



Bienvenido al **séptimo módulo**
de la Academia Latinoamericana de Seguridad Informática



Norma ISO 17799: dominios 6 al 10, Modulo práctico

M O D U L O



INFORMATION SECURITY
Programa Integral de Formación Profesional en
IMPLEMENTACION PRACTICA de medidas de
Seguridad de la Información

Etapa 3: IMPLEMENTACION PRACTICA DEL
PROGRAMA DE SEGURIDAD ISO17799 / BS7799 /
COBIT - Parte 2



INTRODUCCION GENERAL

A continuación presentamos una breve descripción de lo que será esta etapa de la Academia:

- Objetivos
- A quién está dirigido
- Director Académico e Instructor
- Descripción General
- Temario detallado

Objetivos

Los objetivos de esta tercera etapa son poder adquirir conocimientos, metodologías y herramientas de implementación y control de medidas de seguridad de la información de acuerdo con estándares internacionales para:

- La formación PROFESIONAL del individuo
- La IMPLEMENTACION PRACTICA en las organizaciones

A quién esta dirigido

Este Programa está orientado a Responsables de áreas de Seguridad Informática, de TI, Profesionales de Áreas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores de las Tecnologías en general.

Director Académico e Instructor

Licenciado Martín Vila

Business Director I -Sec Information Security (2002-2005)
Country Manager Guarded Networks Argentina (2001)
Gerente experimentado de la práctica de Business Risk Management de Pistrelli, Díaz y Asociados, miembro de Arthur Andersen (abril 1992 - abril 2001)

Ha liderado numerosos proyectos de Auditoría e Implementación de Programas de Seguridad Informática en compañías de primer nivel en el ámbito local e internacional.

Ha desarrollado y participado como instructor en Information Security Courses en USA, Latinoamérica y Argentina (Arthur Andersen, ISACA/ADACSI, Microsoft, Ernst & Young, I-SEC INFORMATION SECURITY INC, entre otros).

Ha sido invitado como Especialista en diversos medios de comunicación masivo como ser CNN, Diario Clarín, El Cronista Comercial, InfoBAE, entre otros.

Descripción General

Esta es la Tercera de las cuatro etapas del Programa:

Etapa 1

MARCO TEORICO ISO17799 / BS 7799

Se desarrollarán los contenidos teóricos básicos y fundamentales para el correcto entendimiento de los requerimientos de la Normativa.

Etapa 2

IMPLEMENTACION PRÁCTICA DEL PROGRAMA DE SEGURIDAD - Parte 1

Etapa 3

IMPLEMENTACION PRÁCTICA DEL PROGRAMA DE SEGURIDAD - Parte 2

Se desarrollará la segunda parte de la **Metodología Práctica de Implementación** de los criterios de seguridad (Módulos Funcionales 7 a 12).

Etapa 4

IMPLEMENTACION FOCALIZADA A TRAVES DE UNA METODOLOGIA: ITIL / MOF

Se desarrollará un enfoque práctico a través de la utilización del MOF (Microsoft) en relación a la aplicación de ITIL.

Temario detallado

Esta es la Segunda Parte de los **12 Módulos Funcionales** desarrollados como una **Metodología Práctica de Implementación** de los criterios de seguridad, y están directamente relacionados con los **10 Dominios de la ISO 17799 TEORICOS con el detalle de los respectivos controles:**

MF.07. Sistemas de Control de Accesos: ID, contraseñas, perfiles, permisos de usuarios.

DOMINIO_6. Gestión de Comunicaciones y Operaciones

DOMINIO_7. Sistema de Control de Accesos

MF.08. Seguridad en el Desarrollo y Mantenimiento de Sistemas.

DOMINIO_6. Gestión de Comunicaciones y Operaciones

DOMINIO_8. Desarrollo y Mantenimiento de Sistemas

MF.09. Seguridad en Sistemas Aplicativos: Consideraciones, Participación en Proyectos de Implementación.

DOMINIO_6. Gestión de Comunicaciones y Operaciones

DOMINIO_8. Desarrollo y Mantenimiento de Sistemas

MF.10. Plan de Continuidad del Negocio.

DOMINIO 9. Plan de Continuidad del Negocio

MF.11. Marco Normativo y Legal: Riesgos vs. Delitos Informáticos, Organismos y Normas Internacionales, Marco legal

DOMINIO 10. Cumplimiento

MF.12. Auditoría de Sistemas: objetivos, metodologías, enfoques proactivos, requerimientos COBIT.

DOMINIO 10. Cumplimiento

MF 07: Sistemas de Control de Accesos

- **Requerimientos ISO 17799**
- **Definición de Sistemas de Control de Accesos**
- **Implementación, Plan de Monitoreo y Mejora Continua**

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Conocer los Requerimientos de control en los sistemas requeridos.
- Definir el Modelo de Seguridad Lógica a implementar.

Paso 1: ¿qué dicen las normas?

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. **Política de Seguridad**
2. **Organización de Seguridad**
3. **Clasificación y Control de Activos**
4. **Aspectos humanos de la seguridad**
5. **Seguridad Física y Ambiental**
6. **Gestión de Comunicaciones y Operaciones**
7. **Sistema de Control de Accesos**
8. **Desarrollo y Mantenimiento de Sistemas**
9. **Plan de Continuidad del Negocio**
10. **Cumplimiento**

Paso 2: ¿cómo lo llevo a la práctica?

Definición de un SISTEMA DE CONTROL DE ACCESOS

Para poder comprender cómo llevar adelante la implementación de todos los controles identificados en la normativa, es necesario diferenciar dos conceptos:

- Proceso de Administración de Permisos
- Accesos Lógicos en los Sistemas

Proceso de Administración de Permisos

Este proceso agrupa todo los controles relacionados con el PROCESO de definición y asignación de PERMISOS, tanto en el software de base como en los sistemas de aplicación:

- Alta de un perfil de usuario: cuando el mismo ingresa a la compañía o requiere acceso a un nuevo sistema.
- Modificación de un perfil de usuario: cuando el mismo requiere nuevos permisos de acceso a igual información y/o a nueva información.
- Baja de un perfil de usuario: cuando el mismo no accede más de manera permanente al sistema o se desvincula de la compañía.

