MASTER INTERUNIVERSITARIO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES
(MISTIC)

TFM - ADHOC: GESTION Y AUDITORIA DE LA SEGURIDAD INFORMATICA

TRABAJO FINAL DE MÁSTER

ESTUDIANTE: MARIBEL AVILA ARZUZA

CONSULTOR: FÉLIX ANTONIO BARRIO JUÁREZ

EMPRESA: INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACION (INTECO)

MAYO 2012

Resumen

Este proyecto se enmarca en el desarrollo del TFM-Trabajo Final de Maestría del Master Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones y que tiene como objetivo el análisis para la implantación de un Sistema de Gestión de Seguridad de la Información, conocido como SGSI, en un entorno real empresarial, en este caso se trabajó bajo la organización del Instituto Nacional de Tecnologías de la Comunicación - INTECO, empresa española que trabaja para fomentar e impulsar la seguridad de la información y su implantación en las empresas y organizaciones.

El SGSI es una parte del sistema global de gestión que, basado en un análisis de los riesgos del negocio, permite asegurar la información frente a la pérdida de: Confidencialidad, Integridad y Disponibilidad, de allí la importancia de implantar un sistema de este tipo.

Para el desarrollo de este trabajo se han seguido los lineamientos establecidos en la norma internacional UNE/ISO 27001, que establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI. Esta norma establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, a partir de la repetición cíclica de cuatro fases: Planificar, Hacer, Verificar y Actuar.

Dentro de las especificaciones de la norma se establece un esquema documental del SGSI, que debe mantenerse actualizado, disponible y enmarcado en un índice, especialmente si la empresa desea superar un proceso de certificación. Sobre este apartado se hizo especial énfasis en el presente proyecto.

Summary

This project is part of the development of TFM-Final Work Master of “Interuniversity Master of Security in Information Technology and Communications” and wich aims to implement the analysis a Safety Management System of Information, known as ISMS, in a real business, in this case, we worked under the umbrella of the National Institute of Communication Technologies - INTECO, a Spanish company that works to encourage and promote information security and its implementation in companies and organizations.

The ISMS is a part of the overall management system that, based on an analysis of business risks, enables secure information against loss of Confidentiality, Integrity and Availability, hence the importance of implementing a system of this type.

To develop this work we have followed the guidelines established by international standard IEC/ISO 27001, which establishes the specifications for the creation, implementation, operation, monitoring, reviewing, maintaining and improving an ISMS. This norm establishes a process approach based on the Deming cycle, which raises the safety management as a process of continuous improvement, from the cyclical repetition of four phases: Plan, Do, Check and Act.

Within the standard specification provides an document outline of the ISMS, which must be updated, available and framed in an index, especially if the company wants to pass a certification process. About this section special emphasis in this project.

Índice

Introducción

Actualmente las empresas de cualquier tipo o sector de actividad manejan sistemas de información en general, y factores como: las exigencias propias de cada negocio, el alto valor de los activos de información que manejan, la confianza frente a los clientes, entre otros, han generado la necesidad de contar con seguridad en dichos sistemas, de tal manera que se preserve la calidad en los servicios y se propenda por la eficacia y eficiencia de los procesos del negocio y el valor de sus activos. Las medidas de seguridad no sólo incluyen tecnología, también se deben tener en cuenta los aspectos organizativos y los relativos al personal, siendo estos últimos uno de los más importantes. La seguridad de la información debe tratarse como un proceso más de la organización, imprescindible para poder alcanzar los objetivos del negocio. No es suficiente establecer controles en forma aislada, ni actuar de modo reactivo y defensivo, se requiere de un Sistema de Gestión de Seguridad de la Información (SGSI) y un accionar proactivo.

Este sistema es una parte del sistema global de gestión que, basado en un análisis de los riesgos del negocio, permite asegurar la información frente a la pérdida de:

- Confidencialidad: sólo accederá a la información quien esté autorizado.
- Integridad: la información será exacta y completa.
- Disponibilidad: los usuarios autorizados tendrán acceso a la información cuando lo requieran.

Aunque la seguridad total es inalcanzable, mediante el proceso de mejora continua del SGSI se puede lograr un nivel de seguridad altamente satisfactorio, que reduzca al mínimo los riesgos a los que se está expuesto y el impacto que ocasionarían si efectivamente se produjeran.

El presente trabajo pretende desarrollar, tomando como referencia lo establecido en la Norma ISO/IEC 27001, un análisis para la implantación de un SGSI completo para la organización INTECO (Instituto Nacional de Tecnologías de la Comunicación), empresa española que trabaja para fomentar e impulsar la seguridad de la información y su implantación en las empresas y organizaciones. Esta norma internacional es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. Especifica también los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI.

