



USAID
FROM THE AMERICAN PEOPLE

ESTANDARES SOBRE SEGURIDAD INFORMATICA ISO-IEC 27002

MAY 2012

This publication was produced for review by the United States Agency for International Development. It was prepared by the team of Global Business Solutions, Inc. and Weidemann Associates, Inc.

ESTANDARES SOBRE SEGURIDAD INFORMATICA ISO- IEC 27002

Contracted under AID-519-C-12-00001

Improving Access to Financial Services Project

DISCLAIMER

The author's views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.



ESTÁNDARES Y BUENAS PRÁCTICAS SOBRE SEGURIDAD INFORMÁTICA ISO-IEC 27002

Freddy Landivar CRISC, CISA

Mayo, 2012



AGENDA

- I. LA EVOLUCIÓN DEL MOVIL**
- II. LA SEGURIDAD EN COMUNICACIONES MOVILES**



Áreas asociadas a la seguridad





Las buenas practicas – ISO 27002

Tenemos 2 normas fundamentales:

- **17799 → 27002 : NORMALIZACION (Mejores Prácticas)**

Homologada en Argentina IRAM-ISO/IEC 27002

- **27001: Sistema de Gestión de Seguridad de la Información (CERTIFICACION)**

Homologada en Argentina IRAM-ISO/IEC 27001

Las certificaciones son con: BS 7799-2 ó ISO 27001



Las buenas practicas – ISO 27002

Está organizada en 11 capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema para llevar adelante una correcta:

GESTION DE SEGURIDAD DE LA INFORMACION

Alcance:

- **Recomendaciones para la gestión de la seguridad de la información**
- **Sirve de Base para el desarrollo de las políticas de seguridad en las organizaciones**



Objetivo

Preservar la:

● confidencialidad:

accesible sólo a aquellas personas autorizadas a tener acceso.

● integridad:

exactitud y totalidad de la información y los métodos de procesamiento.

● disponibilidad:

acceso a la información y a los recursos relacionados con ella toda vez que se requiera.



Dominios

- 1. Política de Seguridad**
 - 2. Organización de Seguridad**
 - 3. Gestión de Activos**
 - 4. Seguridad de los Recursos Humanos**
 - 5. Protección Física y Ambiental**
 - 6. Gestión de Comunicaciones y Operaciones**
 - 7. Control de Accesos**
 - 8. Adquisición, Desarrollo y Mantenimiento de Sistemas**
 - 9. Gestión de los Incidentes de Seguridad**
 - 10. Gestión de la Continuidad del Negocio**
 - 11. Cumplimiento**
-



A que se refiere “La Información”

La información = activo comercial

Tiene valor para una organización y por consiguiente debe ser debidamente protegida.

“Garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades”

“La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados”



Formas y medios de distribución

- **Impresa,**
- **escrita en papel,**
- **almacenada electrónicamente,**
- **transmitida por correo o utilizando medios electrónicos,**
- **presentada en imágenes, o**
- **expuesta en una conversación.**



La gestión de la seguridad de la Información

Implementando un conjunto adecuado de “CONTROLES”:

- **Políticas**
- **Mejores Prácticas**
- **Normas**
- **Procedimientos**
- **Planes**
- **Estándares Tecnológicos**
- **Estructuras Organizacionales**
- **Software**
- **Hardware**



Como establecer los requerimientos de seguridad

● **Evalúan los riesgos:**

- **se hace un relevamiento de los activos,**
- **se identifican las amenazas a esos activos,**
- **se evalúan vulnerabilidades y probabilidades de ocurrencia,**
- **se estima el impacto potencial y**
- **se determina el nivel de riesgo de cada activo.**

● **Evalúan los Requisitos legales, normativos, reglamentarios y contractuales que deben cumplir:**

- **la organización,**
- **sus socios comerciales,**
- **los contratistas y los prestadores de servicios.**



La selección de controles

“Los controles pueden seleccionarse sobre la base de la Norma ISO 27002, de otros estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda”

Costo de implementación vs. riesgos a reducir y las pérdidas monetarias y no monetarias

Revisiones periódicas de:

- **Riesgos**
- **Controles implementados**



La selección de controles

- **Controles “esenciales” desde el punto de vista legal:**
 - ➔ **protección de datos y confidencialidad de información personal**
 - ➔ **protección de registros y documentos de la organización**
 - ➔ **resguardo de derechos de propiedad intelectual**
 - ➔ **protección contra los delitos informáticos**

