



INFORMATION SECURITY

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

MODULO 1: MARCO TEORICO ISO17799 / BS7799



INTRODUCCION GENERAL

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

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

Objetivos

Los objetivos de esta 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 Areas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores de las Tecnologías en general.

Descripción General

Este Programa Integral de Formación Profesional en IMPLEMENTACION PRACTICA de medidas de Seguridad de la Información está alineado con Normas Internacionales de aplicación en la materia y de acuerdo con Certificaciones Internacionales en Seguridad de la Información:

Normas Internacionales

- ISO177799
- BS7799

- ISO9001
- COBIT AUDIT GUIDELINES
- COSO
- ITIL
- SARBANES OXLEY ACT

Alineado con Certificaciones Internacionales

- CISSP
- CISA
- CISM
- CIA
- ISEC+
- COMPTia
- ETHICAL HACKER OSSTMM

A su vez sus contenidos están alineados con los Diplomados Internacionales distintas Universidades en Latinoamérica brindan (Argentina, Ecuador, Bolivia, Perú, Chile, entre otros).

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.

Temario Detallado

Este Programa consta de cuatro etapas:

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 PRACTICA DEL PROGRAMA DE SEGURIDAD - Parte 1

Se desarrollará la primera parte de 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. Esta Metodología Práctica se divide en 12 Módulos Funcionales de aplicación, y en esta primera parte se verán los primeros 6.

Etapa 3

IMPLEMENTACION PRACTICA 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.

Etapa 1

MARCO TEORICO ISO17799 / BS 7799

Objetivos

Los objetivos principales de este módulo son el lograr el conocimiento de:

- Por qué utilizar este estándar internacional
- Cómo se implementa un Programa de Gestión de Seguridad de la Información (ISMS)
- Cómo es un Proceso de Certificación de una Organización
- Principales controles definidos en cada uno de los Dominios de la ISO17799

1. Por qué utilizar ISO 17799

Paso 1: Por que?

El primer paso para abordar el tema de la Seguridad de la Información es:

Reconocer los riesgos y su impacto en los negocios

En etapas anteriores de la Academia se ha visto ya el VALOR que tiene la INFORMACION en una organización y los RIESGOS de los cuales es necesario protegerse.

También hemos visto que debemos tener en cuenta que se puede LOGRAR mucho para que los RIESGOS nos impacten lo menos posible:

- sin grandes inversiones en software
- sin mucha estructura de personal

Tan solo:

- **ordenando la Gestión de Seguridad**
- parametrizando la seguridad propia de los sistemas
- utilizando herramientas licenciadas y libres en la web

Paso 2:

Tenemos que tener en cuenta que:

Si igual voy a hacer algo, porque no lo hago teniendo en cuenta las Normas, Metodologías y Legislaciones Internacionales aplicables

Cuáles son esas Normas, Metodologías y Legislaciones aplicables?

Entre los distintos organismos que dictan resoluciones y que están relacionados comercial y/o institucionalmente con los temas de Seguridad de la Información, podemos encontrar los siguientes:

- Information Systems and Audit Control Association - ISACA: METODOLOGIA COBIT
- British Standards Institute: BS
- International Standards Organization: Normas ISO
- Departamento de Defensa de USA: Orange Book / Common Criteria
- ITSEC - Information Technology Security Evaluation Criteria: White Book
- Sarbanes Oxley Act, HIPAA Act, ...

Gestión de Seguridad Norma ISO 17799

Normas ISO en general

Podemos encontrar numerosas Normas internacionalmente aceptadas, pero aquellas que tienen gran aceptación en la comunidad de negocios son las relacionadas con **GESTION**, entre las que encontramos:

- ISO 9001 - Gestión de Calidad
- ISO 14001 - Gestión Ambiental
- ISO 17799 - Gestión de la Seguridad de la Información

La principal norma internacional de Evaluación, Implementación y Certificación de medidas de Seguridad en Tecnologías de la Información es la NORMA ISO 17799.

Está basada en una normativa local: el BRITISH STANDARD 7799 que le dio origen (BS7799-1 y BS7799-2).

El BS7799 que le dio origen consta de dos partes:

PARTE 1 . NORMALIZACION (Desarrollo de las Mejores Prácticas)

convertida luego en Norma ISO/IEC17799:2000

PARTE 2 . CERTIFICACION (Procesos de Auditoría para la Implementación)

(aún no fue convertida a Norma ISO)

Teniendo en cuenta que la PARTE 2 (mayormente utilizada para la CERTIFICACION) aún no fue publicada oficialmente por ISO, hoy en día las certificaciones son sobre el BS 7799-2.

La versión actualmente en uso de la NORMA ISO 17799 es del año 2000 y existe en el año 2005 un grupo de trabajo que está efectuando una versión revisada que puede ser que esté disponible hacia fines de 2005.

En la actualidad

Hoy en día la MAYORIA de las ORGANIZACIONES en el Mundo que están utilizando ISO17799 están en la primera etapa de NORMALIZACION alinéandose con los REQUERIMIENTOS a través de la IMPLEMENTACION del ISMS (INFORMATION SECURITY MANAGEMENT SYSTEM).

Algunas ya han pasado a la segunda etapa de CERTIFICACION (se explicará en Secciones posteriores).

Qué es ISO 17799?

Es un Código de Práctica para la Administración de la Seguridad de la Información.

A continuación se detallan las GENERALIDADES a tener en cuenta según la Norma:

Por qué proteger la Información?

La norma ISO 17799 asume esos condicionantes ya visto en la Academia en Etapas anteriores y define pasos a seguir para su protección:

VALOR

La información es un BIEN como el resto de los importantes activos comerciales.

MEDIO

La información puede existir en:

- en formato electrónico / magnético / óptico
- en formato impreso
- en el conocimiento de las personas

RIESGOS

Todos los riesgos vistos en etapas anteriores se resumen en tres grandes conceptos, al igual que en otras normativas, el fin principal es reservar la:

confidencialidad:

que la información sea accesible sólo a aquellas personas autorizadas a tener acceso.

integridad:

que se cumpla la exactitud y totalidad de la información y los métodos de procesamiento.

disponibilidad:

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

Objetivos del Programa ISO 17799

El alcance preciso de la Norma es brindar una serie de recomendaciones para la gestión de la seguridad de la información, y servir de base común para el desarrollo de estándares de seguridad, y poder implementar un conjunto adecuado de controles:

- políticas,

- prácticas,
- procedimientos,
- estructuras organizacionales, y
- funciones del software.

