# Sistema de Gestión de Seguridad de la Información

Ms. Ing. Miguel Martín Calderón Su Nóbrega

PMP®, TOGAF ®, BPM®, RUP®

Universidad Nacional Mayor de San Marcos

## ¿Qué es un SGSI?

- SGSI – Sistema de Gestión de Seguridad de la Información es el concepto core sobre el cual se desarrolló la norma ISO 27001 (en inglés ISMS – Information Security Management System).

**Procesos sistemático, documentado y conocido por toda la organización**

**Busca garantizar un adecuado nivel de protección de la información , sensibilizando a la organización respecto de los riesgos asociados a esta.**

**Todo riesgo debe ser conocido, asumido, gestionado y minimizado.**

**La implementación del SGSI debe ser documentada de forma sistémica, estructurada, repetible eficiente y adaptable a los cambios que se produzcan.**

# ¿Qué es la Información?

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas, lo cual debe estar alineado con los demás sistemas de gestión.

Con la política se contribuye a gestionar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

La institución define los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información.



# ¿Qué es la Información?

# Protección de la Información

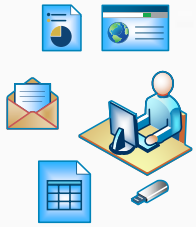
- "Cualquiera que sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe estar protegido en forma adecuada" (ISO-IEC 27002)



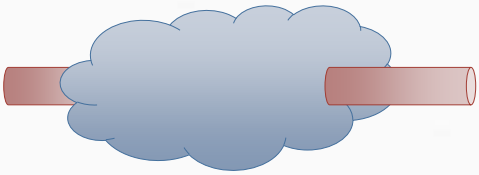

# Protección de la Información

- No existe la "verdad Absoluta" en seguridad informática
- No es posible eliminar todos los riesgos
- No se puede contar con un especialista en todos los temas
- La Dirección está convencida que la Seguridad Informática no haga al negocio de la compañía
- Cada vez los riesgos y el impacto en los negocios son mayores

# Garantizar en la Información



Privacidad
Autenticación
Gestión de Usuarios



Disponibilidad
Escalabilidad
Rendimiento
No Repudio
Confidencialidad
Validez Legal

Seguridad Perimetral
Seguridad en las Aplicaciones
Continuidad de Negocio
Seguridad Física
Auditorías
Gestión de Sistemas
Gestión de Incidencias
Monitorización
Integridad



# ¿Contra qué se debe proteger la Información ?

**Orden fortuito**

- **Destrucción**
- **Incendio**
- **Inundaciones**

**Orden deliberado**

- **Fraude**
- **Espionaje**
- **Sabotaje**
- **Vandalismo**

# Tipificación de Amenazas

| | |
|---|---|
| **Accidentes** | • **Averías, Catástrofes, Interrupciones** |
| **Errores** | • **de Uso, Diseño, Control** |
| **Intencionales Presenciales** | • **Atentado con acceso físico no autorizado** |
| **Intencionales Remotas** | • **Requieren acceso al canal de comunicación** |



# Intencionales Remotas

- **Interceptación pasiva de la información (amenaza a la CONFIDENCIALIDAD)**
- **Corrupción o destrucción de la información (amenaza a la INTEGRIDAD)**
- **Suplantación de origen (amenaza a la AUTENTICACIÓN)**

# ¿Qué es la Seguridad de la Información?




# ¿Qué es el Estándar ISO 2700X?

| | |
|---|---|
| ISO/IEC 27000 | • Sistema de Gestión de Seguridad de la Información: Revisión y vocabulario |
| ISO/IEC 27001 | • Sistema de Gestión de Seguridad de la Información: Requerimientos |
| ISO/IEC 27002 | • Guía para los controles de Seguridad de la Información |
| ISO/IEC 27003 | • Guía de implementación de los Sistemas de Gestión de Seguridad de la Información |
| ISO/IEC 27004 | • Gestión de la Seguridad de la Información: Mediciones |
| ISO/IEC 27005 | • Gestión del Riesgo de la Seguridad de la Información |
| ISO/IEC 27006 | • Requisitos para los organismos que realizan la auditoría y certificación de sistemas de gestión de seguridad de la información |
| ISO/IEC 27007 | • Directrices para la auditoría de sistemas de gestión de seguridad de la información |

# ¿Qué es el Estándar ISO 2700X?

| | |
|---|---|
| ISO/IEC TR 27008 | • Directrices para los auditores, sobre los controles de seguridad de la información. |
| ISO/IEC 27010 | • Gestión de seguridad de la información para las comunicaciones intersectoriales e inter-organizacionales. |
| ISO/IEC 27011 | • Directrices de gestión de seguridad de información para las organizaciones de telecomunicaciones basados en la norma ISO / IEC 27002. |
| ISO/IEC 27013 | • Guía para el desarrollo integrado de la norma ISO / IEC 27001 e ISO / IEC 20000-1. |
| ISO/IEC 27014 | • Gobernanza de seguridad de la información |
| ISO/IEC TR 27015 | • Directrices de Gestión de Información para los Servicios Financieros |
| ISO/IEC TR 27016 | • Gestión de Seguridad de la Información - Economía Organizacional |
| ISO27799: 2008 | • Información en Campo de la Salud - Información de Gestión de Seguridad en Salud utilizando ISO / IEC 27002 |



# Paradigmas en la implementación de un SGSI

Control de las actividades de las personas.