Principios generales de asignación de Permisos

Para una adecuada ADMINISTRACIÓN y posterior CONTROL, en general el mecanismo de asignación de permisos sobre datos considera:

Un USUARIO es ASIGNADO dentro de

Un GRUPO / ROL / PERFIL, al cual le es ASIGNADO

Un MENU de ACCESO (con sus programas asociados) con el que se ACCEDE a

Los DATOS / Base de Datos

De esta manera los USUARIOS no tienen permisos específicos directamente sobre datos, sino los respectivos GRUPOS / ROLES / PERFILES, que a su vez y en la medida que las tecnologías y sistemas lo permitan, tendrán permisos exclusivamente a través de un MENU de ACCESO.

Requisitos para la administración de los accesos:

Podemos identificar los siguientes pasos para estos procesos:

Pasos a seguir en los Procesos de ALTAS y MODIFICACIONES de USUARIOS y/o PERMISOS

1. Solicitud de accesos
2. Especificación de recursos a utilizar
3. Autorización por parte de los Dueños de Datos
4. Definición técnica
5. Ejecución por parte de los administradores

Pasos a seguir en los Procesos de BAJAS de USUARIOS y/o PERMISOS

1. Notificación por parte del Dueño de Datos
2. Especificación de recursos
3. Ejecución por parte de los administradores
4. Control periódico del área de RR.HH. de usuarios que dejan la Organización
5. Control periódico del Área de Seguridad para ver usuarios inactivos en los sistemas

Compromiso del usuario

- Con el objetivo de cubrir aspectos legales, sería conveniente que todo usuario debe firmar un compromiso de responsabilidad y confidencialidad del uso de su cuenta de usuario, de la respectiva contraseña asignada y de la información de los sistemas informáticos a los que acceda.

Accesos Lógicos en los Sistemas

Sistema Automático de control de accesos

- Todas las plataformas y sistemas en donde se procese y/o conserve información sensible deben tener implementado un sistema automático de control de acceso.

Definición de las Cuentas de usuarios

Se deberán identificar y diferenciar las distintas clases de usuarios de los sistemas:

1. Usuarios finales

2. Usuarios especiales (genéricos y genéricos de acceso a datos)

- Los usuarios con máximos permisos de cada equipo y/o sistema no deben utilizarse con fines operativos y sus contraseñas deben someterse a procedimientos de emergencia
- Hay que prestar mucha atención a la Nomenclatura de cuentas especiales, que no deberán identificar el motivo de su creación o uso, y deberá intentar utilizar nomenclaturas similares a las utilizadas para usuarios finales para dificultar su identificación

3. Usuarios de mayor riesgo

- Hay que identificar las CUENTAS de USUARIOS de mayor riesgo, tanto usuarios técnicos (ejemplo, operadores de equipos) como usuarios del negocio (ejemplo, el tesorero de la compañía), con el fin de implementar mayores restricciones y controles en los sistemas.

Datos a incluir en las cuentas de usuarios

Se recomienda tener en cuenta en la descripción de las cuentas algunas recomendaciones tales como:

- En la descripción de cada cuenta de usuario se debe incluir el nombre y apellido completo del responsable de la misma.
- En la descripción de las cuentas no personales debe figurar la función para la que fue creada.

Administración de las contraseñas

En general se identifican algunas recomendaciones básicas en el uso e implementación de las contraseñas:

- Debe ser definida con una longitud mínima de 6 caracteres (según la Norma ISO 17799) NOTA: en general la mayoría de las recomendaciones apuntan a no menos de 8 caracteres.
- Debe permanecer encriptada en archivos ocultos y protegidos.

- No debe ser visible por pantalla al momento de ser ingresada.
- No debe ser en blanco.
- No debe ser identificada en el momento de la transmisión.
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente en un período máximo de 30 a 90 días (en general la mayoría de las recomendaciones apuntan a estos valores, aunque la Norma ISO 17799 no lo especifique).
- Ser distintas por lo menos de las últimas anteriores.
- Permitir ser cambiadas toda vez que el usuario lo requiera.

Generación de contraseñas

Algunas recomendaciones generales para la generación y comunicación de las contraseñas:

- En caso de que el usuario no recuerde su contraseña de inicio a la red, y para poder AUTENTICARLO, deberán utilizarse algunos mecanismos tales como:

 Password Self Service: scripts donde el usuario se valida con preguntas o información previamente cargada a una base de datos

 Conjunto de Preguntas para validar al usuario que llama

 Clave UNICA por Usuario para validar su identidad

 Comprobación Física de la persona

 Uso de algún mecanismo adicional:

- Algo que tenga (ejemplo, tarjetas, tokens)
 - Algo que sea (ejemplo, biometría)
 - Algo que sepa (ejemplo, información)
- El Administrador de Seguridad debe generar las contraseñas debiendo ser distintas unas a otras y deberá utilizar algún mecanismo que no requiera COMUNICARLA (ejemplo, tu fecha de nacimiento, seguido de las tres primeras letras de tu segundo nombre).

Bloqueo de las cuentas

- Toda cuenta de usuario que haya intentado el acceso al sistema en forma fallida y consecutiva tres (3) veces debe ser automáticamente bloqueada.

Manejo de Identidades

Actualmente se están utilizando Soluciones que permiten un MANEJO DE IDENTIDADES con numerosos controles y validaciones, permitiendo la definición centralizada de ROLES para la asignación de los permisos.

En la medida de lo posible, sería recomendable evaluar e implementar este tipo de soluciones automáticas ya que colaboran en el establecimiento de controles automáticos preventivos.

Single Sign ON

Existen también numerosos productos que permiten una mayor facilidad para el usuario en su proceso de autenticación en los sistemas, tratando de concentrar todos los IDS y Contraseñas en UN UNICO par de USUARIO / CONTRASEÑA.

Restricciones adicionales

En algunas organizaciones también se consideran las siguientes medidas de protección:

- Restringir la cuenta de usuario a una sola sesión de trabajo y a determinados días y horas.
- Limitar las conexiones sólo a las estaciones de trabajo autorizadas.
- Cuando los usuarios ingresen a los distintos sistemas, se debe implementar, automáticamente, un mensaje de inicio.