- **Controles considerados como “práctica recomendada” de uso frecuente en la implementación de la seguridad de la información:**
 - ➔ **documentación de la política**
 - ➔ **asignación de responsabilidades en materia de seguridad**
 - ➔ **concientización, capacitación y entrenamiento**
 - ➔ **comunicación de incidentes relativos a la seguridad**
 - ➔ **administración de la continuidad de los negocios**



Factores críticos de éxito

- **política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;**
- **una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;**
- **apoyo y compromiso manifiestos por parte de la gerencia;**
- **un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;**
- **comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;**
- **capacitación del área de TI.**



Factores críticos de éxito

- **distribución de las políticas y estándares de seguridad de la información a todos los empleados y contratistas;**
- **Concientización, capacitación y entrenamiento adecuados;**
- **un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.**



Dominio 1 – Política de Seguridad

Nivel gerencial debe:

- **aprobar y publicar la política de seguridad**
- **comunicarlo a todos los empleados**



Dominio 1 – Política de Seguridad

Debe incluir:

- **objetivos y alcance generales de seguridad**
- **apoyo expreso de la dirección**
- **breve explicación de los valores de seguridad de la organización**
- **definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información**
- **referencias a documentos que puedan respaldar la política**



Dominio 1 – Política de Seguridad





Dominio 1 – Política de Seguridad

Es política de la compañía:

● **Eficacia:**

Garantizar que toda la información utilizada es necesaria y útil para el desarrollo de los negocios.

● **Eficiencia:**

Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

● **Confiabilidad:**

Garantizar que los sistemas informáticos brindan información correcta para ser utilizada en la operatoria de cada uno de los procesos.



Dominio 1 – Política de Seguridad

● Integridad:

Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de los negocios en cada uno de los sistemas informáticos y procesos transaccionales.

● Exactitud:

Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

● Disponibilidad:

Garantizar que la información y la capacidad de su procesamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los negocios.



Dominio 1 – Política de Seguridad

● Legalidad:

Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito.

● Confidencialidad:

Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.



Dominio 1 – Política de Seguridad

● Autorización:

Garantizar que todos los accesos a datos y/o transacciones que los utilicen cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

● Protección Física:

Garantizar que todos los medios de procesamiento y/o conservación de información cuentan con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

● Propiedad:

Asegurar que todos los derechos de propiedad sobre la información utilizada por todos sus empleados en el desarrollo de sus tareas, estén adecuadamente establecidos a favor de la compañía.



Dominio 2 – Organización de la Seguridad

Infraestructura de seguridad de la información:

- **Debe establecerse un marco gerencial para iniciar y controlar la implementación.**
- **Deben establecerse adecuados foros de gestión de seguridad que asignen responsabilidades para cada usuario en la organización.**
- **Se debe establecer una fuente de asesoramiento especializado en materia de seguridad y contactos con organizaciones externas**



Dominio 2 – Organización de la Seguridad

Foros de Gestión: Comité de Seguridad

- **aprobar la política de seguridad de la información**
- **asignar funciones de seguridad**
- **actualizarse ante cambios**
- **coordinar la implementación**
- **definir metodologías y procesos específicos de seguridad**
- **monitorear incidentes de seguridad**
- **lidera el proceso de concientización de usuarios**



Dominio 2 – Organización de la Seguridad

Principales roles y funciones:

Sponsoreo y seguimiento

- Dirección de la Compañía
- Foro / Comité de Seguridad

Autorización

- Dueño de datos

Definición

- Área de Seguridad Informática
- Área de Legales

Administración

- Administrador de Seguridad

Cumplimiento directo

- Usuarios finales
- Terceros y personal contratado
- Área de sistemas

Control

- Auditoría Interna
- Auditoría Externa



Dominio 2 – Organización de la Seguridad

Seguridad frente al acceso por parte de terceros:

- **El acceso por parte de terceros debe ser controlado.**
- **Debe llevarse a cabo una evaluación de riesgos: determinar las incidencias en la seguridad y los requerimientos de control.**
- **Los controles deben ser acordados y definidos en un contrato con la tercera parte.**



Dominio 2 – Organización de la Seguridad

Tipos de terceros:

- **personal de mantenimiento y soporte de hardware y software**
- **limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados**
- **pasantías de estudiantes y otras designaciones contingentes de corto plazo**
- **consultores.**



Dominio 3 Gestión de activos

- **Hacer un Inventario de los Activos de Información**
- **Designar a un propietario para cada uno de ellos**
- **Hacer la Clasificación de la información**



Dominio 3 Gestión de activos

Inventario:

“Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo”

Ejemplos:

● recursos de información:

bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada;

● recursos de software:

software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;



Dominio 3 Gestión de activos

Designar a un propietario para cada recurso de información:

- **Identificarse claramente los diversos recursos y procesos de seguridad relacionados con cada uno de los sistemas.**
- **Designar al responsable de cada recurso o proceso de seguridad y se deben documentar los detalles de esta responsabilidad.**
- **Los niveles de autorización deben ser claramente definidos y documentados.**



Dominio 3 Gestión de activos

Clasificación de la información:

Garantizar que los recursos de información reciban un apropiado nivel de protección.

Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

La información debe ser clasificada para señalar:

- **la necesidad,**
- **las prioridades y**
- **el grado de protección.**



Dominio 3 Gestión de activos

Pautas de clasificación:

Considerar las necesidades de la empresa con respecto a la distribución (uso compartido) o restricción de la información, e incidencia de dichas necesidades en las actividades de la organización.

La información deja de ser sensible o crítica después de un cierto período de tiempo.

La clasificación por exceso ("over classification") puede traducirse en gastos adicionales innecesarios para la organización.



Dominio 3 Gestión de activos

La información y las salidas de los sistemas que administran datos clasificados deben ser rotuladas según su valor y grado de sensibilidad para la organización.

Se debe considerar el número de categorías de clasificación.

La responsabilidad por la definición de la clasificación debe ser asignada al propietario designado de la información.



Dominio 4 –Seguridad de los RRHH

Seguridad en la definición de puestos de trabajo y la asignación de recursos

Las responsabilidades en materia de seguridad deben ser:

- **explicitadas en la etapa de reclutamiento,**
- **incluidas en los contratos y**
- **monitoreadas durante el desempeño como empleado.**



Dominio 4 –Seguridad de los RRHH

Capacitación del usuario

Garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus tareas normales.



Dominio 4 –Seguridad de los RRHH

Respuesta a incidentes y anomalías en materia de seguridad

Minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos.



Dominio 4 –Seguridad de los RRHH

Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.



Dominio 5 – Protección física y ambiental

Impedir accesos no autorizados, daños e interferencia a:

- **Sedes**
- **Instalaciones**
- **Información**



Dominio 5 – Protección física y ambiental

- **Perímetro de seguridad física**
- **Controles de acceso físico**
- **Seguridad del equipamiento**
- **Suministros de energía**
- **Cableado de energía eléctrica y de comunicaciones**
- **Mantenimiento de equipos**
- **Seguridad del equipamiento fuera del ámbito de la organización**
- **Políticas de escritorios y pantallas limpias**
- **Retiro de bienes**



Dominio 5 – Protección física y ambiental

Ejemplos:

● Suministro de energía:

Asegurar el suministro permanente de corriente eléctrica, instalando UPS y generadores alternativos. Asegurar el combustible necesario para dichos generadores.

● Escritorios y pantallas limpias:

Sobre los escritorios no deben de quedar papeles sensibles.

Las pantallas deben quedar protegidas con protectores de pantalla con contraseña.

● Retiro de bienes:

Establecer políticas de retiros de bienes de la compañía, ya sea por reparación, mantenimiento, trabajos fuera de la oficina, etc.



Dominio 6 – Gestión de Operaciones y Comunicaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

- **Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información.**
- **Se debe implementar la separación de funciones cuando corresponda.**
- **Se deben documentar los procedimientos de operación**



Dominio 6 – Gestión de Operaciones y Comunicaciones

Separación entre instalaciones de desarrollo e instalaciones operativas

Deben separarse las instalaciones de:

- **Desarrollo**
- **Prueba**
- **Operaciones**

Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.