Este Código de Práctica es un punto de partida para el desarrollo de lineamientos específicos, aplicables a cada organización, considerando que NO todos los lineamientos y controles definidos resultan aplicables y que además probablemente deban agregarse controles que no están incluidos en esta Normativa.

También hay que tener en cuenta que según define la Normativa:

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

Cómo establecer los requerimientos MINIMOS de seguridad

Hay que analizar tres aspectos:

- Evaluar los riesgos que enfrenta la organización
- Identificar Requisitos EXTERNOS: legales, normativos, reglamentarios y contractuales
- Identificar Requisitos INTERNOS: principios, objetivos y requisitos para el procesamiento de la información que ha desarrollado la organización

Factores críticos del éxito

Tal como recomienda la NORMA, las principales consideraciones a tener en cuenta para poder cumplir con los objetivos planteados son:

- 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;
- distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas;
- instrucción 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.

NOTA: En las Etapas siguientes se definirán como implementar cada uno de estos requerimientos generales.

Contenido temático de la Norma

La norma ISO 17799 está organizada en diez DOMINIOS en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema para llevar adelante una correcta implementación:

- 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**

2. Cómo se implementa un Programa de Gestión de Seguridad de la Información (ISMS)

Porqué Implementar un ISMS / SISTEMA DE GESTION ISO17799?

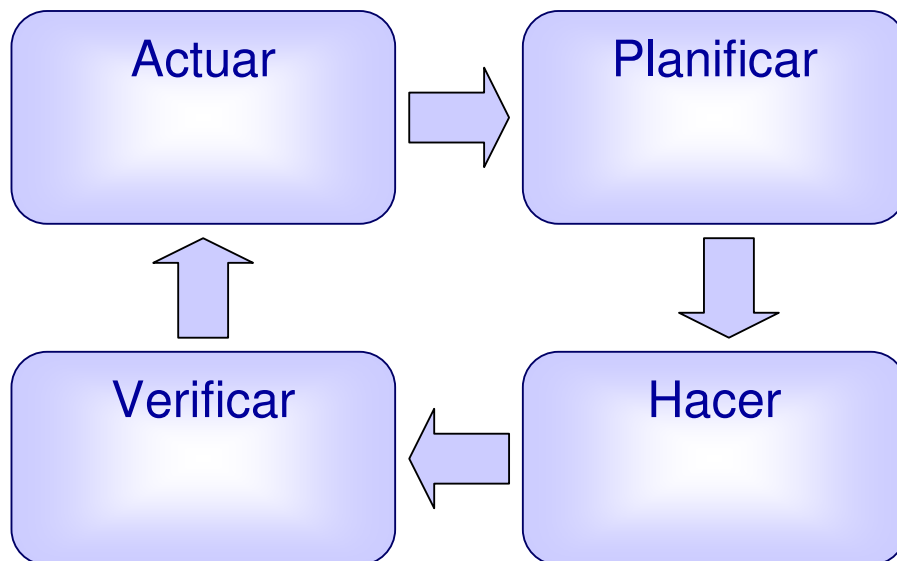
Algunas consideraciones generales de porqué implementarlo:

- Para poder tener una Metodológica dedicada a la seguridad de información reconocida internacionalmente
- Contar con un proceso definido para Evaluar, Implementar, Mantener y Administrar la seguridad de la información
- Diferenciarse en el mercado de otras organizaciones
- Satisfacer requerimientos de clientes, proveedores y Organismos de Contralor
- Potenciales disminuciones de costos e inversiones
- FORMALIZAR las responsabilidades operativas y LEGALES de los USUARIOS Internos y Externos de la Información
- Cumplir con disposiciones legales (por ej. Leyes de Protección de Datos, Privacidad, etc.)
- Tener una Metodología para poder ADMINISTRAR los RIESGOS

SGSI SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Está basado en el Modelo utilizado por las NORMAS ISO en general:

“Planificar - Hacer - Verificar - Actuar” (PHVA)”



Planificar (definir el SGSI)

Establecer los **CONTROLES** y **POLITICAS** / **PROCEDIMIENTOS** para la administración de los riesgos y mejora de la seguridad de la información.

Hacer (implementar y operar el SGSI)

Llevar adelante las acciones concretas definidas en los controles, los procesos y los procedimientos.

Verificar (realizar el seguimiento y revisar el SGSI)

Evaluar y medir el desempeño de los procesos respecto a las definiciones aprobadas e informar los resultados para la revisión.

Actuar (mantener y mejorar el SGSI)

Tomar acciones preventivas y correctivas para el logro de la **mejora continua** del SGSI.

NOTA: Estos conceptos están alineados con el estándar BS7799-2 relacionado con la Implementación de un SGSI.

Principales PASOS a seguir en la IMPLEMENTACION del SGSI

Implementación del SGSI en 12 PASOS:

Para un entendimiento PRACTICO del Proceso de IMPLEMENTACION del SGSI, se definen a continuación las principales TAREAS a incluir en el PLAN de ACCION son:

- 1) Definir el alcance del SGSI desde el punto de vista de las características de la actividad, la organización, su ubicación, sus activos y su tecnología
- 2) Definir una Política GENERAL del SGSI
- 3) Definir una METODOLOGIA para la CLASIFICACION de los RIESGOS
- 4) Identificar y Valorar los riesgos
- 5) Identificar y definir ALTERNATIVAS para el tratamiento de riesgos:
 - Aplicar controles
 - Aceptar los riesgos
 - Evitar riesgos
 - Transferir los riesgos asociados de las actividades a otras partes (ejemplo a Compañías de Seguros)
- 6) Seleccionar **objetivos de control** y controles específicos a IMPLMENTAR

El detalle de los controles se incluye en la Sección Dominios de ISO 17799.

Cualquier EXCLUSION de controles que se considera como necesaria para satisfacer el criterio de aceptación de riesgo, se debe justificar y se debe

proporcionar la evidencia. Cuando se realizan exclusiones, no se podrá alegar conformidad con esta norma a menos que dichas exclusiones no afecten la capacidad de la organización, y/o su responsabilidad para proveer seguridad de información cumpliendo con los requisitos de seguridad determinados por la evaluación de riesgo y los requisitos regulatorios aplicables.