¿Control sobre las intenciones de las personas?

# Enfoque del SGSI

- Diferencial el "¿Qué se debe hacer?" del "¿Cómo se debe hacer?"
- Establecer Acuerdos, Responsables y Fechas de Compromiso

**¿Cómo Implementar las Buenas Prácticas?**

- Habilidades Rígidas
- Habilidades Blandas

**¿Cómo asegurar que las personas son las indicadas?**

- Predisposición
- Relación interdepartamental
- Armonía, no disonancia

**¿Cómo aseguramos los ámbitos?**

- Documentación
- Diagramación de Procesos
- Relación entre Procesos

**¿Cómo aseguramos que se haga lo que se requiere?**



# ¿Por qué aumentan las amenazas?

- Las Organizaciones son cada vez mas dependientes de sus Sistemas y Servicios de Información, por lo tanto podemos afirmar que son cada vez mas vulnerables a las amenazas concernientes a su seguridad.
- El costo de la información el mayor al costo de los dispositivos que la pueden almacenar y permiten la ventaja de una organización frente a otra.

**Crecimiento exponencial de las Redes y Usuarios Interconectados**

**Profusión de las BD On-Line**

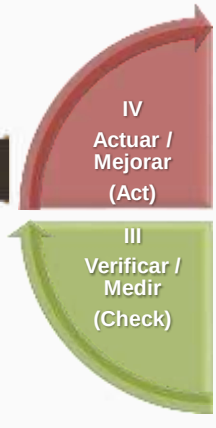
**Inmadurez de las Nuevas Tecnologías**

**Alta disponibilidad de Herramientas Automatizadas de Ataques**

- Nuevas Técnicas de Ataque Distribuido (Ej:DDoS)

**Técnicas de Ingeniería Social**

# Implementación del SGSI




Establecer los lineamientos del SGSI pertinentes a la gestión de riesgo y mejorar la seguridad de la información para obtener resultados alineados con los objetivos organizacionales.

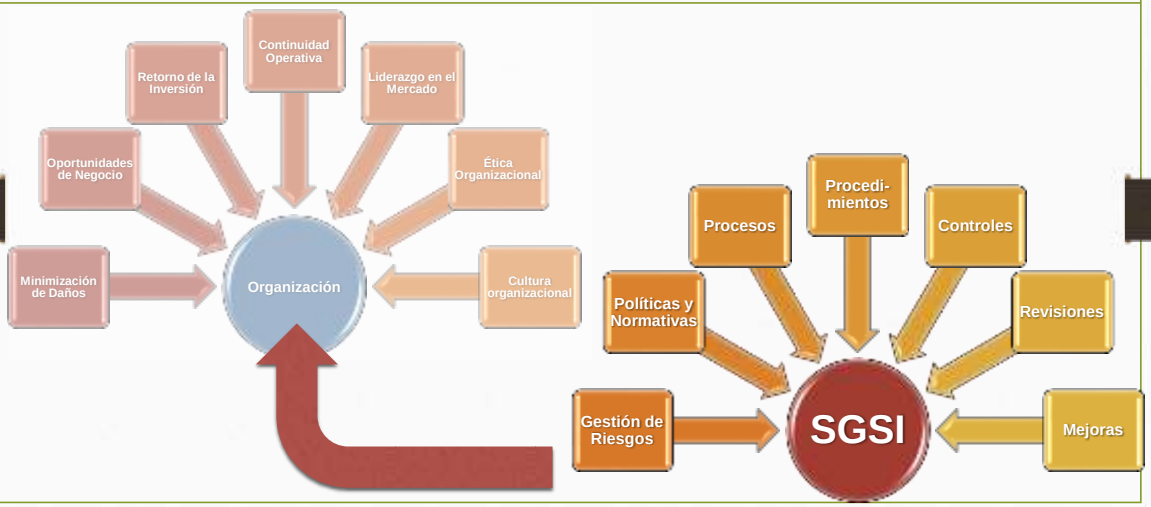
Implementar y operar la política, controles, procesos y procedimientos definidos en la planificación del SGSI.

Evaluar y medir el rendimiento del proceso contra la política del SGSI, sus objetivos y experiencia práctica e informar los resultados para gestionar su revisión.

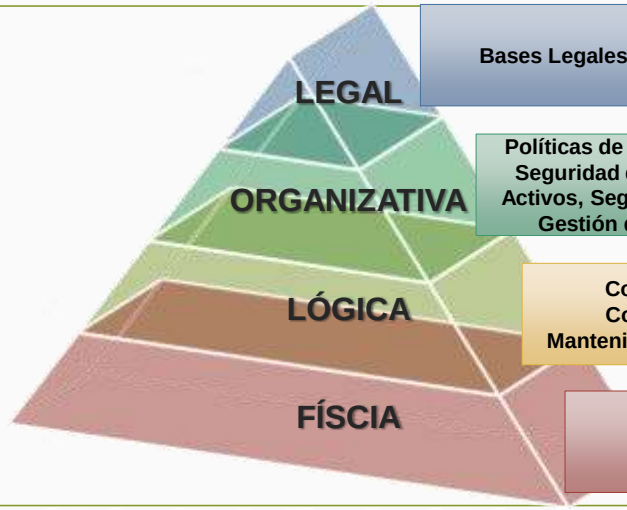
Tomar acciones preventivas y correctivas, basadas en los resultados de auditorías internas del SGSI y de revisión de gestión u otra información relevante para lograr la mejora continua del SGSI.