Protector de Pantalla

- Se deberá utilizar las facilidades de protector de pantalla con contraseña para las estaciones de trabajo, con activación automática a los pocos minutos de inactividad en el sistema.

Desconexión

- Se debe desconectar toda sesión activa cuando la estación de trabajo no verifique uso durante pocos minutos, siempre y cuando se disponga de las herramientas automáticas para hacerlo.

Implementación, Plan de Monitoreo y Mejora Continua

Implementación

Para proceder a la Implementación de estos controles, generalmente se siguen los siguientes pasos:

- Redacción de la Normativa
- Definición de los Autorizadores (Dueños de Datos)
- Definición del PROCESO
- Estrategia de GRUPOS / PERFILES / PUESTOS
- Asignación de MENUES o MODELOS DE ACCESOS a los GRUPOS / PERFILES / PUESTOS

Plan de Monitoreo

Los procesos de monitoreos son llevados a cabo por:

- Supervisores/Jefes/gerente TI
- Administrador de Seguridad
- Oficial de Seguridad
- Auditoría Interna
- Auditoría Externa
- Entes de Contralor

Mejora Continua

Tal como recomienda la Normativa ISO 17799, para un programa de mejora continua es necesario:

- Redefinición de los:
 - Permisos Asignados
 - Procesos de Asignación
 - Marco Normativo
- Recordemos el Enfoque ISO: PLAN-DO-CHECK-ACT

NOTA FINAL DEL MODULO:

Para este tema en particular, recomendamos CONOCER en detalle los requerimientos y definiciones detalladas en la NORMA ISO 17799, sección SEGURIDAD DE ACCESOS.

MF.08. Seguridad en el Desarrollo y Mantenimiento de Sistemas

- **Requerimientos ISO 17799**
- **Normativa relacionada**
- **Implementación, Plan de Monitoreo y Mejora Continua**

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Conocer los Requerimientos de control en los sistemas requeridos.
- Identificar los distintos ambientes de procesamiento y las medidas de seguridad a implementar
- Definir un adecuado procedimiento de Pasaje a Producción de Programas y Configuraciones.

Paso 1: ¿qué dicen las normas?

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

Paso 2: ¿cómo lo llevo a la práctica?

Principales conceptos de la separación de ambientes

El objetivo principal es poder definir las pautas generales para asegurar una adecuada separación de ambientes lógicos de procesamiento de la información.

Implementación de distintos ambientes de procesamiento

Como primer paso deberemos identificar los distintos ambientes y las consideraciones generales para la implementación de cada uno de ellos:

- **Ambiente de Desarrollo de Sistemas:** ambiente para efectuar tareas de análisis y programación en sus etapas de desarrollo, mantenimiento y prueba.

A este ambiente solo debe acceder el personal del área de Desarrollo de Sistemas, los usuarios de sistemas autorizados para la prueba de los desarrollos, el Responsable definido para el Pasaje al Ambiente de Testing, el personal del área de Operaciones para efectuar tareas de administración de los equipos y el Administrador de Seguridad.

- **Ambiente Intermedio de Testing / Prueba / Pasaje a Producción:** ambiente con versiones para efectuar las pruebas finales de usuarios y que luego de aprobadas se efectuará el pasaje a producción. Residen las versiones fuentes para compilar y luego probar por los usuarios para su aprobación y posterior pasaje a producción.

En este ambiente solo deben acceder los usuarios autorizados para la prueba de los desarrollos (tanto de sistemas como usuarios finales), el Oficial de Seguridad, el Responsable definido para la compilación y el Pasaje a Producción, el personal del área de Operaciones para efectuar tareas de administración de los equipos y el Administrador de Seguridad.

- **Producción:** ambiente de datos reales.

En este ambiente solo deben acceder los usuarios finales, el personal del área de Operaciones para efectuar tareas de administración de los equipos y el Administrador de Seguridad.

Accesos de emergencia al ambiente de Producción

Con el objetivo de limitar y monitorear el acceso al ambiente productivo, se deben definir de procedimientos de emergencias predefinidos, con usuarios especiales habilitados para tal fin, cuyo accionar se encuentre auditado automáticamente por el sistema y, previamente obtener la autorización expresa del Dueño de Datos o Delegado correspondiente o, en su defecto, notificarlo luego de efectuadas las acciones.

Inventario de las versiones

El área de Operaciones (para software de base) y el Responsable definido para el Pasaje a Producción (para software aplicativo) son responsables de llevar un registro de todas las versiones de software en los equipos de procesamiento centralizado.

Datos de Prueba

La norma ISO 17799 recomienda en caso de usarse datos reales para las pruebas, efectuar procedimientos de DESPERSONALIZACIÓN de los datos, y preferentemente, BORRAR esos datos una vez efectuadas las tareas.

Evaluación de los controles y de la seguridad

Como parte de la Metodología de Desarrollo de Sistemas, debe contemplarse la posibilidad que previamente a la instalación en producción, el Oficial de Seguridad debe identificar las funciones provistas por cada nuevo software que pudieran comprometer la seguridad de los datos establecida y definir las medidas de seguridad adicionales necesarias.

Esta tarea puede convertirse en un proyecto en si mismo, por lo que es necesario que esté definido desde el inicio del desarrollo de los sistemas (como se verá en el módulo siguiente).

Controles y Seguridad de los sistemas

Todo software desarrollado debe poseer medidas de control y seguridad:

- Sistema de control de accesos de los usuarios que permita:
 - La identificación del usuario.
 - La segregación de funciones desde un punto de vista de control interno.
 - La asignación de permisos a través de grupos o perfiles modelos.
- Reportes y registros de auditoría automáticos sobre transacciones y archivos críticos que identifiquen usuario, fecha, hora, estación de trabajo, función realizada y preferentemente situación antes/después.
- Mecanismos de recuperación automática de datos de manera de garantizar la integridad y continuidad de las transacciones ante cancelaciones y/o interrupciones en el procesamiento.
- Todo sistema debe contar con la correspondiente ayuda en línea y manuales de uso, de operaciones y de mantenimiento.

Procedimiento: Pasaje al Ambiente de Producción

La normativa requiere que se defina un Procedimiento Formal para la Solicitud de Requerimientos de Cambios y el posterior Pasaje al ambiente Productivo.