7) Preparar una DDA Declaración de Aplicabilidad (qué CONTROLES se van a IMPLEMENTAR)

8) Obtener la aprobación de la Dirección de:

- DDA Declaración de Aplicabilidad
- Riesgos Residuales no cubiertos

9) Formular un plan CONCRETO y DETALLADO para:

- Tratamiento de los riesgos
- Controles a Implementar
- Programas de entrenamiento y concientización de usuarios
- Gestionar el SGSI
- Procesos de detección y respuesta a los incidentes de seguridad

10) Implementar los CONTROLES

- Controles en los Procesos de Usuarios
- Controles Automáticos en las Tecnologías
- Documentación Respaldatoria
- Registros Respaldatorios

11) Realizar Revisiones Periódicas (Auditoría Interna y la Dirección):

- controles implementados

- nuevos riesgos
- riesgos residuales

12) Implementar las mejoras identificadas en el SGSI

Requisitos FUNDAMENTALES de la Documentación SOPORTE en un SGSI

Es necesario también tener en cuenta que más allá de la implementación, es necesario el MANTENIMIENTO ACTUALIZADO Y PROTEGIDO de la Documentación Respaldataoria del SGSI, para lo cual hay que establecer:

- Documentación mínima de respaldo
- Procedimiento de Gestión de dicha documentación

Documentación MINIMA del SGSI:

- a) Declaraciones documentadas de la política de seguridad y los objetivos de control
- b) El alcance y los procedimientos y controles de apoyo
- c) El informe de evaluación de riesgos
- d) El plan de tratamiento de riesgo
- e) Los procedimientos documentados necesarios para la planificación, la operación y el control del SGSI
- f) Los registros requeridos:

Los registros se deben establecer y mantener para proveer evidencia de conformidad con los requisitos, deben permanecer legibles, fácilmente identificables y recuperables. Algunos ejemplos: logs de los sistemas para auditorías, formularios firmados de accesos, etc.

- g) La DDA Declaración de Aplicabilidad

Procedimiento de GESTION de la Documentación

Los documentos requeridos deben cumplir con los requerimientos FORMALES del ISMS para:

- a) aprobar los documentos previos a su distribución
- b) revisar y actualizar los documentos según la necesidad y aprobarlos nuevamente
- c) asegurarse de que los cambios y las revisiones de los documentos estén identificados
- d) asegurarse de que las versiones más recientes de los documentos pertinentes están disponibles en cualquier punto de uso
- e) asegurarse de que los documentos se mantengan legibles y fácilmente identificables
- f) asegurarse de que los documentos de origen externo estén identificados
- g) asegurarse de que la distribución de documentos este controlada
- h) prevenir el uso no intencionado de documentos obsoletos
- i) realizar una adecuada identificación si se retienen por cualquier causa

NOTA: existen Software que ayudan al mantenimiento de esta Gestión Documental disponibles en el mercado.

3. Cómo es un Proceso de Certificación de una Organización

Para poder entender cómo es el proceso de CERTIFICACION, a continuación se detallan algunos conceptos FUNDAMENTALES para entender dicho PROCESO.

QUÉ ES CERTIFICAR?

El proceso de Certificación es la Generación de un INFORME Firmado por parte de un TERCERO (ajeno a la organización) que define que, de acuerdo con su CRITERIO PROFESIONAL, dicha Organización CUMPLE o NO CUMPLE con los Requerimientos establecidos en la Normativa.

PORQUE CERTIFICAR?

Para poder Mostrar al Mercado que la Organización tiene un adecuado SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN.

Una empresa CERTIFICADA no implica que NO TIENE MAS RIESGOS DE SEGURIDAD DE LA INFORMACION, sino que tienen un adecuado Sistema de Gestión de dichos Riesgos y Proceso de MEJORA CONTINUA.

QUE ORGANIZACIONES PUEDEN CERTIFICAR?

Cualquier Organización, grande o pequeña, pública o privada, de Gobierno o sin fines de lucro, etc, está en condiciones y habilitada para CERTIFICARSE.

QUIENES ESTAN AUTORIZADOS A EFECTUAR LA CERTIFICACION?

Cualquier Agente ajeno a la Organización (Profesional Independiente o Compañía) puede Firmar el Informe antes mencionado.

Pero dado que la Certificación además de un valor Interno de Asegurarse de Cumplir con la Normativa, tiene un fin principal de poder Mostrar dicha Certificación al Mercado Externo, generalmente se recurre a Organizaciones que estén Técnicamente Aceptadas y además reconocidas INTERNACIONALMENTE para efectuar dicho trabajo. Por ello se recurre a

Organizaciones que estén ACREDITADAS (este es el término técnico utilizado) en el Organismo Internacional de Acreditación. Ejemplo de este tipo de Organizaciones son el Bureau Veritas BVQI, Det Norske Veritas DNV, TÜV, etc.

LA CERTIFICACION ES SEGÚN ISO 17799 O SEGÚN BS7799?

Tal como se comentó en Secciones anteriores, la Norma ISO 17799 está basado en el estándar británico BS7799, que tiene 2 partes:

BS7799-1 NORMALIZACION (Desarrollo de las Mejores Prácticas)

Convertido a ISO/IEC17799:2000

BS7799-2 IMPLEMENTACION SGSI/ CERTIFICACION (Procesos de Auditoría para la Implementación)

Aún no convertida a Norma ISO

Teniendo en cuenta que la PARTE 2 (mayormente utilizada para la CERTIFICACION) aún no fue publicada oficialmente por ISO, hoy en día las certificaciones son sobre el BS 7799-2.

En conclusión: las Organizaciones implementan de acuerdo a ISO17799-1 pero las Empresas Certificadoras utilizan el BS7799-2 para hacer los Informes de Certificación.

COMO ES EL PROCESO DE CERTIFICACION?

El requerimiento previo es que la Organización cumpla con la Implementación del SGSI definido en la Sección anterior.

Luego se convoca al Tercero para efectuar la CERTIFICACION.

Los principales PASOS son:

- 1) Preparar la Documentación Soporte a Presentar
- 2) Efectuar la PREAUDITORIA para conocer el GAP Analisis respecto al Estándar

- 3) Identificar conjuntamente:
 - a. las NO CONFORMIDADES (incumplimientos de acuerdo al Estándar)
 - b. las NO CONFORMIDADES que son ACEPTADAS (sólo se documentan los argumentos de justificación)
 - c. las NO CONFORMIDADES que NO son ACEPTADAS (se definen las MEJORAS a implementar)
- 4) Implementar las MEJORAS y Generar los Soportes Documentales correspondientes
- 5) Efectuar la AUDITORIA DE CERTIFICACION y Generación del Informe Final de Certificación incluyendo las NO CONFORMIDADES (aceptadas o NO y sus Riesgos Residuales aceptados por la Dirección de la Organización)
- 6) Gestionar los respaldos para la Acreditación Internacional de la Certificación lograda
- 7) Auditorías periódicas de la Empresa Certificadora para validar el continuo cumplimiento de los Requerimientos de la Normativa

PUEDE UNA ORGANIZACION PERDER LA CERTIFICACION?