# Enfoque de la Implementación



# Niveles de Aseguramiento del SGSI




**Bases Legales, constitución Política**

**Políticas de Seguridad, Organización de la Seguridad de la Información, Gestión de Activos, Seguridad de Recursos Humanos, Gestión de Incidentes de Seguridad**

**Control de Accesos, Gestión de Comunicaciones, Adquisición y Mantenimiento de sistemas de Información**

**Seguridad Físico Perimetral**



# Políticas, Estándares y Procedimientos

- Conjunto de requisitos definidos por los responsables directos o indirectos de un Sistema que indica en términos generales qué está permitido y qué no lo está en el área de seguridad durante la operación general de dicho sistema

| | |
|---|---|
| **Política** | • **El porqué una organización protege la información** |
| **Estándares** | • **Lo que la organización quiere hacer para implementar y administrar la seguridad de la información** |
| **Procedimientos** | • **Cómo la organización obtendrá los requerimientos de seguridad** |

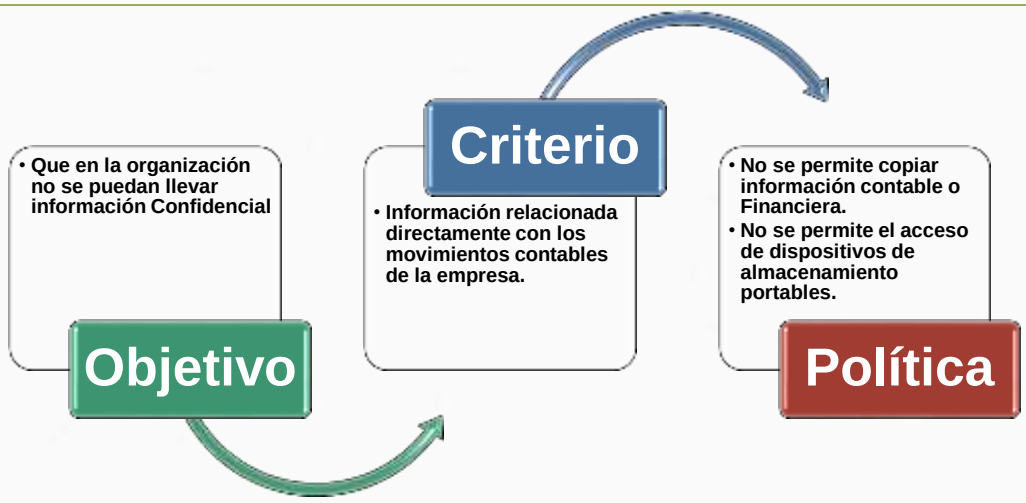
# Alcance del SGSI

- Protección de los datos y la privacidad de la información
- Protección del registro de la información
- Derechos de propiedad intelectual
- Documentos de la política de seguridad de la información
- Asignaciones de responsabilidades de los colaboradores
- Sociabilización de la Seguridad de la Información
- Identificación de vulnerabilidades técnicas
- Gestión de Incidentes de Seguridad
- Gestión de Continuidad operativa



# Enfoque de Alcance del SGSI

# ¿Cómo Definir las Políticas?





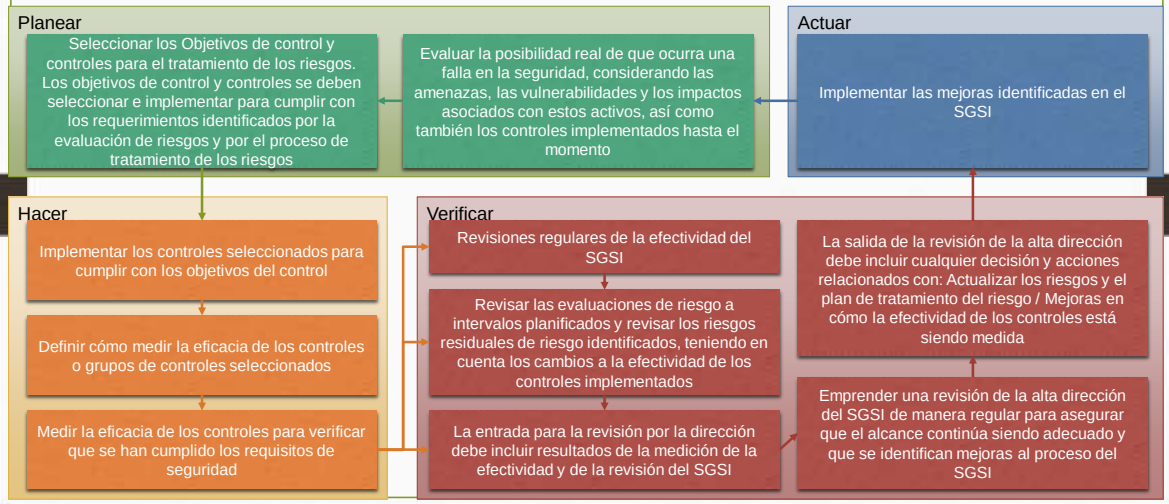

# Identificación de Roles Claves

- Comité de Seguridad de la Información
- Oficial de Seguridad de la Información
- Equipo de Aseguramiento de la Calidad
- Auditores Internos en Calidad y Seguridad de la Información