Para ello, adjuntamos un Modelo de este Procedimiento, en el cual se definirán las acciones necesarias para las tareas relacionadas con el pasaje de modificaciones de aplicaciones desde el ambiente de desarrollo a los distintos ambientes de producción.

Responsables del cumplimiento

Todos los Administradores de Seguridad, Dueños de datos, el área de Desarrollo y el área de Operaciones son responsables del cumplimiento de este procedimiento.

Procedimiento: Pasaje al Ambiente de Producción

Pasos	Responsables
1. Solicita cambios y/o nuevos desarrollos al área de Desarrollo.	Dueño de Datos Area de Sistemas Auditoría
2. Asigna un responsable dentro del área para administrar los cambios en las aplicaciones.	Jefe de Desarrollo
3. Efectúa la estimación de recursos y la envía al Jefe de Desarrollo para su aprobación. En esta etapa se debe requerir la participación del área de Seguridad de la Información cuando las modificaciones sean significativas desde un punto de vista de seguridad.	Jefe de Proyecto
4. Analiza y envía al Dueño de datos las estimaciones efectuadas para su aprobación.	Jefe de Desarrollo

Procedimiento: Pasaje al Ambiente de Producción

Pasos	Responsables
5. Aprueba las estimaciones recibidas y envía la autorización para la realización de las modificaciones al área de Desarrollo.	Dueño de datos
6. Efectúan las tareas de análisis y programación necesarias en el ambiente de desarrollo. Solicita la participación del área de Seguridad de la Información.	Personal del área de Desarrollo
7. Efectúa el pasaje al ambiente de Pruebas para efectuar las pruebas de usuarios necesarias.	Administrador de cambios
8. Efectúan las pruebas necesarias en el ambiente de Pruebas. Solicitan la participación y la aprobación formal del sector usuario.	Personal del área de Desarrollo Seguridad de la Información Sector Usuario

Procedimiento: Pasaje al Ambiente de Producción

Pasos	Responsables
9. Luego de haberse obtenido la aprobación correspondiente, solicita al Administrador de cambios que efectúe el pasaje de los programas fuentes y/o configuraciones al ambiente de Producción, generando los instructivos en caso de ser necesario.	Jefe de Proyecto
10. Ejecuta el pasaje de los programas fuentes y/o configuraciones al ambiente de Producción, realiza las compilaciones correspondientes y posteriormente elimina los mismos del ambiente de Pruebas.	Administrador de cambios de Producción
11. Notifica a los responsables solicitantes de las modificaciones que las mismas ya fueron implementadas.	Jefe de Proyecto

Implementación, Plan de Monitoreo y Mejora Continua

Implementación

Para proceder a la Implementación de estos controles, generalmente se siguen los siguientes pasos:

- Redacción de la Normativa (Norma y Procedimiento)
- Definición de los Autorizadores (Dueños de Datos Sistemas)
- Implementación de Entornos
- Implementación de GRUPOS / PERFILES para los ambientes de Desarrollo y Testing
- Asignación de ACCESOS a los GRUPOS / PERFILES / PUESTOS

En esta etapa en general se tienen en cuenta además de los requerimientos de la Norma ISO 17799, algunas otras metodologías internacionales, como ITIL, CMMI, entre otras.

Adicionalmente es bueno tener en cuenta que este proceso es uno de los más considerados en la implementación de CONTROLES para aquellas compañías alcanzadas por la Ley Sarbanes Oxley (USA).

Plan de Monitoreo

Los procesos de monitoreos son llevados a cabo por:

- Supervisores/Jefes/gerente de TI
- Administrador de Seguridad
- Oficial de Seguridad
- Auditoría Interna
- Auditoría Externa
- Entes de Contralor

Mejora Continua

Tal como recomienda la Normativa ISO 17799, para un programa de mejora continua es necesario:

- Redefinición de los:
 - Entornos
 - Permisos Asignados
 - Procesos de Asignación
 - Marco Normativo
- Recordemos el Enfoque ISO: PLAN-DO-CHECK-ACT

MF09. Seguridad en Sistemas Aplicativos

- Requerimientos ISO 17799
- Participación en Proyectos de Desarrollo e Implementación de Sistemas

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Conocer los Requerimientos de control en los sistemas.
- Definir los pasos a seguir por el Área de Seguridad de la Información en los procesos de Desarrollo y Puesta en Producción de Sistemas.

Paso 1: ¿qué dicen las normas?

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

Paso 2: ¿cómo lo llevo a la práctica?

Participación en Proyectos de Desarrollo e Implementación

Es necesario considerar que el Área de Seguridad debe participar en los procesos de Desarrollo y Puesta en Producción de Sistemas, conservando como propia la decisión de PARTICIPAR o NO de acuerdo al análisis de criticidad efectuada por el Dueño de Datos.

Para ello vamos a analizar dos conceptos:

- **Principales consideraciones a tener en cuenta**
- **Responsabilidades en cada Etapa del proyecto**

Principales consideraciones a tener en cuenta

Análisis general de los componentes y procesos del sistema

Inicialmente debemos considerar las generalidades del sistema:

- Funciones de negocio soportadas
- Principales sectores usuarios del sistema
- Estructura general de bases de datos y archivos

Análisis de la seguridad de accesos de los usuarios a los datos

A continuación se identifican y definen aspectos funcionales:

- Menús definidos.
- Perfiles/grupos/roles de usuarios.
- Personas/funciones a los que se le asignaron los usuarios.
- Accesos por fuera de los menús.

Controles internos definidos en el sistema

En la etapa siguiente se analiza internamente el sistema, identificando para cada proceso / transacción:

- Controles preventivos
- Controles de procesos
- Controles de salida

Análisis de la seguridad de aspectos técnicos del sistema

En esta etapa se analizan los requerimientos de control para los aspectos más técnicos del sistema:

- Estructura general de la aplicación
- Comunicación e Interfaces internas en sus componentes
- Proceso de Validación de usuarios
- Módulo de Administración de Usuarios (altas, bajas, asignación de permisos)
- Restricciones para no salir de las aplicaciones
- Integración con la Base de Datos
- Logs y Auditorías
- Control de integridad de los datos y transacciones
- Esquema de reportes
- Procedimiento de Backup y Recovery

Análisis de la integración del sistema con la arquitectura técnica de la red de datos

Por último también se definen los requerimientos de control teniendo en cuenta la integración del sistema con la arquitectura técnica, analizando la relación con:

- Servidores
- Motor de Base de datos
- Principales interfaces externas con otros sistemas

Participación en Proyectos de Desarrollo e Implementación

Es necesario identificar y además DEFINIR FORMALMENTE las Responsabilidades en cada Etapa del proyecto del Área de Seguridad de la Información:

Planificación

- Desarrollar el Plan de trabajo específico para Seguridad y Controles.
- Adaptar la metodología de trabajo a la del proyecto.
- Integrar el equipo de trabajo con el equipo del proyecto.