Si una Organización no cumple con los requerimientos, puede ocurrir que en la Auditoría Periódica la Empresa Certificadora solicite que se saque la Certificación Obtenida inicialmente.

4. Principales controles definidos en cada uno de los Dominios de la ISO17799

Una vez comprendidos:

- el POR QUE usar la Normativa ISO 17799,
- Cómo Implementar el ISMS, y
- Cómo luego poder ser CERTIFICADO,

a continuación detallaremos cada uno de los principales CONTROLES que conforman cada uno de los 10 DOMINIOS de la ISO17799:

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

NOTA: en las Etapas 2 y 3 de la Academia se comentará la metodología de IMPLEMENTACION PRACTICA de cada uno de estos CONTROLES.

DOMINIO 1 POLÍTICA DE SEGURIDAD

Qué busca la Norma ISO 17799 en este Dominio?

Objetivo:

El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información.

Cuáles son los conceptos fundamentales para lograrlo?

Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados.

Debe garantizarse que se lleve a cabo una revisión periódica para tener en cuenta cualquier cambio que pueda afectar la situación original.

DOMINIO 2 ORGANIZACIÓN DE LA SEGURIDAD

Qué busca la Norma ISO 17799 en este Dominio?

2.1 Infraestructura de seguridad de la información

Objetivo:

Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización.

2.2 Seguridad frente al acceso por parte de terceros

Objetivo:

Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

2.3 Tercerización

Objetivo:

Mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue delegada a otra organización.

Cuáles son los conceptos fundamentales para lograrlo?

RESPONSABILIDADES

Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad.

Propietario de Datos

Una práctica común es designar a un propietario para cada recurso de información que además se haga responsable de su seguridad de manera permanente. Para ello, los Gerentes deben ser responsables de todas las actividades relacionadas con la seguridad para la Información que se utiliza en los procesos de su área de trabajo, para lo cual se deben establecer claramente las áreas sobre las cuales son responsables.

También se documentan las responsabilidades de cada uno y los accesos permitidos.

Oficial de Seguridad

Adicionalmente, en muchas organizaciones, se asigna a un gerente de seguridad de la información la responsabilidad general por el desarrollo, implementación y asesoramiento en materia de seguridad y por el soporte a la identificación de controles. No obstante, la responsabilidad por la reasignación e implementación de controles a menudo es retenida por cada uno de los gerentes.

Revision Independiente

También es necesaria la **revisión independiente** del ISMS para garantizar que las prácticas de la organización reflejan adecuadamente la política, por lo que dicha revisión puede ser llevada a cabo por la función de auditoría interna, por un gerente independiente o una organización externa especializada.

ACCESOS DE TERCEROS

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado, y previamente debe llevarse a cabo una evaluación de riesgos para 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.

Algunos ejemplos de Accesos

Tipos de acceso

- acceso físico
- acceso lógico

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.

TERCERIZACION

De igual manera que en la Sección anterior, los acuerdos de tercerización deben contemplar los riesgos, los controles de seguridad y los procedimientos para sistemas de información, redes y/o ambientes informáticos en el contrato entre las partes.

3 CLASIFICACIÓN Y CONTROL DE ACTIVOS

Qué busca la Norma ISO 17799 en este Dominio?

3.1 Responsabilidad por rendición de cuentas de los activos

Objetivo: Mantener una adecuada protección de los activos de la organización.

3.2 Clasificación de la información

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

Cuáles son los conceptos fundamentales para lograrlo?

INVENTARIO DE ACTIVOS

Se debe efectuar un INVENTARIO de ACTIVOS (información y recursos relacionados con el uso / procesamiento de la Información).

Se debe designar un propietario para cada uno de los ACTIVOS IMPORTANTES (en el Dominio anterior ya se definió la necesidad de Identificar FORMALMENTE los Responsables por cada Activo relacionado con la Información).

Tal como lo define la Norma, algunos ejemplos de activos asociados a sistemas de información son los siguientes:

- a) 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, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada;
- b) recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- c) activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos

- (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento ;
- d) servicios: servicios informáticos y de comunicaciones, utilitarios generales, por ej., calefacción, iluminación, energía eléctrica, aire acondicionado.

CLASIFICACION DE LA INFORMACION Y ACTIVOS

La información debe ser clasificada utilizando 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.

Pautas de clasificación

- Se debe tomar cuenta de las necesidades de la empresa con respecto a la distribución (uso compartido) o restricción de la información, y de la incidencia de dichas necesidades en las actividades de la organización.
- Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo.
- También es necesario tener en cuenta la clasificación por exceso ("todo es crítico").

4 SEGURIDAD DEL PERSONAL

Qué busca la Norma ISO 17799 en este Dominio?

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

Objetivo:

Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

4.2 Capacitación del usuario

Objetivo:

Garantizar que los usuarios conocen las amenazas y sus responsabilidades en materia de seguridad de la información en el transcurso de sus tareas normales.

4.3 Respuesta a incidentes y anomalías en materia de seguridad

Objetivo:

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

Cuáles son los conceptos fundamentales para lograrlo?

PUESTOS DE TRABAJOS

Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.

Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados, especialmente si se trata de tareas críticas.

Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad.

Los usuarios externos aún no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso a las instalaciones de procesamiento de información.

CAPACITACION

Todos los empleados de la organización y los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles del negocio, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información.

Este Programa de Capacitación y Concientización debe ser CONTINUO y MEDIBLE.

ADMINISTRACION DE INCIDENTES

Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.

Se debe concientizar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la organización.

Para lograr manejar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto como sea posible una vez ocurrido el hecho.

Deberán implementarse adecuados procesos de "feedback" para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos los mismos.

Debe haberse implementado mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías (ejemplo, utilización de TABLEROS DE CONTROL).

PROCESO DISCIPLINARIO

La organización debe establecer un proceso disciplinario formal para ocuparse de los empleados que no cumplan con las Políticas de Seguridad.

5 SEGURIDAD FÍSICA Y AMBIENTAL

Qué busca la Norma ISO 17799 en este Dominio?

5.1 Áreas seguras

Objetivo:

Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

5.2 Seguridad del equipamiento

Objetivo:

Impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.

5.3 Controles generales

Objetivo:

Impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma.

Cuáles son los conceptos fundamentales para lograrlo?

AREAS SEGURAS

Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados.

La protección provista debe ser proporcional a los riesgos identificados.