# Análisis Resumido de la Norma ISO2700X



# Aplicación de la norma sobre el ciclo de Deming

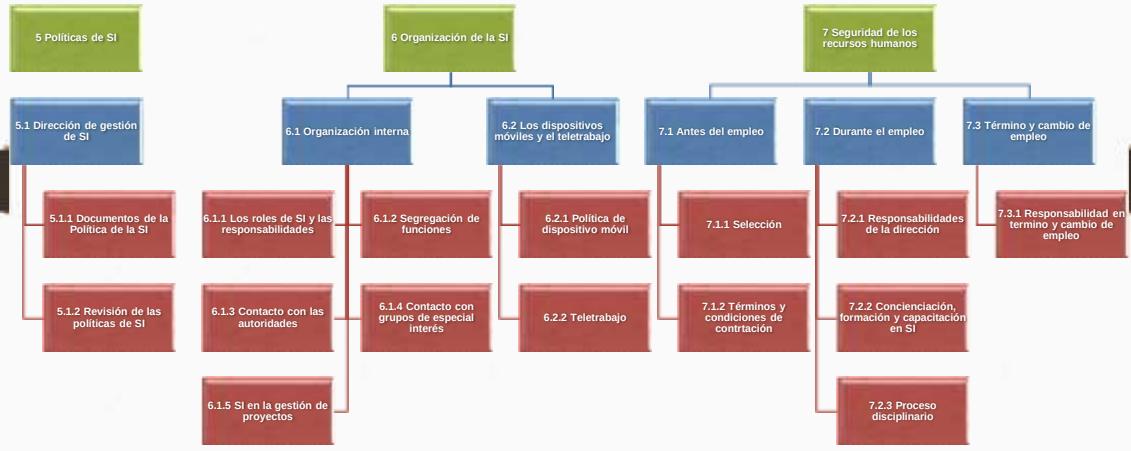


# ISO 27001:2013 - Dominios

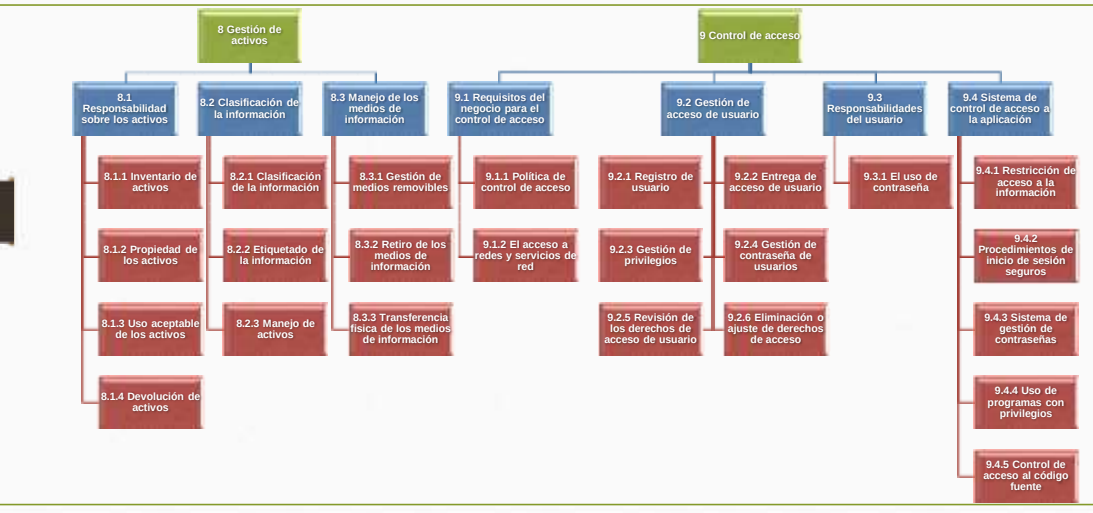
- A.5 Políticas de Seguridad
- A.6 Organización de la Seguridad de la Información
- A.7 Seguridad de los RR.HH.
- A.8 Gestión de Activos
- A.9 Control de Accesos
- A.10 Criptografía
- A.11 Seguridad Física y Ambiental
- A.12 Seguridad de las Operaciones
- A.13 Transferencia de Información
- A.14 Adquisición de Sistemas, Desarrollo y Mantenimiento
- A.15 Relación con Proveedores
- A.16 Gestión de los Incidentes de Seguridad
- A.17 Continuidad de Negocio
- A.18 Cumplimiento con los requerimientos legales y contractuales