Implementación del Entorno de trabajo del proyecto

- Definir la seguridad y el control en los ambientes de desarrollo a utilizar.
- Integrar el esquema de seguridad con el esquema de los sistemas de la Compañía.

Diseño Conceptual

- Identificar los mecanismos de control propios de la aplicación.
- Identificar los requerimientos de los usuarios.
- Análisis de la criticidad de cada módulo/función.
- Evaluar riesgos propios en las herramientas de la nueva arquitectura / sistema.
- Identificar las mejores prácticas.
- Definir el modelo general de seguridad applicativa integrado con seguridad del entorno de trabajo.

Definición y Parametrización

- Diseñar controles a incluir en los programas.
- Revisar el diseño de interfaces.
- Definir parámetros que permitan cubrir los riesgos identificados en diseño.
- Determinación de los riesgos remanentes.
- Definición de controles manuales alternativos.
- Diseño de los perfiles de usuarios en la aplicación y en el entorno.
- Desarrollo de los procedimientos manuales.

Conversión

- Revisar diseño de conversiones e inclusión de controles que aseguren la integridad y exactitud de los datos convertidos.

Prueba

- Identificar controles críticos a verificar.
- Probar el diseño y el funcionamiento de los controles.
- Identificar áreas de mejoras.
- Desarrollar nuevos controles manuales alternativos.

Capacitación

- Incluir temas de control en material de capacitación.
- Participar en entrenamiento sobre temas de control y seguridad.

Implementación

- Verificar la correcta conversión de los datos.
- Verificar la correcta implementación de los controles y seguridad.
- Atender problemas de lanzamiento.
- Participar en equipo de Mesa de Ayuda de Control y Seguridad hasta la estabilización del software.

MF 10: Plan de Continuidad de los Negocios

- Consideraciones Generales
- Requerimientos ISO 17799
- Etapas de un Plan
- Implementación, Plan de Monitoreo y Mejora Continua

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Identificar el alcance de un Plan de Continuidad de Negocios
- Conocer los Requerimientos de acuerdo a la Normativa
- Definir una Metodología Práctica de desarrollos de Sistemas

Paso 1: ¿qué dicen las normas?

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

Paso 2: ¿cómo lo llevo a la práctica?

Desarrollo de un Plan de Continuidad del Negocio

Inicialmente debemos considerar qué es un **Plan de Continuidad del Negocio**:

- Conjunto de acciones a ser llevadas a cabo ante distintos escenarios de desastres que pudieran afectar la correcta marcha de los negocios.

El punto central es focalizarse específicamente en la recuperación de las **funciones y sistemas críticos** para el negocio, cuya interrupción puede afectar directamente los objetivos de la compañía.

¿Quiénes son Responsables de la Definición e Implementación?

- Dirección y Gerencias
- Área de Seguridad de la Información
- Área de Sistemas / IT
- Auditores Internos
- En algunas Organizaciones también los Dueños / Accionistas

Denominaciones

En general podemos ver las distintas denominaciones que se le da a este tema:

- BCP Business Continuity Plan
- BCP Business Contingency Plan
- DRP Disaster Recovery Plan
- CP Contingency Plan
- BRP Business Recovery Plan

NOTA:

Hay que considerar que el **Plan de Continuidad del Procesamiento** es parte integrante del Plan de Continuidad del Negocio y se enmarca específicamente en:

- Definir los riesgos emergentes ante una situación de interrupción no prevista del **procesamiento de la información** relacionada con las operaciones de los sistemas y definir los planes de recupero de la capacidad de procesamiento para minimizar los impactos de la interrupción en la correcta marcha del negocio.

En algunas metodologías, a este Plan lo denominan DRP Disaster Recovery Plan.

Componentes de un Plan de Continuidad de los Negocios

Tiene dos componentes principales:

- Tecnológico: procesamiento de los sistemas
- Funcional: procedimientos del personal

Principales Etapas

A continuación identificaremos las principales tareas de un BCP

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

Clasificación de los distintos escenarios de desastres

- Identificar los distintos tipos de “desastres”

- TECNOLÓGICOS (ejemplo: caída en el procesamiento de los equipos)
 - HUMANOS:
 - o INTENCIONALES (ejemplo: huelga del personal)
 - o NO INTENCIONALES (ejemplo: error del operador de la red)
 - NATURALES (ejemplo: inundación)
- Clasificación de los distintos escenarios de desastres:
- Ponderar su probabilidad de ocurrencia
 - **FINALMENTE: Fijar el alcance del proyecto a los desastres de mayor probabilidad**

Evaluación de impacto en el negocio

- Definir los perjuicios “claves” en la evaluación del impacto en el negocio.
 - Económicos
 - Financieros
 - Políticos
 - Sociales
 - De imagen
 - Legales
 - Gremiales
 - Otros
- Identificar los usuarios claves de cada sector.
- Relevar las funciones críticas del negocio.
- Definir un tiempo máximo para disponer de la información sin que impacte en el negocio.
- Efectuar estimaciones cualitativas y cuantitativas del perjuicio para la compañía.
- **FINALMENTE: Definir las funciones críticas que se identifican para la recuperación.**

En algunas metodologías, a esta etapa se la denomina BIA (Business Impact Analysis).

