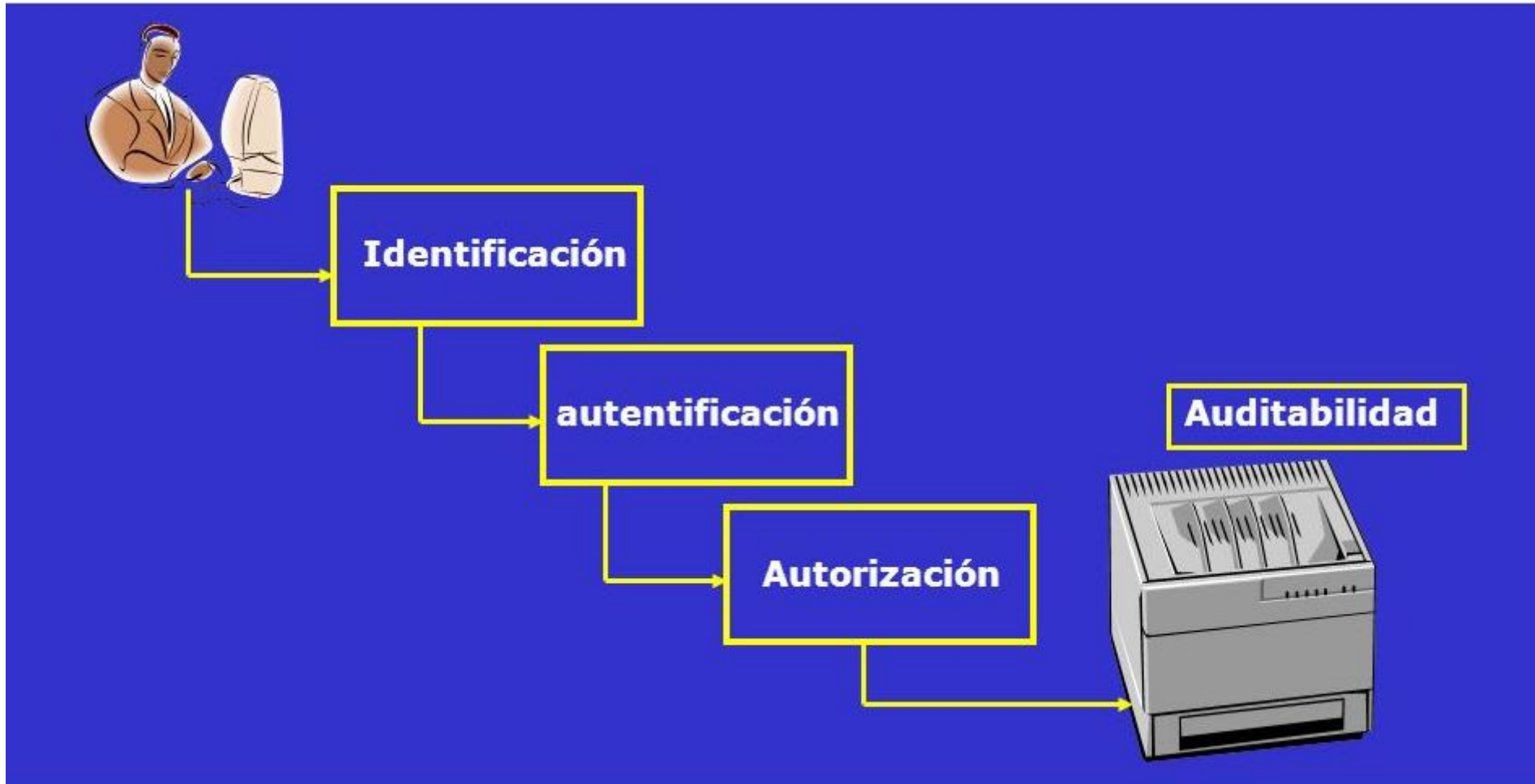
Para la mayoría de las organizaciones, el objetivo de la seguridad se cumple cuando:

La información está disponible y se puede utilizar cuando se le requiere, y los sistemas que la proporcionan pueden resistir ataques en forma apropiada (disponibilidad)

La información se divulga sólo a aquellos que tengan derecho a conocerla y sólo puede ser observada por ellos (confidencialidad)

La información está protegida contra modificaciones no autorizadas (integridad) Se puede confiar en las transacciones de negocio y en el intercambio de información entre locaciones de la empresa o con socios (autenticidad y no repudio)

Accesos a la información





No repudio

No hay una única formula
para establecer controles
adecuados

**NIST
(800-53 Rev 3)**

Propone un catálogo de 20 grupos de control de seguridad y privacidad para ayudar a las agencias y organizaciones federales de los EE.UU.