# ISO 27002:2013 - Controles

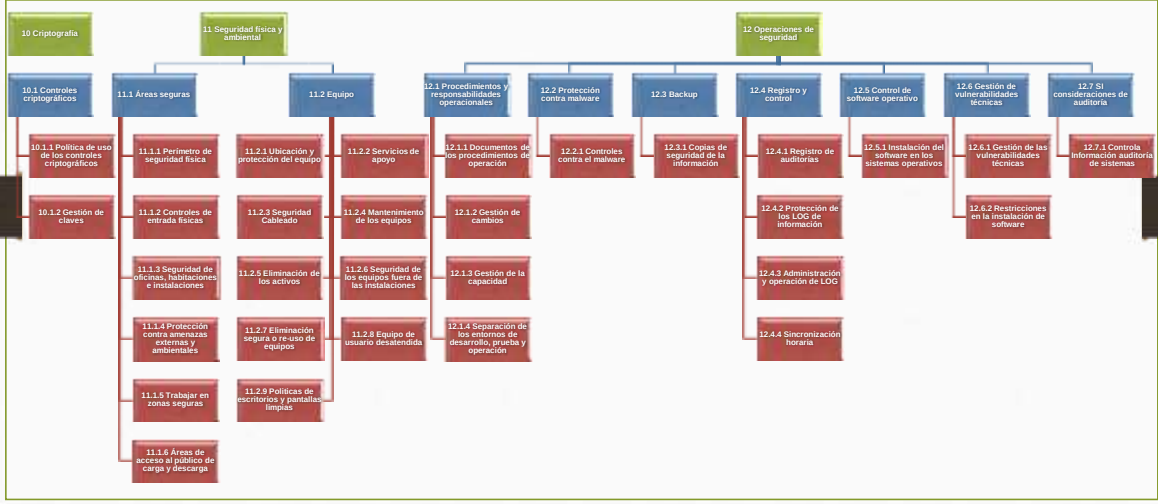


# ISO 27002:2013 - Controles

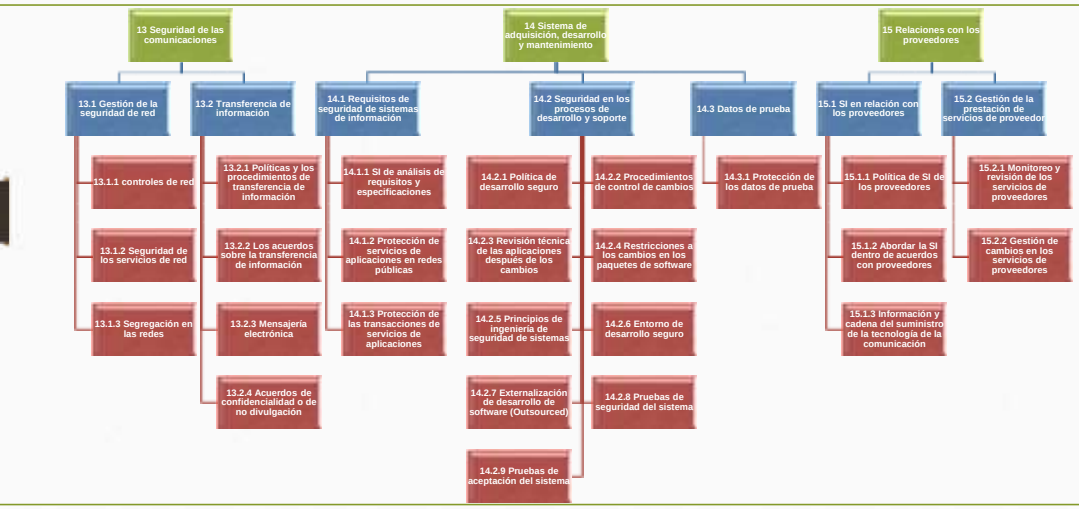





# ISO 27002:2013 - Controles

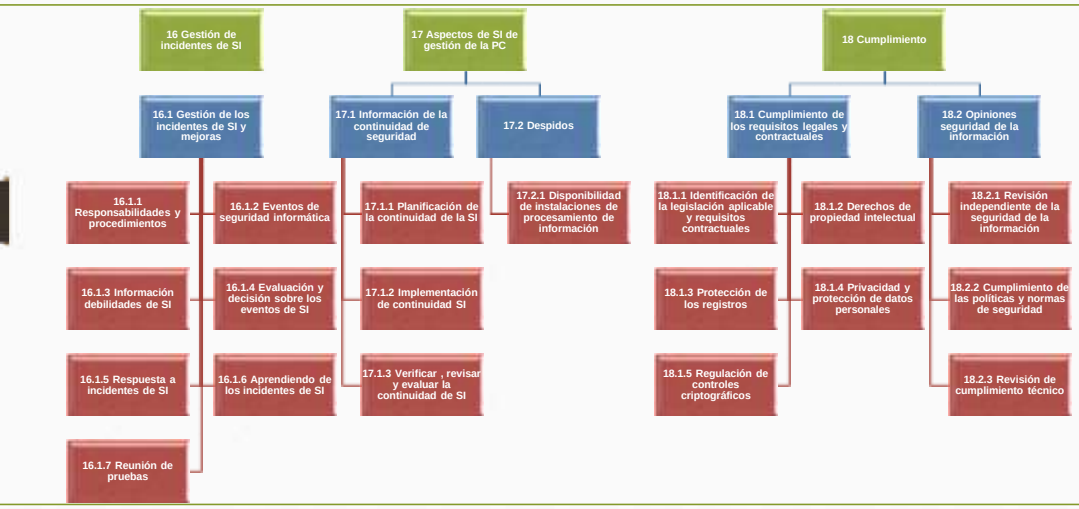


# ISO 27002:2013 - Controles






# ISO 27002:2013 - Controles



# ISO 27004: Medición

- Esta norma provee una guía en el desarrollo y uso de medidas y mediciones, de manera de evaluar la efectividad de un Sistema de Gestión de Seguridad de la Información (SGSI) implementado y de los controles o grupos de controles, como los especificados en la ISO/IEC 27001.

- OBJETIVOS
  - Evaluar la efectividad de los controles o grupos de controles implementados
  - Evaluar la efectividad del SGSI implementado Verificar el grado de cumplimiento de los requerimientos de seguridad identificados
  - Facilitar la mejora del desempeño de la seguridad de la información en términos de los riesgos generales de negocio de la organización
  - Proveer resultados de las mediciones para asistir a la revisión por la alta dirección y facilitar la toma de decisiones relacionada con el SGSI y justificar las necesidades de mejoras del SGSI implementado



# ISO 27004: Medición

# ISO 27004: ¿Qué Puedo Medir?

- Rendimiento de los controles implementados en el SGSI
- Estado de los activos de información protegidos por los controles
- Rendimiento de los procesos implementados en el SGSI
- Comportamiento del personal que forma par-te del SGSI implementado
- Actividades de las unidades organizacionales responsables por la seguridad de la información
- Grado de satisfacción de las partes interesadas



# ISO 27004: ¿Cuál puede ser la fuente de la Medición?

- Resultados de la evaluación y el análisis de riesgos