Dominio 6 – Gestión de Operaciones y Comunicaciones

Procesos / Procedimientos de:

- **Planificación y aprobación de sistemas**
- **Protección contra software malicioso**
- **Mantenimiento back up**
- **Administración de la red**
- **Administración y seguridad de los medios de almacenamiento**
- **Acuerdos de intercambio de información y software**



Dominio 7 – Control de accesos

Requerimientos de negocio para el control de accesos:

- **Coherencia entre las políticas de control de acceso y de clasificación de información de los diferentes sistemas y redes**

Administración de accesos de usuarios:

- **Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.**



Dominio 7 – Control de accesos

- **Administración de accesos de usuarios**
- **Administración de privilegios**
- **Responsabilidades del usuario**
- **Control de acceso a la red**
- **Camino forzado**
- **Autenticación de usuarios para conexiones externas**
- **Monitoreo del acceso y uso de los sistemas**



Dominio 7 – Control de accesos

Ejemplo:

Camino forzado:

“Forzar” al usuario a seguir una ruta de menú preestablecida hasta llegar al recuso y/o transacción solicitada sin la posibilidad de evitar algún paso previo.



Dominio 8 – Adquisición, desarrollo y mantenimiento de sistemas de información

Requerimientos de seguridad de los sistemas.

Asegurar que la seguridad es incorporada a los sistemas de información.

- **Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.**



Dominio 8 – Adquisición, desarrollo y mantenimiento de sistemas de información

Seguridad en los sistemas de aplicación

Se deben diseñar en los sistemas de aplicación, **incluyendo las aplicaciones realizadas por el usuario**, controles apropiados y pistas de auditoria o registros de actividad, incluyendo:

- la validación de datos de entrada,
- procesamiento interno, y
- salidas.



Dominio 9 – Gestión de los incidentes de seguridad de la información

Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados para que puedan ser corregidos en tiempo y forma.

- **Reporte de eventos de seguridad de la información**
- **Reporte de las debilidades de la seguridad**
- **Gestión de incidentes y mejoras**
- **Recolección de evidencia**



Dominio 10 – Gestión de la continuidad del negocio

Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres.

- **Se debe implementar un proceso de administración de la continuidad del negocio**
- **Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio.**



Dominio 10 – Gestión de la continuidad del negocio

- **Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos.**
- **Los planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.**
- **La administración de la continuidad del negocio debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.**



Dominio 10 – Gestión de la continuidad del negocio

Principales etapas:

- **Clasificación de los distintos escenarios de desastres**
- **Evaluación de impacto en el negocio**
- **Desarrollo de una estrategia de recuperero**
- **Implementación de la estrategia**
- **Documentación del plan de recuperero**
- **Testing y mantenimiento del plan**



Dominio 11 – Cumplimiento

- **Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.**
- **Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la organización.**
- **Maximizar la efectividad y minimizar las interferencias de los procesos de auditoría de sistemas.**



Dominio 11 – Cumplimiento

Recolección de evidencia:

La evidencia presentada debe cumplir con las pautas establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso:

- **Validez de la evidencia: si puede o no utilizarse la misma en el tribunal**
- **Peso de la evidencia: la calidad y totalidad de la misma**



Dominio 11 – Cumplimiento

- **Adecuada evidencia de que los controles han funcionado en forma correcta y consistente durante todo el período en que la evidencia a recuperar fue almacenada y procesada por el sistema.**

Para lograr la validez de la evidencia, las organizaciones deben garantizar que sus sistemas de información cumplan con los estándares o códigos de práctica relativos a la producción de evidencia válida.



Dominio 11 – Cumplimiento

Revisiones de la política de seguridad y la compatibilidad técnica:

Garantizar la compatibilidad de los sistemas con las políticas y estándares (normas) de seguridad de la organización.



Dominio 11 – Cumplimiento

Auditoria de sistemas:

Optimizar la eficacia del proceso de auditoria de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditorias de sistemas.



Dominio 11 – Cumplimiento

Relación entre **RIESGOS** y **DELITOS** informáticos:

Delitos tradicionalmente denominados informáticos

Delitos convencionales

Infracciones por “Mal uso”



Dominio 11 – Cumplimiento

Principales Leyes relacionadas con la Seguridad Informática

- **Protección de Datos Personales – “Habeas Data”**
- **Firma Digital.**
- **Propiedad intelectual / Software Legal**
- **Regulación de las Comunicaciones Comerciales Publicitarias por Correo Electrónico – “Antispam”**
- **Delitos Informáticos**
- **Confidencialidad de la Información y productos protegidos**



Preguntas ??

Fuentes:

- Propia
- J. Eterovic Seguridad Informatica
- Wikipedia