PCI-DSS

Describe 12 puntos de seguridad para implementar mejores prácticas para organizaciones que procesan y almacenan detalles de tarjetas de pago.

**SANS
(20 CIS Critical
Security Controls)**

Describe 20 controles de seguridad críticos proporcionando un enfoque prioritario y bastante técnico para obtener resultados inmediatos de alto impacto.

ISO/IEC 27001:2013

Presenta un enfoque menos técnico basado en la gestión de riesgos. Proporcionando recomendaciones en seis fases definidas.

No hay una forma
única
de establecer
controles

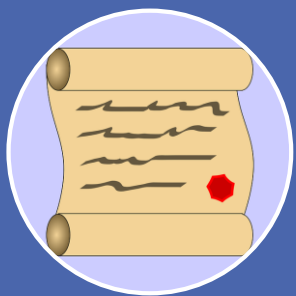
CoBIT v5
Control Objectives
for Information and
related Technology

Es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI).

MGCTI
Manual de Gobierno
y Control de
Tecnologías de
Información

Ha sido elaborado con el objetivo de ofrecer un framework común para Entidades Financieras, fiscalizadas por el Banco Central del Paraguay. Integra: CoBIT, ISO 27001, COSO, ITIL, Prince.

Política de seguridad y privacidad de la Información



Políticas de seguridad
y privacidad de la
Información



Compendio de
políticas
complementarias de
seguridad y privacidad
de la Información



Políticas de gestión de
incidentes



Política de
tratamiento de datos
personales



Que necesitamos conocer como administrador de la seguridad de la Información

Firewalls

- Administración de cuentas de usuarios

Sistema antivirus

- Herramientas anti spam

Sistemas de identificación (biometría, tarjetas de proximidad y otros)

- Encriptación

Que necesitamos conocer como administrador de la seguridad de la Información

Firma digital

- Redes privadas virtuales

Análisis forense

Tecnologías de monitoreo

Accesos remotos seguros

Sistema de gestión de Seguridad de la Información

Se lleva a cabo de manera consistente el análisis de impacto y riesgo de seguridad de la información.

Las políticas y las prácticas de seguridad se completan con niveles mínimos específicos de seguridad.

Las sesiones de concienciación sobre la seguridad se han vuelto obligatorias.

La identificación, autenticación y autorización de usuarios se han homologado.

Se ha establecido la certificación de seguridad del personal.

Las pruebas de intrusos son un proceso establecido y formalizado que conduce a mejoras.



Los fundamentos de un programa de seguridad de la información son:

- ❑ La estrategia de seguridad
- ❑ El plan de acción
- ❑ El programa es, en esencia, el plan de proyecto para implementar y establecer gestión en curso de alguna parte o partes de la estrategia.

Aplicar las mejores prácticas en materia de seguridad de la información



Alinearse a la norma internacional ISO/IEC 27001.

Esta norma ha sido elaborada para constituir un sistema o modelo para la implementación, operación, seguimiento, revisión, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.



Aplicar las mejores prácticas en materia de seguridad de la información

La norma ISO/IEC 27002 (nueva versión de la ISO/IEC 17799) constituye un código de buenas prácticas para la gestión de la seguridad de la información; complementaria de la anterior, aporta los requisitos para la implantación de aquélla.



Aplicar las mejores prácticas en materia de seguridad de la información

La norma ISO/IEC 27004 provee guías para el desarrollo y uso de medidas y mediciones, con el objetivo de evaluar la efectividad de un sistema de gestión de seguridad de la información.

Aplicar las mejores prácticas en materia de seguridad de la información

ISO 27005 RISK MANAGER

La norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos de la Seguridad de la Información en una organización en apoyo a la aplicación de los requisitos planteados en la ISO/IEC 27001.

