DIPLOMATURA INTERNACIONAL
MANAGER
SEGURIDAD DE LA INFORMACION

2016

Martin Vila
martin.vila@isec-global.com

Dirección del Programa

Martín Diego Vila Toscano
Business Director ISEC Information Security (2002- 2016)

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, dirigido y participado en Information Security Courses en USA, Latinoamérica y principalmente en Argentina.

Objetivo

Adquirir conocimientos, metodologías y herramientas de implementación para el proceso de

INFOSEC MANAGEMENT

PRIMERA ETAPA

RISK ASSESMENT

SEGUNDA ETAPA

INFORMATION SECURITY MANAGEMENT SYSTEM

INFORMATION SECURITY MANAGEMENT SYSTEM

QUE TAMBIEN REQUIERE DE

PROTECCION LOGICA Y FISICA DE REDES Y EQUIPOS TECNOLOGICOS
PROTECCION FISICA DE MAQUINARIAS
SEGURIDAD DE EJECUTIVOS
INTELIGENCIA Y CONTRAINTELIGENCIA

ASPECTOS LEGALES
ANALISIS FORENSE
CONTINUIDAD DEL NEGOCIO
CONCIENTIZACION DE USUARIOS
CUMPLIMIENTO DE NORMAS
PROTECCION DE TELEFONIA FIJA Y MOVIL, VIDEOCONFERENCIAS, MICROFONOS
ETC ETC

NORMAS APLICABLES

- Information Systems and Audit Control Association - ISACA: **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
- Sans Institute, Security Focus, etc
- Sarbanes Oxley Act, Basilea II, HIPAA Act, **Leyes NACIONALES**
- **ITIL, PCI**
- OSSTMM, ISM3, **ISO27001, ISO27002, ISO27005, ISO31000, ISO270XX**
- **Regulaciones locales**

Elegimos la más aceptada a nivel mundial

Norma ISO 27001/2 y sus relacionadas

Gestión de Seguridad

Normas de Gestión ISO

- ISO9001 – Calidad
- ISO14001 – Ambiental

- **ISO27002 – Seguridad de la Información - NORMALIZACION (Mejores Prácticas)**

- **ISO 27001 – CERTIFICACION de Seguridad de la Información**

Norma ISO 27001/2 Seguridad de la Información

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

GESTION DE SEGURIDAD DE LA INFORMACION

Alcance

Recomendaciones para la gestión de la seguridad de la información

Base común para el desarrollo de estándares de seguridad

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27003: DISEÑO DE SGSI

Publicada en 2010. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

ISO/IEC 27004: METRICAS

Publicada en 2009. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

ISO/IEC 27005: GESTION DE RIESGOS

Publicada en 2011. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27006: ACREDITACION DE ENTIDADES

Publicada en 2011. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO/IEC 27007: GUIA DE AUDITORIA GENERAL

Publicada en 2011. Es una guía de auditoría de un SGSI.

ISO/IEC TR 27008: GUIA DE AUDITORIA ESPECIFICA

Publicada en 2011. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

ISO/IEC 27009: APLICACIÓN A SERVICIOS

En proceso. Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios especifícos en emisión de certificaciones acreditadas de tercera parte.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27010: INTERCAMBIO DE INFORMACION

Publicada en 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores, y es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.

ISO/IEC 27011: APLICACIÓN A ORGANIZACIONES DE TELECOMUNICACIONES

Publicada en 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

ISO/IEC 27013: SEGURIDAD INTEGRADA CON GESTION DE SERVICIOS

Publicada en 2012. Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014: GOBIERNO DE LA SEGURIDAD

Publicada en 2013. Consiste en una guía de gobierno corporativo de la seguridad de la información.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC TR 27015: APLICACIÓN A ORGANIZACIONES DE SECTOR FINANCIERO

Publicada en 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

ISO/IEC TR 27016: ASPECTOS FINANCIEROS DEL SGSI

Publicada en 2014. Consiste en una guía de valoración de los aspectos financieros de la seguridad de la información.

ISO/IEC TS 27017: SEGUIRDAD EN CLOUD COMPUTING

Publicada en 2014. Consiste en una guía de seguridad para Cloud Computing.

ISO/IEC 27018: PROTECCION DE DATOS EN CLOUD COMPUTING

Publicada en 2014. Consiste en un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

ISO/IEC TR 27019: APLICACIÓN A ORGANIZACIONES DE SECTOR ENERGIA

Publicada en 2013. Guía con referencia a ISO/IEC 27002 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC TR 27021: COMPETENCIAS REQUERIDAS PARA UN PROFESIONAL DE SEGURIDAD

En proceso. Guía para los skills necesarios para un Profesional de Seguridad de la Informacion.