- Cuestionarios y entrevistas personales
- Reportes de auditoría internos y/o externos
- Registros de eventos, tales como eventos del sistema, reportes estadísticos y pistas de auditorías
- Reportes de incidentes, particularmente aquellos de mayor impacto
- Resultados de pruebas, por ejemplo: pruebas de penetración, ingeniería social, herramien-tas de cumplimiento y de auditoría de seguridad;
- Registros de la seguridad de la información de la organización relacionados con los procedimientos y los programas

# ISO 27004: Factores Críticos de Éxito

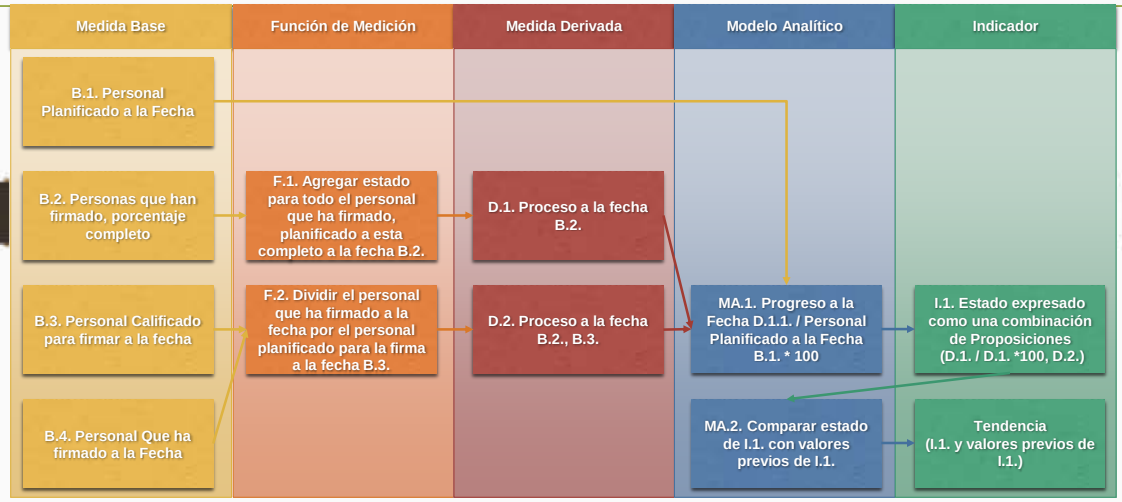
- Compromiso de la alta dirección soportado por los recursos apropiados
- Existencia de los procesos y procedimientos del SGSI
- Un proceso repetible capaz de capturar y reportar datos significativos de manera de proveer tendencias sobre un período de tiempo
- Medidas cuantificables basadas en los objetivos del SGSI
- Datos de fácil obtención que puedan ser utilizados en las mediciones
- Valoración de la efectividad del Programa de medición de la Seguridad de la Información y la implementación de mejoras identificadas
- Recolección, análisis, y reporte periódico y consistente de datos de mediciones de una forma que sea significativa
- Uso de los resultados de las mediciones por las partes interesadas correspondientes, para identificar necesidades de mejora del SGSI implementado
- Aceptación de la respuesta de los resultados de las mediciones por las partes interesadas correspondientes
- Evaluaciones de la utilidad de los resultados de las mediciones y de las implementaciones de las mejoras identificadas