Selección de una estrategia de recupero

- Analizar impacto de desastres seleccionados y funciones críticas identificadas:

- cada uno de los distintos escenarios de desastres seleccionados,
 - cada una de las funciones críticas del negocio identificadas.
- Definir alternativas de recupero del negocio:
 - Funcionales (ejemplo: facturación manual)
 - Técnicas (ejemplo: sitio alternativo)
 - Algunos ejemplos adicionales para los equipos de procesamiento que se encuentran en las metodologías son:
 - Recuperación interna
 - Reemplazo de equipos
 - Contratos entre compañías
 - Hot Site
 - Cold Site
 - Service Bureau
- Analizar los costos actuales y futuros de las soluciones
 - “El costo real de la planificación de recupero no reside solo en la implementación de la solución, sino además en el testeo y mantenimiento continuo.”
- Elegir la/las soluciones a implementar

Implementación de la estrategia

- Desarrollar las medidas a implementar en cada una de las etapas:
 - Identificación del desastre.
 - “Declaración” del desastre.
 - Actividades a desarrollar durante el desastre.
 - Recuperación del procesamiento para volver a la “situación normal”.
- Suscribir los contratos comerciales necesarios para la ejecución de los procedimientos seleccionados.
- Suscribir los contratos de seguros en caso de ser definido.
- Implementar los mecanismos tecnológicos necesarios.

- Generación de back up alternativos.
 - Implementación de vínculos de enlaces paralelos.
 - Configuración de equipos espejados.
 - Otros.
- Asignar las responsabilidades a cada una de las personas / sectores de la Compañía involucradas en el Plan:
 - en las distintas etapas del desastre,
 - en el mantenimiento del plan a lo largo del tiempo
- Capacitar al personal involucrado.
 - Definir acciones complementarias:
 - Comunicación a clientes y proveedores.
 - Distribución física de lugares de trabajo del personal.
 - Estrategias de trabajo “en cada casa”.
 - Otros recursos (teléfonos, fax, etc.).

NOTA: es necesario considerar los efectos SICOLOGICOS Y EMOCIONALES que pueden impactar en el PERSONAL una vez ocurrido el DESASTRE.

Documentación del plan de recupero

- Desarrollar los procedimientos funcionales y técnicos:

Funcionales:

- para la ejecución de las tareas para el personal de cada sector.
- para la operación de los equipos por parte de personal especializado.

Técnicos:

- para la instalación y configuración de la tecnología involucrada

- Desarrollar los inventarios:

- personal

- documentación
- requisitos de espacio
- hardware
- software
- redes
- Registros electrónicos
- otros

Testeo y mantenimiento del plan

- Testeo
 - Desarrollar pruebas:
 - Unitaria
 - Integral
 - Asemejar pruebas a la realidad
- Mantenimiento
 - Definir mecanismo para su actualización.
 - Efectuar pruebas periódicas del correcto funcionamiento

Implementación, Plan de Monitoreo y Mejora Continua

De acuerdo a los requerimientos de la NORMA ISO 17799, es necesario definir FORMALMENTE los mecanismos de Implementación, Plan de Monitoreo y Mejora Continua para el BCP.

Implementación

- Desarrollo del Plan
- Prueba y Aprobación Final

Plan de Monitoreo

- Controles efectuados por parte de:
 - Dirección de la Compañía
 - Oficial de Seguridad
 - Auditoría Interna

- Auditoría Externa
- Entes de Contralor

Mejora Continua

Tal como recomienda la Normativa ISO 17799, para un programa de mejora continua es necesario:

- Mantenimiento Permanente:
 - Pruebas periódicas
 - Redefinición del Plan y Estrategias de Recuperación
 - Documentación de Cambios
- Recordemos el Enfoque ISO: PLAN-DO-CHECK-ACT

MF 11: Marco Normativo y Legal

- Requerimientos Normativos
- Riesgos y Delitos Informáticos

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Conocer los Requerimientos de acuerdo a la Normativa
- Identificar la relación entre un RIESGO del NEGOCIO y un DELITO

Paso 1: ¿qué dicen las normas?

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

Paso 2: ¿cómo lo llevo a la práctica?

Algunas consideraciones a tener en cuenta:

Para poder evaluar el real impacto en la organización de estos aspectos, es IMPRESCINDIBLE trabajar conjuntamente con otras áreas:

- **Legales**
- **Recursos Humanos**
- **Auditoría Interna**
- **Seguridad Física y Vigilancia**
- **Dirección de la Compañía**
- **Agentes Externos (Policía, Justicia, etc.)**

En este tema es MUY IMPORTANTE:

- **Actitud Preventiva:**

Desarrollar medidas de control de forma ANTICIPADA.

- **Definición y Conservación de Evidencias**

Identificar los requerimientos legales en cada una de las JURISDICCIONES donde opera la Organización, tanto para las Evidencias:

- **Técnicas**
- **Físicas**

- **Análisis Forense**

Definir las acciones a seguir una vez que suceden los hechos.

RIESGOS del Negocio y DELITOS Informáticos

En esta etapa se deben identificar la relación en el impacto que puede tener un mismo hecho tanto en los aspectos relacionados con el NEGOCIO, como en las responsabilidades y compromisos LEGALES que pueden generarse para la COMPAÑÍA y para sus FUNCIONARIOS y DIRECTIVOS.

DELITO INFORMATICO

- El concepto de delito informático engloba tanto los delitos cometidos mediante el uso de sistemas informáticos como los delitos cometidos contra los bienes jurídicos que históricamente se han relacionado con las tecnologías de la

información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.

- Independientemente de que existen riesgos informáticos, solo algunos de ellos pueden ser catalogados como delitos.
- Aquellos delitos cometidos mediante la utilización de los recursos informáticos son difíciles de perseguir debido a la propia naturaleza del entorno y a la falta de tipificación de las modalidades de comisión y de los medios empleados.

Relación entre RIESGOS y DELITOS informáticos

Entre los delitos, infracciones administrativas y malos usos que se pueden llevar a cabo se pueden identificar los siguientes:

Delitos tradicionalmente denominados informáticos

Delitos convencionales

Infracciones por “Mal uso”

Delitos tradicionalmente denominados

- **Acceso no autorizado:**
 - El uso ilegítimo de passwords y la entrada en un sistema informático sin la autorización del propietario.
- **Destrucción de datos:**
 - Los daños causados en la red mediante la introducción de virus, bombas lógicas y demás actos de sabotaje informático.
- **Infracción de los derechos de autor:**
 - Copia, distribución, cesión y comunicación pública de los programas.
- **Infracción del copyright de bases de datos:**
 - El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los archivos contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.
- **Intercepción de e-mail:**
 - En este caso, se propone una ampliación de los preceptos que castigan la violación de correspondencia y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.
- **Estafas electrónicas:**
 - La proliferación de las compras vía Internet permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que

además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra.