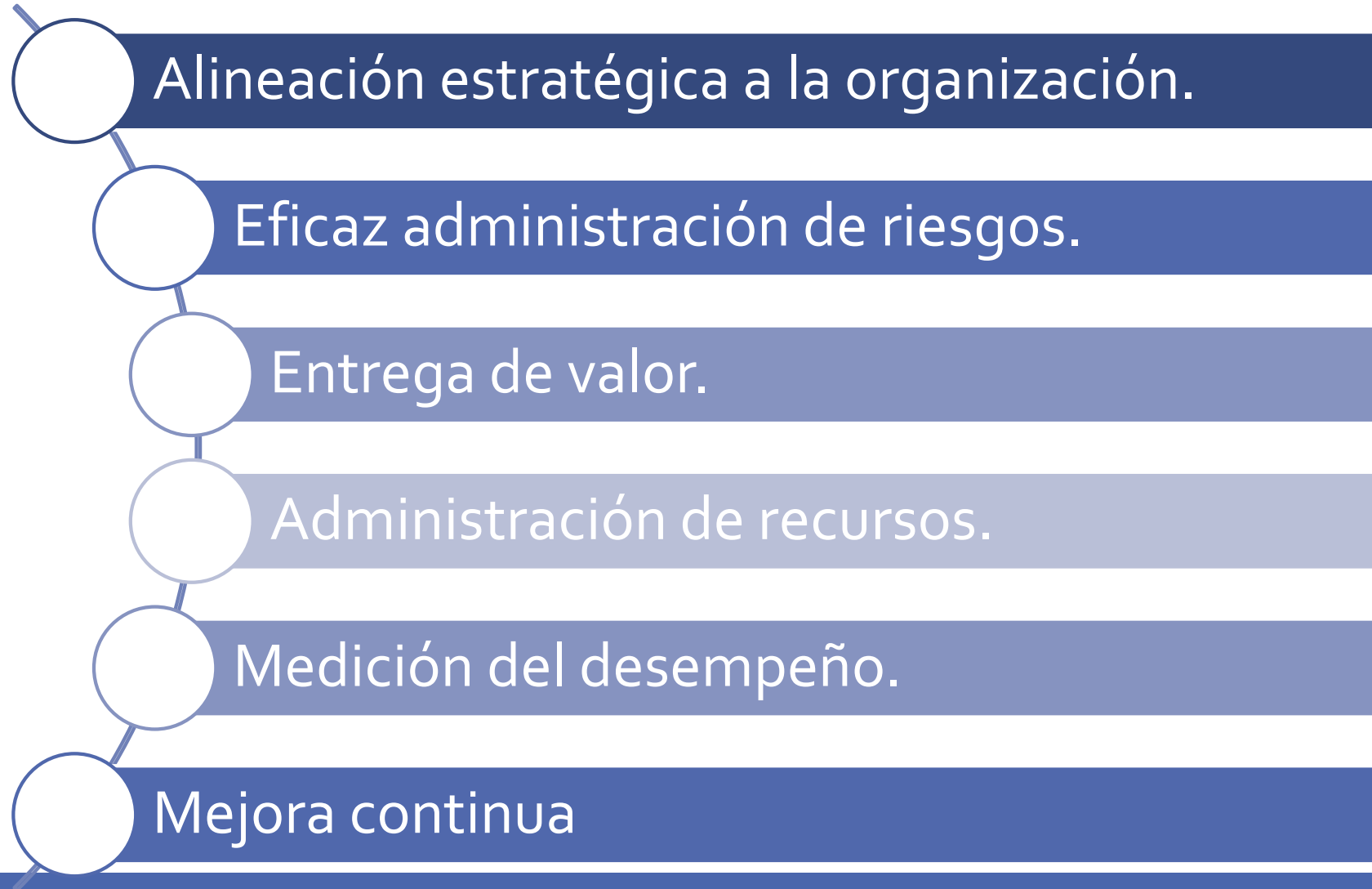
En particular, esta última adopta un enfoque basado en procesos para el desarrollo de un Sistema de Gestión de Seguridad de la Información.



Aplicar las mejores prácticas en materia de seguridad de la información

El modelo denominado PDCA (Plan, Do, Check, Act) es aplicado para estructurar todos los procesos del sistema de gestión.

Cualquiera sea la estrategia de seguridad adoptada, los objetivos fundamentales consisten en:



Conclusión

Hoy en día las organizaciones dependen en gran medida de su tecnología y sus activos de información.

Por lo anterior, impera una protección adecuada a las informaciones importantes. Seguridad no es un producto, es un proceso que debe ser administrado.



EJERCICIO

Establezca 10 puntos de como su empresa en el gobierno de la seguridad identifica y cumple con los requerimientos regulatorios de su país.

1. USA
2. PANAMA
3. COSTA RICA
4. REPUBLICA DOMINICANA
5. CHILE
6. UNIÓN EUROPEA
7. GUATEMALA
8. MEXICO



GRACIAS!!