# ISO 27004: Ejemplo de Mediciones

| | Objetivo de la Medición | Atributo | Método de Medición | Medidas de Base |
|---|---|---|---|---|
| Control 1 | O1.1. Planes de Entrenamiento en concentración de la seguridad de la información | A.1.1. Personal Identificado en el Plan | M.1. Contar con la cantidad de personal programados para la firma y que lo haya completado a esta fecha | B.1. Personal Planificado a la Fecha |
| | O.1.2. Personal que haya completado o que esté en proceso de entrenamiento | A.1.2. Estado del Personal con respecto al entrenamiento | M.2. Preguntar al individuo el porcentaje completado de cada personal que haya firmado | B.2. Personal que haya firmado, porcentaje completo |
| Control 2 | O2.1. Planificación para la firma de los acuerdos de usuario | A.2.1. Personal identificado en el plan para firmar. | M-.3. Contar la cantidad de personal programado para la firma a la fecha. | B.3. Personal Planificado para la firma a la fecha |
| | O2.2. Personal que ha firmado los acuerdos | A.2.2. Estado del personal con respecto a la firma de los acuerdos | M.4. Contar la cantidad de personal que ha firmado los acuerdos de usuario. | B.3. Personal Planificado para la firma a la fecha |

# ISO 27004: Implementación de Indicadores






# Ejemplo de Aplicación del Proceso del SGSI

# Ejemplo de Planificación (Plan)

- Identificación de Necesidades
- Definición del Alcance
- Identificación de Restricciones
- Definición del Equipo SGSI
- Asignación de Responsabilidades
- Identificación de Riesgos
- Identificación de Interesados



# Ejemplo de Planificación

| | |
|---|---|
| Evaluar los riesgos que enfrenta la organización | • Se identifican las amenazas a los activos<br>• Se evalúan las vulnerabilidades y probabilidades de ocurrencia<br>• Se estima el impacto potencial |
| Tener en cuenta los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir | • La organización<br>• Sus socios comerciales<br>• Los contratistas<br>• Los prestadores de servicios |
| Definir Principios | • Establecer un conjunto específico de principios, objetivos y requisitos para el procesamiento de la información |

# Ejemplo de Planificación (Plan)

| IMPACTO | NO PROBABLE (1) | OCACIONAL (2) | PROBABLE (3) | MUY PROBABLE (4) |
|---|---|---|---|---|
| MUY ALTO (4) | 3 | 4 | 5 | 5 |
| ALTO (3) | 3 | 3 | 4 | 5 |
| BAJO (2) | 2 | 3 | 3 | 4 |
| MUY BAJO (1) | 1 | 2 | 3 | 3 |

PROBABILIDAD

| | |
|---|---|
| Evitar | •Esta es la mejor forma de atacar a un riesgo.<br>•Se buscan las causas que podrían provocar al riesgo y se eliminan para que el riesgo no suceda. |
| Transferir | •La segunda mejor forma de atacar un riesgo.<br>•El riesgo no se elimina, pero se transfiere a otra persona u organización para que lo administre. |
| Mitigar | •Si no podemos evitar o transferir un riesgo, lo mejor que podemos hacer es mitigarlo buscando una manera de reducir la probabilidad de que el riesgo ocurra y/o el impacto que el riesgo generará en el proyecto. |
| Aceptar | •La última y peor forma de atacar un riesgo es aceptarlo. |
| Ignorar | •Si el Riesgo no es relevante, se deja mapeado, pero no se toma acción, hasta que su estado cambie. |



# Ejemplo de Hacer / Implementar (Do)

| | | | |
|---|---|---|---|
| Fase I: Documentación | Fase II: Implementación | Fase III: Análisis Crítico | Fase IV: Certificación |
| Capacitación formal al equipo de Implementación SGSI. | Difusión de plan SGSI | Auditorías Internas | Identificación de Brechas |
| Documentación de Requisitos Normativos | Despliegue de Capacitaciones e Inducciones | Ajustes en Políticas, Normas | Levantamiento de Observaciones |
| Publicación de Documentos SGSI | Instrumentación SGSI | Implementación de Mejoras | Certificación |

# Ejemplo de Hacer / Implementar (Do)

**Análisis de vulnerabilidades de los servidores Web de las Entidades Publicas.**

**Boletines de Seguridad de la información**

**Boletines de Alertas de Antivirus.**

**Presentaciones técnicas sobre seguridad.**

**Consultorías y apoyo en recomendaciones técnicas.**



# Ejemplo de Verificar / Medir (Check)

**Programa Anual de Aditoría**

**Tipo de Revisión**

| | | | |
|---|---|---|---|
| AI | Auditoría Interna | AV | Auditoría de Re-Certificación |
| RG | Revisión Gerencial | AR | Auditoría de Vigilancia |
| AP | Auditoría de Pre-Certificación | | |