ISO/IEC TR 27023: COMPARATIVO ENTRE VERSION ANTERIOR Y ACTUAL DE ISO27001/2

Publicada en 2013. Guía para mapear las diferencias entre las versiones anterior y actual de las ISO27001/2.

ISO/IEC 27031: CONTINUIDAD DEL NEGOCIO

Publicada en 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

ISO/IEC 27032: CIBERSEGURIDAD

Publicada en 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27033: NETWORK SECURITY

Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada en 2009 y en revisión para 2015), 27033-2, directrices de diseño e implementación de seguridad en redes (publicada en 2012), 27033-3, escenarios de referencia de redes (publicada en 2010), 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (publicada en 2014) ; 27033-5, aseguramiento de comunicaciones mediante VPNs (publicada en 2013); 27033-6, convergencia IP (prevista para 2015); 27033-7, redes inalámbricas (en proceso).

ISO/IEC 27034: SEGURIDAD EN APLICACIONES

Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: 27034-1, conceptos generales (publicada en 2011), 27034-2, marco normativo de la organización (en proceso), 27034-3, proceso de gestión de seguridad en aplicaciones (en proceso), 27034-4, validación de la seguridad en aplicaciones (en proceso), 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (en proceso), 27034-6, guía de seguridad para aplicaciones de uso específico (en proceso).

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27035: GESTION DE INCIDENTES

Publicada en 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. 27035-1, principios de gestión de incidentes, 27035-2, respuesta ante incidentes, 27035-3, operaciones de incidentes.

ISO/IEC 27036: RELACION CON PROVEEDORES

Publicado en 2013. Consiste en una guía en cuatro partes de seguridad en las relaciones con proveedores: 27036-1, visión general y conceptos; 27036-2, requisitos comunes; 27036-3, seguridad en la cadena de suministro TIC; 27036-4, seguridad en entornos de servicios Cloud (en proceso).

ISO/IEC 27037: EVIDENCIAS DIGITALES

Publicada en 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27038: REDACCION DIGITAL

Publicada en 2014. Consiste en una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039: GESTIONI DE IDS / IPS

Publicada en 2015. Consiste en una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040: SEGURIDAD EN STORAGE

Publicada en 2015. Consiste en una guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041: INVESTIGACIONES

En proceso. Consistirá en una guía para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042: INTERPRETACION DE EVIDENCIAS DIGITALES

En proceso. Consiste en una guía con directrices para el análisis e interpretación de las evidencias digitales.

INVENTARIO DE FAMILIA ISO27000

ISO/IEC 27043: INVESTIGACION DE INCIDENTES

Publicada en 2015. Consiste principios y procesos de investigación de incidentes.

ISO/IEC 27044: GESTION DE EVENTOS

En proceso. Gestión de eventos y de la seguridad de la información - Security Information and Event Management (SIEM).

ISO/IEC 27050: EVIDENCIAS ELECTRONICAS

En proceso. Consiste en una guía con directrices para el análisis e interpretación de las evidencias electronicas.

ISO 27799: APLICACIÓN A ORGANIZACIONES DE SECTOR SANITARIO

Publicada en 2008. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

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

Porqué Implementar un ISMS / SISTEMA DE GESTION ISO?

Algunas consideraciones generales de porqué implementarlo:

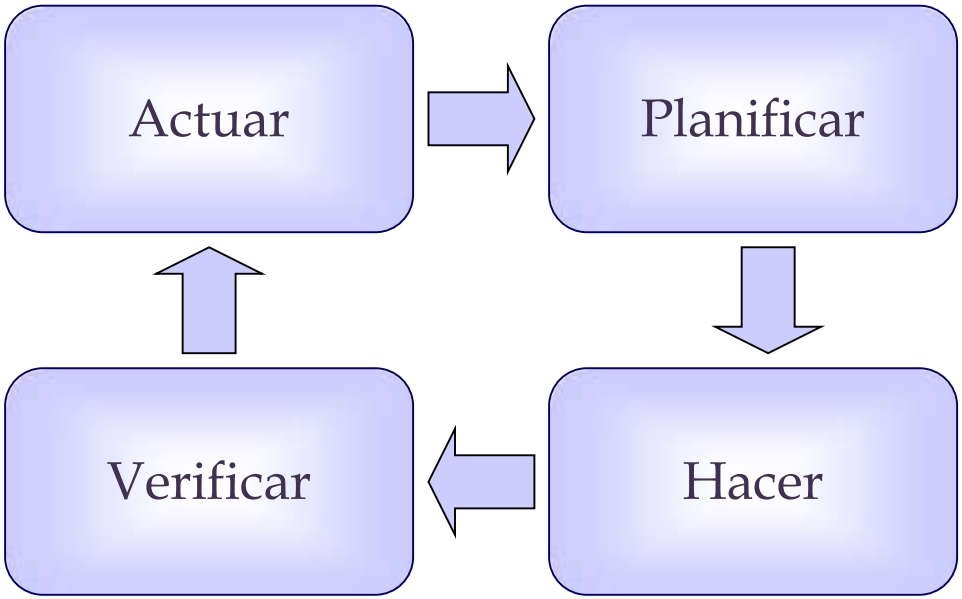
- Para poder tener una Metodológica dedicada a la seguridad de información reconocida internacionalmente