➤ **Transferencias de fondos:**

- Este es el típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático. A pesar de que en algunas legislaciones y en sentencias aisladas se ha asimilado el uso de passwords y tarjetas electrónicas falsificadas al empleo de llaves falsas, calificando dicha conducta como robo, existe todavía una falta de uniformidad en la materia.

Delitos convencionales

Los delitos convencionales son todos aquellos que tradicionalmente ya se estaban dando en la "vida real" sin el empleo de medios informáticos:

➤ **Espionaje:**

- Se han dado casos de accesos no autorizados a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.

➤ **Espionaje industrial:**

- También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que

posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

➤ **Terrorismo:**

- La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha sido aprovechado por grupos terroristas para remitir consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

• **Narcotráfico:**

- Existen mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha detectado el uso de la red para la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

• **Otros delitos:**

- Las mismas ventajas que encuentran en Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, etc.

Infracciones por “Mal uso”

➤ **Usos comerciales no éticos:**

- Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailings electrónicos" al colectivo de usuarios de un gateway, un nodo o un territorio determinado. Ello, aunque no constituye una infracción, es

mal recibido por los usuarios de Internet, poco acostumbrados, hasta fechas recientes, a un uso comercial de la red.

➤ **Usos particulares no éticos:**

- Emplear los recursos informáticos para distribuir obscenidades, insultos, etc.

➤ **Publicación no autorizada:**

- Poner a disposición de usuarios determinada información cuyo acceso puede no estar permitido o que requiera autorización previa o erogación económica. Ejemplo de esto es el intercambio gratuito de música. Esto puede ocurrir al conectar un servidor a Internet o el envío a través de correos electrónicos.

➤ **Acceso a la información privada de las personas::**

- Puede darse a través de la publicación de información personal residente en bases de datos y/o en registros de monitoreos de los sistemas, o por la interceptación de los correos electrónicos enviados por Internet.

MF.12.Auditoría de Sistemas

- **Objetivos y metodologías**
- **Plan de Auditoría Anual según ISO 17799 y COBIT**
- **Programa de Auditoría detallado de cada dominio**
- **Integración con el Programa de Seguridad de la compañía**
- **Informes, Presentaciones y Soportes documentales**

OBJETIVOS

Los objetivos planteados para este Módulo son:

- Conocer los Requerimientos de la Norma ISO 17799 para la Auditoría de Seguridad
- Conocer otras Metodologías para la Auditoría de Sistemas.

Paso 1: ¿qué dicen las normas?

En general para poder desarrollar estas tareas, la comunidad de profesionales utiliza no solamente la Norma ISO 17799, sino principalmente la METODOLOGIA COBIT Audit Guidelines de ISACA.

¿Con cuál de los Dominios de la ISO 17799 Seguridad de la Información está relacionada?

Marco Normativo ISO 17799

1. Política de Seguridad
2. Organización de Seguridad
3. Clasificación y Control de Activos
4. Aspectos humanos de la seguridad
5. Seguridad Física y Ambiental
6. Gestión de Comunicaciones y Operaciones
7. Sistema de Control de Accesos
8. Desarrollo y Mantenimiento de Sistemas
9. Plan de Continuidad del Negocio
10. Cumplimiento

Otras Metodologías aplicables: COBIT AUDIT GUIDELINES:

Esta es la principal Metodología Internacionalmente aceptada para la Práctica de Auditoría de Sistemas de Información.

Comprenden una serie de Objetivos de Control a cumplir en los distintos aspectos del “gobierno” de IT:

- Planeamiento y organización
- Adquisición e implementación
- Entrega de servicios y soporte
- Monitoreo

Paso 2: ¿cómo lo llevo a la práctica?

Principales consideraciones para la Auditoría

Inicialmente es necesario identificar las diferencias entre:

AUDITORIA DE SEGURIDAD (ISO 17799)

Vs.

AUDITORIA DE SISTEMAS (COBIT)

La auditoría basada en ISO 17799 abarca todos los procesos relacionados con INFORMACION de la Compañía y se fundamenta en validar el cumplimiento de los 10 dominios de la norma.

La auditoría basada en COBIT se focaliza más en los CONTROLES del AREA DE TI y de la TECNOLOGIA, siendo más INTEGRAL en estos aspectos más específicos.

Algunas consideraciones generales

Definiciones generales de Auditoría de Sistemas

- La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.
- La actividad dirigida a verificar y juzgar información.
- El examen y evaluación de los procesos del Área de Procesamiento Electrónico de Datos (PED) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas.
- El proceso de recolección y evaluación de evidencia para determinar si un sistema:
 - Salvaguarda activos
 - Ø Daños
 - Ø Destrucción
 - Ø Uso no autorizado
 - Ø Robo
 - Mantiene Integridad de los datos
 - Ø Información Precisa
 - Ø Completa
 - Ø Oportuna
 - Ø Confiable
 - Alcanza metas organizacionales
 - Ø Contribución de la función informática
 - Consume recursos eficientemente
 - Ø Utiliza los recursos adecuadamente

- Es el examen o revisión de carácter objetivo (independiente), crítico (evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a:
 - Eficiencia en el uso de los recursos informáticos
 - Validez de la información
 - Efectividad de los controles establecidos

Objetivos Generales de la Auditoría de Sistemas

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados por el PED
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos
- Incluir la seguridad de personal, datos, hardware, software e instalaciones
- Apoyo de función informática a las metas y objetivos de la organización
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático
- Minimizar existencias de riesgos en el uso de Tecnología de información
- Decisiones de inversión y gastos innecesarios
- Capacitación y educación sobre controles en los Sistemas de Información
- Aumento considerable e injustificado del presupuesto del PED (Departamento de Procesamiento Electrónico de Datos)
- Desconocimiento en el nivel directivo de la situación informática de la empresa
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con los sistemas informáticos