**Estado**

- No Realizada
- Programada
- Realizada

| | | Timestre 1 | | | Timestre 2 | | | Timestre 3 | | | Timestre 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ENE. | FEB. | MAR. | ABR. | MAY. | JUN. | JUL. | AGO. | SEP. | OCT. | NOV. | DIC. |
| 4. | Sistema de Gestión de Seguridad de Información | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.1. Requisitos Generales | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.2. Establecimiento del SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.2.1. Establecer el SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.2.2. Implementar y Operar el SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.2.3. Monitorear y Revisar el SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.2.4. Mantener y Mejorar el SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.3. Requisitos Documentales | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.3.1. Generales | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.3.2. Control de Documentación | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 4.3.3. Control de Registros | AI | | RG | | AR | AR | AI | | RG | | AR | |
| 5. | Responsbilidades de la Gerencia | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 5.1 Compromiso de la Gerencia | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 5.2 Gestión de Recursos | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 5.2.1. Provisión de Recursos | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 5.2.2. Capacitación, Conocimiento y Capacidad | AI | | RG | | AR | AR | AI | | RG | | AR | |
| 6. | Auditorías Internas SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 6.1. Procedimiento de Auditorías Internas | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 6.2. Plan de Auditorías Internas | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 6.3. Tratamiento a las No-Conformidades | AI | | RG | | AR | AR | AI | | RG | | AR | |
| 7. | Revisión Gerencial | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 7.1. Revisión General | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 7.2. Insumos de Revisión | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 7.3. Resultados de Revisión | AI | | RG | | AR | AR | AI | | RG | | AR | |
| 8. | Mejoramiento del SGSI | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 8.1. Mejoramiento Continuo | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 8.2. Acciones Preventivas | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 8.3. Acciones Correctivas | AI | | RG | | AR | AR | AI | | RG | | AR | |
| 9. | Objetivos de Control y Controles | AI | | RG | | AR | AR | AI | | RG | | AR | |
| | 9.1. Anexo A de la Norma | AI | | RG | | AR | AR | AI | | RG | | AR | |

# Matriz de Responsabilidades

| Nivel de Intervención (Legal, Organizativa, Lógica, Física) | Grupo de Participante (Comité, Oficial, Controlador, Auditor) | Rol de Participante | Participante (Nombre, Teléfono, Correo) | Responsabilidad | Tipo de Acción (RACI) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |



# Matriz de Riesgos

| Amenaza | Consecuencia | Probabilidad (1-4) | Impacto (1-4) | Exposición al Riesgo (1-5) | Tipo Acción (Evitar, Transferir, Mitigar, Aceptar) | Detalle de Acción | Responsable |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

# Ejemplo de Requerimientos Normativos



# Requerimientos Normativos

Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

- Políticas de Seguridad de la Información.
  - Recomendaciones para el establecimiento de políticas de seguridad de la información.
- Organización de Seguridad de la Información.
  - Actividades para el establecimiento de un marco para la gestión de la seguridad de la información a través de la organización.
- Seguridad de Recursos Humanos
  - Prácticas de seguridad de la información relacionadas al control de recursos humanos internos y externos.
- Gestión de Activos.
  - Actividades para el control de activos de información
- Control de Acceso.
  - Prácticas para el control de acceso a los activos de información o información

# Requerimientos Normativos

Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

- Criptografía.
  - Lineamientos para la protección de la información por medios criptográficos.
- Seguridad Física y Ambiental.
  - Actividades para la prevención de eventos que pueden dañar los activos de información.
- Seguridad en las operaciones.
  - Prácticas para asegurar el apropiado control y seguridad sobre los activos de procesamiento.
- Seguridad en las Comunicaciones.
  - Prácticas para asegurar el apropiado control y seguridad sobre los activos de comunicación.
- Adquisición, desarrollo y mantenimiento de Sistemas.
  - Actividades para el aseguramiento del siclo de vida desarrollo, mantenimiento o adquisición de sistemas..



# Requerimientos Normativos

Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

- Relacionamiento con los Proveedores.
  - Prácticas para la administración de la seguridad de la información con proveedores.
- Gestión de Incidentes de Seguridad de la
  - Actividades para la gestión de incidentes de seguridad de la información.
- Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocios.
  - Actividades para el establecimiento de un plan de continuidad del negocio.
- Cumplimiento.
  - Actividades para el monitoreo del cumplimiento respecto al sistema de gestión de seguridad.

# Requerimientos Normativos

Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
- Privacidad y protección de Información Personal Identificable.
  - Actividades prevenir brechas relacionadas a la seguridad de información personal



# Requerimientos Normativos

El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.

Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular.

Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
- Privacidad y protección de Información Personal Identificable.
  - Actividades prevenir brechas relacionadas a la seguridad de información personal

# Requerimientos Normativos

El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
- Privacidad y protección de Información Personal Identificable.
  - Actividades prevenir brechas relacionadas a la seguridad de información personal



# Requerimientos Normativos

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.
- Protección de registros.
  - Actividades para la protección de registros de acuerdo a las regulaciones, legislaciones, contratos y requerimientos de negocio vigentes.
- Privacidad y protección de Información Personal Identificable.
  - Actividades prevenir brechas relacionadas a la seguridad de información personal

# Requerimientos Normativos

Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.



# Requerimientos Normativos

A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento.

Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.

- Identificación de legislación aplicable y requerimientos contractuales.
  - Proceso para la identificación y formalización de requerimientos regulatorios, legales y contractuales.