El personal sólo debe tener conocimiento de la existencia de un área protegida, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información.

Algunas consideraciones adicionales:

- a) Los visitantes deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados.
- b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas, y se debe mantenerse una pista protegida que permita auditar todos los accesos.
- c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible.
- d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.
- e) Las instalaciones claves deben ubicarse en lugares a los cuales no pueda acceder el público.
- f) Los sitios de procesamiento de información deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- g) Se deben implementar adecuados sistemas de detección de intrusos.
- h) Las instalaciones de procesamiento de información administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.
- i) Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área protegida.
- j) El equipamiento de sistemas de soporte de reposición de información perdida y los medios informáticos de resguardo deben estar situados a una distancia prudencial para evitar daños ocasionados por eventuales desastres en el sitio principal.

SEGURIDAD DEL EQUIPAMIENTO

El equipamiento debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales y oportunidades de acceso no autorizado.

Algunas de las amenazas identificadas en la Norma son:

- 1) robo
- 2) incendio
- 3) explosivos
- 4) humo
- 5) agua (exceso o falta de suministro)
- 6) polvo
- 7) vibraciones
- 8) efectos químicos
- 9) interferencia en el suministro de energía eléctrica
- 10) radiación electromagnética

Suministros de energía

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas:

- a) múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía
- b) suministro de energía ininterrumpible (UPS)
- c) generador de respaldo.

Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.

Mantenimiento de equipos

El equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes, respetando los intervalos de servicio y especificaciones recomendados por el proveedor, manteniendo un registro del personal de mantenimiento autorizado y de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo, tanto sea para equipos dentro de la Organización o cuando se retiran.

Baja o reutilización de equipamiento

Los medios de almacenamiento conteniendo material sensible, deben ser físicamente destruidos o sobrescritos en forma segura.

POLITICAS DE ESCRITORIOS Y PANTALLAS LIMPIAS

Se recomienda la implementación políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información.

6 GESTIÓN DE COMUNICACIONES Y OPERACIONES

Qué busca la Norma ISO 17799 en este Dominio?

6.1 Procedimientos y responsabilidades operativas

Objetivo:

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

6.2 Planificación y aprobación de sistemas

Objetivo:

Minimizar el riesgo de fallas en los sistemas.

6.3 Protección contra software malicioso

Objetivo:

Proteger la integridad del software y la información.

6.4 Mantenimiento

Objetivo:

Mantener la integridad y disponibilidad de los servicios de procesamiento y comunicación de información.

6.5 Administración de la red

Objetivo:

Garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo.

6.6 Administración y seguridad de los medios de almacenamiento

Objetivo:

Los medios de almacenamiento deben ser controlados y protegidos lógicamente y físicamente.

6.7 Intercambios de información y software

Objetivo:

Impedir la pérdida, modificación o uso inadecuado de la información que intercambian las organizaciones.

Cuáles son los conceptos fundamentales para lograrlo?

OPERACIÓN DE LOS EQUIPOS

Dentro del Área de Sistemas y/o Tecnología, se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información, teniendo en cuenta la correcta SEGREGACION DE FUNCIONES desde el punto de vista de control interno.

Documentación de los procedimientos operativos

Se deben documentar y mantener los procedimientos operativos, que deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.

Control de cambios en las operaciones

Se deben implementar responsabilidades y procedimientos gerenciales formales para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software o los procedimientos.

Cuando se cambian los programas, se debe retener un registro de auditoría que contenga toda la información relevante:

- a) identificación y registro de cambios significativos
- b) evaluación del posible impacto de dichos cambios
- c) procedimiento de aprobación formal de los cambios propuestos
- d) comunicación de detalles de cambios a todas las personas pertinentes
- e) procedimientos que identifican las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Separación de funciones

Se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios.

Las pequeñas organizaciones pueden encontrar este método de control difícil de cumplir, pero el principio debe aplicarse en la medida de lo posible.

Siempre que sea difícil llevar a cabo la separación, se deben tener en cuenta otros controles como el monitoreo de las actividades, las pistas de auditoría y la supervisión gerencial.

Separación entre instalaciones de desarrollo e instalaciones operativas

La separación entre las instalaciones de desarrollo, prueba y operaciones es importante para lograr la separación de los roles involucradas.

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

Se deben utilizar diferentes procedimientos de conexión para sistemas en operaciones y de prueba.

PLANIFICACION Y APROBACION DE SISTEMAS

Se requiere una planificación y preparación anticipada de los sistemas, efectuando proyecciones para futuros requerimientos de capacidad y documentando y probando los requerimientos operativos de nuevos sistemas antes de su aprobación y uso.

Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados.

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Es necesario instalar mecanismos automáticos para prevenir y detectar la introducción de software malicioso, así como procedimientos de gestión adecuados para prevenir y minimizar el impacto de los daños.

Según marca la Norma, es necesario tener:

- a) una política formal que requiera el uso de software con licencia y prohíba el uso de software no autorizado
- b) una política formal con el fin de proteger contra los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas
- c) instalación y actualización periódica de software de detección y reparación antivirus
- d) realización de revisiones periódicas del contenido de software y datos de los sistemas que sustentan procesos críticos de la empresa
- e) verificación de la presencia de virus en archivos de medios electrónicos de origen incierto o no autorizado, o en archivos recibidos a través de redes no confiables, antes de su uso
- f) verificación de la presencia de software malicioso en archivos adjuntos a mensajes de correo electrónico y archivos descargados por Internet antes de su uso
- g) adecuados planes de continuidad de los negocios para la recuperación respecto de ataques de virus
- h) adecuados planes de concientización de usuarios
- i) revisar los boletines de alerta a fin de estar actualizados preventivamente y evitar virus falsos

MANTENIMIENTO

Se deben establecer procedimientos para llevar a cabo la estrategia de resguardo acordada, realizando copias de resguardo de los datos y pruebas de su correcto restablecimiento.

Se debe determinar el período de guarda de la información esencial para la empresa de acuerdo con requerimientos internos y externos (legales, impositivos, etc).

ADMINISTRACION DE LA RED

Los administradores de redes deben implementar controles para garantizar la seguridad de los datos y la protección de los servicios conectados contra el acceso no autorizado.

ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, casetes), datos de entrada/salida y documentación, tanto para:

- Conservación
- Retiro
- Destrucción

Algunos ejemplos que define la Norma son:

- 1) documentos en papel,
- 2) voces u otras grabaciones;
- 3) papel carbónico;
- 4) informes de salida,
- 5) cintas de impresora de un solo uso;
- 6) cintas magnéticas;
- 7) discos o casetes removibles;
- 8) medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor);
- 9) listados de programas;
- 10) datos de prueba;
- 11) documentación del sistema,

SEGURIDAD DE LA DOCUMENTACIÓN DEL SISTEMA

La documentación del sistema puede contener cierta cantidad de información sensible, por ej. descripción de procesos de aplicaciones, procedimientos, estructuras de datos, etc, por lo que debe ser protegida.

INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE

Los intercambios de información y software entre organizaciones deben ser controlados, cumpliendo con la legislación vigente y de acuerdo con los acuerdos FORMALES existentes.

Para los envíos de información física, deben considerarse:

- a) medios de transporte o servicios de mensajería confiables
- b) uso de recipientes cerrados
- c) entrega en mano
- d) embalaje a prueba de apertura no autorizada
- e) en casos excepcionales, división y envío por diferentes rutas

Para los intercambios de información electrónica:

Puede comprender:

- el uso de intercambio electrónico de datos
- correo electrónico
- y transacciones en línea a través de redes públicas como Internet

Las consideraciones generales a tener en cuenta son entre otras cosas:

- a) Autenticación
- b) Autorización
- c) Confidencialidad
- d) Integridad
- e) Prueba de envío, recepción y no repudio
- f) Validez de los datos de la transacción
- g) Evidencia del Cierre de la transacción
- h) Responsabilidad legal y comercial ante fraudes

Gran parte de las consideraciones mencionadas pueden resolverse mediante la aplicación de las técnicas criptográficas.

7 CONTROL DE ACCESOS

Qué busca la Norma ISO 17799 en este Dominio?

7.1 Requerimientos de negocio para el control de accesos

Objetivo:

Controlar el acceso de información.

7.2 Administración de accesos de usuarios

Objeto:

Impedir el acceso no autorizado en los sistemas de información.

7.3 Responsabilidades del usuario

Objeto:

Impedir el acceso usuarios no autorizados

7.4 Control de acceso a la red

Objetivo:

La protección de los servicios de red.

7.5 Control de acceso al sistema operativo

Objetivo:

Impedir el acceso no autorizado a los recursos informáticos.

7.6 Control de acceso a las aplicaciones

Objetivo:

Impedir el acceso no autorizado a la información contenida en los sistemas de información.

7.7 Monitoreo del acceso y uso de los sistemas

Objetivo:

Detectar actividades no autorizadas

7.8 Computación móvil y trabajo remoto

Objetivo:

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remotas.

Cuáles son los conceptos fundamentales para lograrlo?

Las consideraciones definidas en la Norma para este Dominio son las que generalmente se considera como SEGURIDAD LOGICA.

REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

Se deben cumplir las siguientes definiciones:

- definir y documentar los requerimientos de negocio para el control de accesos

- diferenciar entre reglas que siempre deben imponerse y reglas optativas o condicionales
- establecer reglas sobre la base de la premisa “Todo esta prohibido excepto lo que esté AUTORIZADO formalmente”

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, considerando:

- a) uso de IDs de usuario únicos
- b) uso de IDs grupales solo por excepción y autorizados
- c) firma de usuarios aceptando sus responsabilidades
- d) verificar periódicamente IDs en los sistemas
- e) cancelar IDs y cuentas de usuarios redundantes
- f) los IDs de usuario no deben dar ningún inicio del nivel de privilegio del usuario

REVISIÓN DE DERECHOS DE ACCESO DE USUARIO

La gerencia debe llevar a cabo un proceso formal a intervalos regulares (la norma define 6 meses para usuarios comunes y 3 meses para privilegios especiales), a fin de revisar los derechos de acceso de los usuarios.

ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO

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

De acuerdo a lo específicamente definido en la Norma, los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, notificándolos que deben:

- a) mantener las contraseñas en secreto;
- b) evitar mantener un registro en papel de las contraseñas, a menos que este pueda ser almacenado en forma segura;
- c) cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas;
- d) seleccionar contraseñas de calidad, con una longitud mínima de **seis** caracteres que:
 - 1) sean fácil de recordar;

- 2) no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ej. nombres, números de teléfono, fecha de nacimiento, etc. ;
 - 3) no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- e) cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas ;
 - f) cambiar las contraseñas provisionales en el primer inicio de sesión
 - g) no incluir contraseñas en los procesos automatizados de inicio de sesión, por ej. aquellas almacenadas en una tecla de función o macro ;
 - h) no compartir las contraseñas individuales de usuario;
 - i) utilizar protectores de pantallas de las terminales con CONTRASEÑA;
 - j) firmar una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto

Se debe evaluar el uso de otras tecnologías de identificación y autenticación de usuarios, como la biométrica, verificación de firma, uso de elementos de hardware, etc.

CONTROL DE ACCESO A LA RED

Se debe controlar el acceso a los servicios de red tanto internos como externos, garantizando:

- a) interfaces inadecuadas entre la red de la organización y las redes de otras organizaciones, o redes públicas ;
- b) mecanismos de autenticación apropiados para usuarios y equipamiento ;
- c) control de acceso de usuarios a los servicios de información.

Camino forzado

El objetivo de un camino forzado es evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo está autorizado a acceder.

Autenticación de usuarios para conexiones externas

El acceso de usuarios remotos debe estar sujeto a mecanismos APROBADOS de autenticación, considerando:

- técnicas basadas en criptografía,
- “tokens” de hardware,
- protocolos de pregunta/respuesta,
- líneas dedicadas privadas,
- herramientas de verificación de la dirección del usuario de red,
- procedimientos y controles de rellamada,
- autenticación de nodos, etc.

El acceso a los puertos de diagnóstico debe ser controlado de manera segura.

Subdivisión de redes

Se debe considerar la SEGMENTACIÓN DE LA RED, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

Control de ruteo de red

Como medida adicional de seguridad, es necesario verificar específicamente las direcciones de origen y destino y proceder en la medida de lo posible a la traducción de direcciones de red.

CONTROL DE ACCESO AL SISTEMA OPERATIVO

De acuerdo con lo definido por la Norma, los mecanismos de seguridad a nivel del sistema operativo deben permitir:

- identificar y verificar la identidad de USUARIO y TERMINAL
- registrar los accesos exitosos y fallidos
- suministrar medios de autenticación apropiados
- restringir los tiempos de conexión
- no desplegar identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión
- desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder a la computadora

- no dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión
- validar la información de la conexión sólo al completarse la totalidad de los datos de entrada ;
- limitar el número de intentos de conexión no exitosos permitidos (tres) y considerar:
 - registrar los intentos no exitosos ;
 - implementar una demora obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización específica ;
- limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión ;
- desconectar luego de cierto tiempo de inactividad;
- desplegar la siguiente información al completarse una conexión exitosa:
 - flechas y hora de la conexión exitosa anterior;
 - detalles de los intentos de conexión no exitosos desde la última conexión exitosa.
- Restringir el horario de conexión a las aplicaciones de alto riesgo;

ALARMAS SILENCIOSAS PARA LA PROTECCIÓN DE LOS USUARIOS

Según la Norma, debe considerarse la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción, luego de aprobado formalmente por la Dirección.