- 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:



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 27002.

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 concientizacion 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

ISO/IEC 27001/2:2013

4 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8. GESTIÓN DE ACTIVOS.
9. CONTROL DE ACCESOS.
10. CIFRADO.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
12. SEGURIDAD EN LA OPERATIVA.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
15. RELACIONES CON SUMINISTRADORES.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
18. CUMPLIMIENTO.

5. POLÍTICAS DE SEGURIDAD.

5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.

6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la seguridad. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.

6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.

7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en seguridad. de la informacion.
7.2.3 Proceso disciplinario.

7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.

8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.

8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.

8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.

9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
9.2.3 Gestión de los derechos de acceso con privilegios especiales.
9.2.4 Gestión de información confidencial de autenticación de usuarios.
9.2.5 Revisión de los derechos de acceso de los usuarios.
9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario.
9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.
9.4.1 Restricción del acceso a la información.
9.4.2 Procedimientos seguros de inicio de sesión.
9.4.3 Gestión de contraseñas de usuario.
9.4.4 Uso de herramientas de administración de sistemas.
9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.

10.1 Controles criptográficos.
10.1.1 Política de uso de los controles criptográficos.
10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.

11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.

11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA. (1de2)

12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.

12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.

12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.

12. SEGURIDAD EN LA OPERATIVA. (2de2)

12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.

12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.

12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
13.1.2 Mecanismos de seguridad asociados a servicios en red.
13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.
13.2.1 Políticas y procedimientos de intercambio de información.
13.2.2 Acuerdos de intercambio.
13.2.3 Mensajería electrónica.
13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.
14.1.1 Análisis y especificación de los requisitos de seguridad.
14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.

14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.

15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

17.2 Redundancias.
17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.

18.1 Cumplimiento de los requisitos legales y contractuales.
18.1.1 Identificación de la legislación aplicable.
18.1.2 Derechos de propiedad intelectual (DPI).
18.1.3 Protección de los registros de la organización.
18.1.4 Protección de datos y privacidad de la información personal.
18.1.5 Regulación de los controles criptográficos.

18.2 Revisiones de la seguridad de la información.
18.2.1 Revisión independiente de la seguridad de la información.
18.2.2 Cumplimiento de las políticas y normas de seguridad.
18.2.3 Comprobación del cumplimiento.

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 Respaldatoria 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.

Cómo es un Proceso de Certificación ISO 27001 de una Organización?

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 27002 O SEGÚN ISO27001?

Las Organizaciones implementan de acuerdo a ISO27002 pero las Empresas Certificadoras utilizan el ISO27001 (antes 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.

COMO ES EL PROCESO DE CERTIFICACION?

Los principales PASOS son:

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

COMO ES EL PROCESO DE CERTIFICACION?

- Identificar conjuntamente:
  - las NO CONFORMIDADES (incumplimientos de acuerdo al Estándar)
  - las NO CONFORMIDADES que son ACEPTADAS (sólo se documentan los argumentos de justificación)
  - las NO CONFORMIDADES que NO son ACEPTADAS (se definen las MEJORAS a implementar)

COMO ES EL PROCESO DE CERTIFICACION?

- Implementar las MEJORAS y Generar los Soportes Documentales correspondientes

- 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)

COMO ES EL PROCESO DE CERTIFICACION?

- Gestionar los respaldos para la Acreditación Internacional de la Certificación lograda

- 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.

SISTEMA DE GESTION
DE SEGURIDAD DE LA INFORMACION

TRACK
INFOSEC MANAGEMENT

Muchas Gracias