Algunas Actividades a desarrollar

- Como toda auditoría, depende del alcance de lo que se pretenda revisar o analizar, pero como estándar analizaremos las cuatro fases básicas de un proceso de revisión:
 - Estudio preliminar
 - Revisión y evaluación de controles y seguridades
 - Examen detallado de áreas críticas
 - Comunicación de resultados
- **Estudio preliminar.**- Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, Manuales de políticas, reglamentos, Entrevistas con los principales funcionarios del PED.
- **Revisión y evaluación de controles y seguridades.**- Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas críticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.
- **Examen detallado de áreas críticas.**-Con las fases anteriores el auditor descubre las áreas críticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance Recursos que usara, definirá la metodología de trabajo, la duración de la auditoría, Presentará el plan de trabajo y analizara detalladamente cada problema encontrado con todo lo anteriormente analizado en este folleto.
- **Comunicación de resultados.**- Se elaborara el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual presentara esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

Principales ETAPAS para desarrollar el Proceso de la Auditoría de Sistemas y Seguridad

Algunas consideraciones básicas son necesarias para este proceso:

- Integrarla con el Plan de Controles del Programa de Seguridad de la Compañía
- Definir el Plan de Auditoría desde el comienzo del Programa
- Considerar evidencias / soportes documentales
- Definir responsables de la ejecución
- Incorporar los controles surgidos de ISO 17799 / COBIT
- Integrarla con la Auditoría Integral de Sistemas y de Negocio

Integrarla con el Plan de Controles del Programa de Seguridad de la Compañía

Sponsoreo y seguimiento

- Dirección de la Compañía
- Foro / Comité de Seguridad

Autorización

- Dueño de datos

Definición

- Área de Seguridad Informática
- Área de Legales, RRHH

Administración

- Administrador de Seguridad

Cumplimiento directo

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

Control

- Auditoría Interna
- Auditoría Externa

Definir el Plan de Auditoría desde el comienzo del Programa

Una vez identificados los procesos, definir los mecanismos de control, evidencias a conservar y procesos de auditorías a desarrollar.

Algunos de los procesos definidos pueden ser:

- Administración de Usuarios y Claves de Acceso y Permisos
- Separación de Ambientes de Trabajo
- Licencias legales de Software

- Copias de Respaldo
- Seguridad Física de las Instalaciones
- Prevención de Virus
- Continuidad del Procesamiento
- Seguridad en las Comunicaciones
- Logs de Auditoría y Reporting
- Instalación de Software
- Seguridad de la red perimetral

Considerar evidencias / soportes documentales

- Soportes documentales
- Logs de los sistemas
- Protección de las herramientas a utilizar (la Norma ISO 17799 define conservar estas herramientas en el ambiente de producción como el resto de los software de la compañía)

En este momento es IMPRESCINDIBLE incorporar al área de LEGALES.

Definir responsables

De acuerdo a la norma ISO 17799 este proceso de Auditoría debe ser llevado a cabo por:

- Auditoría Interna (si existiera)
- Gerente Independiente (si no hay Auditoría Interna)
- Auditores Externos (opcional)

La Metodología COBIT es más estricta y sugiere una MAYOR independencia de criterios entre el AUDITOR y el AUDITADO.

Incorporar los controles surgidos de ISO 17799 / COBIT

Norma ISO 17799: Seguridad de la Información

En todos los módulos anteriores hemos definidos los controles sujetos a la auditoría.

Metodología - COBIT

- **Desarrollada por el Information Systems and Audit Control Association - ISACA**

- Uno de los principales organismos que reúne a los Auditores de Sistemas es el ISACA, que a través de las COBIT AUDIT GUIDELINES (COBIT Control Objectives for Information and Related Technology), define los principales estándares internacionalmente aceptados para la práctica de Auditoría de Sistemas.
- Comprenden una serie de Objetivos de Control a cumplir en los distintos aspectos del “gobierno” de IT, dentro de los cuales se encuentran los temas específicos de Seguridad y Control:

Planeación y Organización

Plan Estratégico

Arquitectura de Información

Organización de TI

Inversión en TI

Administración de Recursos Humanos

Evaluación de Riesgos

Administración de proyectos y de Calidad

Adquisición e Implementación

Identificación de Soluciones

Adquisición y Mantenimiento de Software y Arquitectura de Tecnología

Desarrollo y Mantenimiento de Procedimientos de TI

Administración de Cambios

Entrega de Servicios y Soporte

Administración de Servicios propios y de Terceros

Servicio Continuo

Seguridad de Sistemas

Educación y Entrenamiento de Usuarios

Administración de la Configuración y Datos

Manejo de Incidentes

Monitoreo

Monitoreo del Proceso y del Control Interno

Auditoría Independiente

Integrarla con la Auditoría Integral de Sistemas y de Negocio

Es necesario que estos procesos estén integrados con las Auditorías Operativas y Económicas de la Organización.

Contenido del Informe

A continuación ejemplificamos el contenido que podría incluir un INFORME DE AUDITORIA DE SISTEMAS:

- Objetivo
- Alcance
- Estructura Orgánico-Funcional del área Informática
- Configuración general de los Sistemas de Información
- Resultados de la Auditoría:
 - o Riesgo relevado
 - o Equipo relevado
 - o Descripción de la observación
 - o Criticidad relativa e IMPACTO EN EL NEGOCIO
 - o Acción detallada a implementar
 - o Plazo de solución
 - o Comentarios del responsable de la implementación
 - o Status a fecha del reporte final (implementado/pendiente)
 - o Documentación soporte / papeles de trabajo

En algunas ocasiones se desarrolla un resumen ejecutivo final a los responsables de la compañía:

- o Objetivo y alcance
- o Riesgos identificados y clasificados
- o Plan de acción concreto a implementar
 - Ø Corto Plazo
 - Ø Mediano Plazo
 - Ø Largo Plazo
- o Responsables de implementación y seguimiento

Implementación, Plan de Monitoreo y Mejora Continua

Teniendo en cuenta el enfoque de Mejora Continua de la Norma ISO 17799 (PLAN-DO-CHECK-ACT), es necesario que el proceso de AUDITORIA sea PERMANENTE a lo largo del año:

- Proactivas
- Detectivas

Cierre del Entrenamiento



**Facilidad en el USO vs. mejor PROTECCION
de la Información**