CONTROL DE ACCESO A LAS APLICACIONES

Se deben respetar las condiciones de protección antes mencionadas, pero considerando algunas particularidades de los Sistemas de Aplicación:

- Uso de menús de accesos
- Aislamiento de sistemas sensibles de la red corporativa
- Limitación de los privilegios a datos (lectura, escritura, supresión y ejecución)

MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS

Los sistemas deben ser monitoreados para detectar desviaciones respecto de la política de control de accesos y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad.

De acuerdo a lo definido en la Norma, **los registros de auditorias** también deben incluir en la medida de lo posible:

- a) ID de usuario;
- b) Fecha y hora de inicio y terminación;
- c) Identidad o ubicación de la terminal;
- d) Registros de intentos exitosos fallidos de acceso al sistema ;
- e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

Algunas de las principales actividades a monitorear definidas en la Norma son:

- a) accesos no autorizados
- b) todas las operaciones con privilegios como ser por ejemplo:
 - 1) Utilización de cuenta de supervisor;
 - 2) Inicio y cierre del sistema;
 - 3) Conexión y desconexión de dispositivos;
- c) intentos de acceso no autorizados:
 - 1) Intentos fallidos;
 - 2) Violaciones de la política de accesos;
 - 3) Alertas de sistemas para detención de intrusiones ;
- d) alertas o fallas de sistema como:
 - 1) alertas o mensajes;
 - 2) excepciones del sistema de registro;
 - 3) alarmas del sistema de administración de redes.

Sincronización de relojes

La correcta configuración de los relojes de las computadoras es importante para garantizar la exactitud de los registros de auditoria, que pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios.

COMPUTACIÓN MÓVIL Y TRABAJO REMOTO

Cuando se utilizan dispositivos informáticos móviles, por ej. notebooks, palmtops, laptops, teléfonos móviles, etc, se debe adoptar una política formal que tome en cuenta los riesgos y defina los controles necesarios para cada tipo de tecnología.

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar fuera de la organización, por lo que es importante que sea autorizado y controlado por la gerencia, y que se implementen adecuados mecanismos de seguridad, tanto físico como lógicos.

Para ambas situaciones ya se han definido en secciones anteriores los controles necesarios.

8 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Qué busca la Norma ISO 17799 en este Dominio?

8.1 Requerimientos de seguridad de los sistemas

Objetivo:

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

8.2 Seguridad en los sistemas de aplicación

Objetivo:

Prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación.

8.3 Controles criptográficos

Objetivo:

Proteger la confidencialidad, autenticidad o integridad de la información a través del uso de técnicas criptográficas.

8.4 Seguridad de los archivos del sistema

Objetivo:

Garantizar que los proyectos y actividades de soporte de TI se lleven a cabo de manera segura.

8.5 Seguridad de los procesos de desarrollo y soporte

Objetivo:

Mantener la seguridad del software y la información del sistema de aplicación en los distintos entornos de los proyectos y sistemas.

Cuáles son los conceptos fundamentales para lograrlo?

REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS

Se deben implementar los esquemas de seguridad para:

- Infraestructura tecnológica
- Servicios de red
- Aplicaciones comerciales
- Aplicaciones desarrolladas por el usuario

Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información, y deben comprender:

- controles automáticos a incorporar al sistema y
- controles manuales de apoyo.

SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN

Se deben diseñar en los sistemas de aplicación los controles de validación de datos de:

- entrada,
- procesamiento interno y
- salida de datos

CONTROLES CRIPTOGRÁFICOS

Dentro del desarrollo de los sistemas se deben utilizar sistemas y técnicas criptográficas para la protección de software y datos.

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos.

Se den tomar recaudos para proteger la integridad y confidencialidad de las claves privadas y públicas usadas en la encriptación y en las firmas digitales, utilizando procedimientos formales, propietarios para las claves, certificados externos de claves, uso de algoritmos seguros, adecuada longitud de las claves, entre otras consideraciones.

SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

Se debe controlar el acceso a los archivos del sistema en todas sus etapas de desarrollo, testeo y puesta en producción, tanto para los programas fuentes como los objeto o ejecutables.

Si se define el uso de archivos reales para propósitos de prueba, deberían efectuarse procesos de DESPERSONALIZACION.

Los listados de programas deben ser almacenados en un ambiente seguro.

Las viejas versiones de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operaciones, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.

SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE

Es necesario conocer que según la NORMA: Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte. De esta manera, delegan generalmente en el Gerente de Sistemas / Tecnología esta función de control.

Restricción del cambio en los paquetes de software

Según la Norma, se debe desalentar la realización de modificaciones a los paquetes de software con el objetivo de no agregar nuevos riesgos de seguridad.

En caso de producirse, todos los cambios deben ser probados y documentados exhaustivamente, de manera que pueden aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software.

Canales ocultos y código troyano

La Norma sugiere en la medida de lo posible (algunas de estas definiciones son de difícil ejecución):

- a) solo comprar programas de proveedores acreditados;
- b) comprar programas en código fuente de manera que el mismo pueda ser verificado;
- c) utilizar productos evaluados;
- d) examinar todo el código fuente antes de utilizar operativamente el programa;
- e) controlar el acceso y las modificaciones al código una vez instalado el mismo;
- f) emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

Desarrollo externo de software

Cuando se terceriza el desarrollo de software, la Norma sugiere que se deben considerar algunos conceptos adicionales:

- a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual;
- b) certificación de la calidad y precisión del trabajo llevado a cabo;
- c) acuerdos de custodia en caso de quiebra de la tercera parte;
- d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;
- e) requerimientos contractuales con respecto a la calidad del código;
- f) realización de pruebas previas a la instalación para detectar códigos troyanos.

9 ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

Qué busca la Norma ISO 17799 en este Dominio?

9.1 Aspectos de la administración de la continuidad de los negocios

Objetivo:

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

Cuáles son los conceptos fundamentales para lograrlo?

ASPECTOS DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

Según la Norma, se debe implementar un **proceso de administración de la continuidad de los negocios** para reducir la **discontinuidad ocasionada por desastres y fallas de seguridad** (que pueden ser el resultado de, por ej., desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptables mediante una combinación de controles preventivos y de recuperación.

Para ello es imprescindible analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio previamente, para luego poder definir e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.

La responsabilidad por la coordinación del proceso de administración de la continuidad debe ser asignada a un nivel jerárquico adecuado dentro de la organización, por ej. al foro de seguridad de la información (ver 4.1.1).

Proceso general de administración de la continuidad de los negocios

Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad de los negocios en toda la organización considerando:

- a) Definición del **equipo responsable** del Desarrollo del Plan
- b) **Identificación de los riesgos** que enfrenta la organización
- c) Análisis de la **probabilidad de ocurrencia** de las causas generadoras de dichos riesgos
- d) **Inventario y clasificación de los procesos más críticos** de los negocios
- e) Análisis del **impacto en dichos procesos de los riesgos mas frecuentes**
- f) Elaboración y documentación de una **estrategia de continuidad** de los negocios (que incluye incidentes de mayor y menor impacto)
- g) Elaboración y documentación de **planes detallados**
- h) Capacitación adecuada del personal en materia de procedimientos y procesos de emergencia, incluyendo el manejo de crisis
- i) Desarrollo de **pruebas y actualización periódicas** de los planes y procesos implementados;
- j) Garantizar que la administración de la continuidad de los negocios esté incorporada a los **procesos y estructura** de la organización, incluyendo responsables de su actualización, plazos de revisión, etc

Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios

A continuación se detallan algunas de los procedimientos de Prueba sugeridos por la Norma:

- a) pruebas de discusión de diversos escenarios;
- b) simulaciones;
- c) pruebas de recuperación técnica;
- d) pruebas de recuperación en un sitio alternativo;
- e) pruebas de instalaciones y servicios de proveedores;
- f) ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones);

Mantenimiento y reevaluación del plan

Algunas de las razones que considera la norma para definir como "necesaria" la reevaluación del Plan, pueden ser ante cambios de:

- a) personal
- b) direcciones o números telefónicos;
- c) estrategia de los negocios;
- d) ubicación, instalaciones y recursos;

- e) legislación;
- f) contratistas, proveedores y clientes clave;
- g) procesos, o procesos nuevos/eliminados;
- h) riesgos (operacionales y financieros).

10 CUMPLIMIENTO

Qué busca la Norma ISO 17799 en este Dominio?

12.1 Cumplimiento de requisitos legales

Objetivo:

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.

12.2 Revisiones de la política de seguridad y la compatibilidad técnica

Objetivo:

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

12.3 Consideraciones de auditoria de sistemas

Objetivo:

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

Cuáles son los conceptos fundamentales para lograrlo?

CUMPLIMIENTO DE REQUISITOS LEGALES

Debido a que el diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual, se debe procurar el asesoramiento pertinente, para poder identificarlos fehacientemente.

La Norma enfoca específicamente consideraciones para:

Derechos de propiedad intelectual (DPI)

Uso legal del material respecto del cual puedan existir derechos de propiedad intelectual (software, bases de datos, información, diseños, entre otros).

La norma sugiere principalmente:

- a) publicación de una política formal de cumplimiento del uso legal de productos de información y de software;
- b) emisión de estándares para los procedimientos de adquisición de productos de software;
- c) mantenimiento adecuados de registros de activos;
- d) comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;
- e) emisión de una política con respecto a la eliminación o transferencia de software a terceros;
- f) utilización de herramientas de auditoría adecuadas;
- g) cumplimiento de términos y condiciones con respecto a la obtención de software e información en redes públicas.

Protección de los registros de la organización

Dado que algunos registros pueden requerir una retención segura para cumplir con requisitos legales o normativos, así como para respaldar actividades esenciales del negocio, o como evidencias legales, dichos registros deben tener mecanismos para evitar la pérdida, destrucción y/o falsificación.

Se debe considerar también la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros.

Por ello, si se seleccionan medios de almacenamiento electrónicos, deben incluirse procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Protección de datos y privacidad de la información personal

Es necesario tener en cuenta si existiera legislación relacionada con datos personales que implique responsabilidades a aquellas personas que recopilan, procesan y divulgan información personal, y pueden limitar la capacidad de transferir dichos datos.

Prevención del uso inadecuado de los recursos de procesamiento de información

Los recursos de procesamiento de información de una organización se suministran con propósitos de negocio, y la gerencia debe autorizar el uso que se da a los mismos, por lo que la utilización de estos recursos con propósitos no autorizados o ajenos a los negocios, sin la aprobación de la gerencia, debe ser considerada como **uso indebido**. Los empleados y los usuarios externos deben ser advertidos de la prohibición de todo acceso que no esté expresamente autorizado.

La legalidad del monitoreo del uso de los recursos mencionados varía en cada legislación y puede requerir que los empleados sean advertidos de dichas actividades o que se obtenga el consentimiento de los mismos. Se debe obtener asesoramiento jurídico antes de implementar los procedimientos de monitoreo.

Regulación de controles para el uso de criptografía

Se deben tener en cuenta también que algunos países han implementado acuerdos, leyes, normas y demás instrumentos para controlar el acceso a los controles criptográficos o el uso de los mismos.

Recolección de evidencia

Cuando un control definido en la normativa interna, implica la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con las normas de evidencia establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso.

REVISIONES DE LA POLÍTICA DE SEGURIDAD Y LA COMPATIBILIDAD TÉCNICA

La seguridad de los sistemas de información debe revisarse periódicamente de acuerdo con las políticas vigentes.

Cada Gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad.

Entre las áreas a revisar deben incluirse las siguientes:

- a) sistemas de información;
- b) proveedores de sistemas;
- c) propietarios de información y de recursos de información;
- d) usuarios;
- e) gerentes.

La verificación de compatibilidad también puede comprender pruebas de penetración, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito.

CONSIDERACIONES DE AUDITORIA DE SISTEMAS

Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoría en el transcurso de las auditorías de sistemas, entre ellos:

- a) los responsables de la auditoría deben tener un acceso de sólo lectura del software de datos
- b) el acceso que no sea de sólo lectura solamente debe permitirse para copias aisladas de archivos del sistema
- c) todos los accesos deben ser monitoreados y registrados a fin de generar una pista de referencia;
- d) se deben documentar todos los procedimientos, requerimientos y responsabilidades
- e) Las herramientas de auditoría deben estar conservadas en ambientes protegidos