1. Marco teórico y normativo

Según la Norma UNE-ISO/IEC 27001 un Sistema de Gestión de Seguridad de la Información (SGSI), es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Lo cual indica que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización. Permitirá conocer mejor la organización, cómo funciona y qué se puede hacer para que la situación mejore.

Esta norma internacional sigue el modelo PDCA o "Planificar–Hacer–Verificar–Actuar" (Plan–Do–Check–Act por sus siglas en inglés), que se aplica para estructurar todos los procesos del SGSI, como se muestra en la Figura 1.

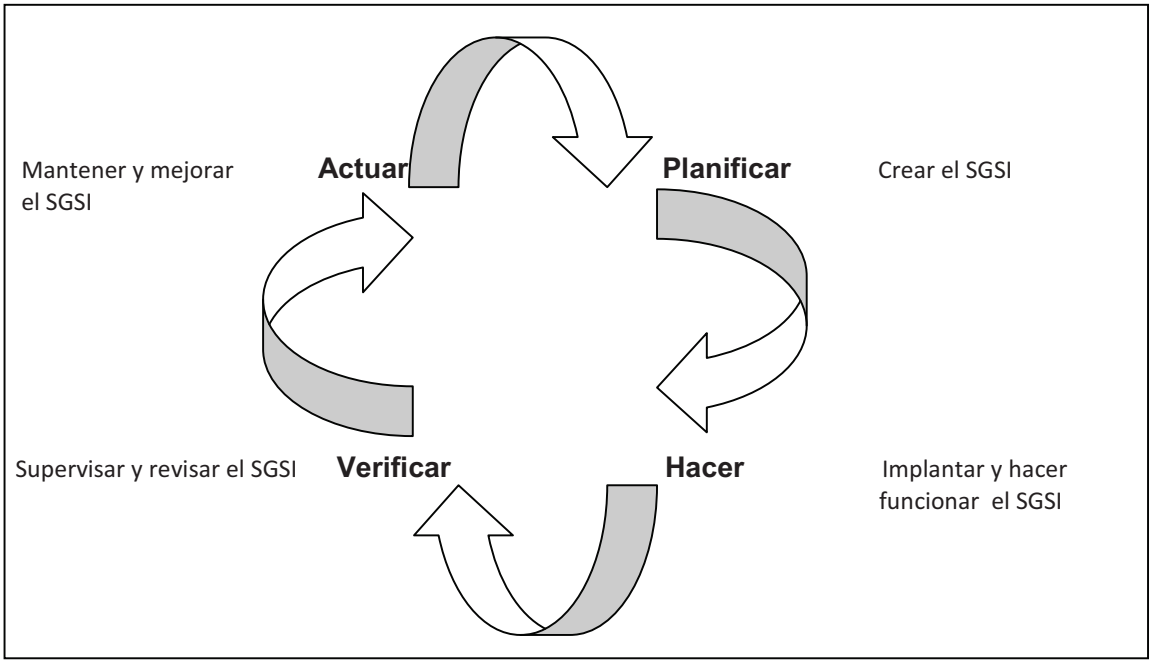

Figura 1. MODELO PDCA APLICADO A LOS PROCESOS DEL SGSI

De acuerdo a como lo establece la norma ISO/IEC 27001 y al modelo PDCA, se siguen los pasos descritos en la Figura 1. para el proceso de implementación del SGSI, así:

1. Definición del alcance

2. Análisis y gestión del riesgo

3. Generación y gestión de los diferentes proyectos de seguridad para implantar las medidas ISO 27002

4. Implantar las medidas y controles

5. Creación del marco de gestión ISO 27001

  5.1. Gestión de la documentación

  5.2. Gestión de la formación y concienciación

  5.3. Gestión de la auditoria interna

  5.4. Gestión de la revisión del sistema

  5.5. Gestión de la mejora continua: acciones preventivas y correctivas

6 Elaboración de la documentación formal necesaria para construir el SGSI

  6.1. Normas de seguridad

  6.2. Procedimientos de seguridad

7. Acciones formativas y de concienciación

Este modelo de mejora continua permite establecer un proceso para ir alcanzando los objetivos en diferentes iteraciones, de forma que el sistema de gestión se va ampliando gradualmente, y permite tener en marcha un proceso de revisión para asegurar que los problemas se detectan y corrigen, que se incorporan las lecciones aprendidas en cada nueva iteración y que se implantan mejoras justificadas, permitiendo evolucionar paso a paso.

2. Análisis de la empresa

A continuación se hace un breve análisis de la empresa para situarnos dentro del proceso de implantación.

2.1. Descripción de la empresa

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) es una empresa española, que trabaja para fomentar e impulsar la seguridad de la información y su implantación en las empresas y organizaciones. Su página web es: http://www.inteco.es. Su organización es la que se observa en la Figura 2:

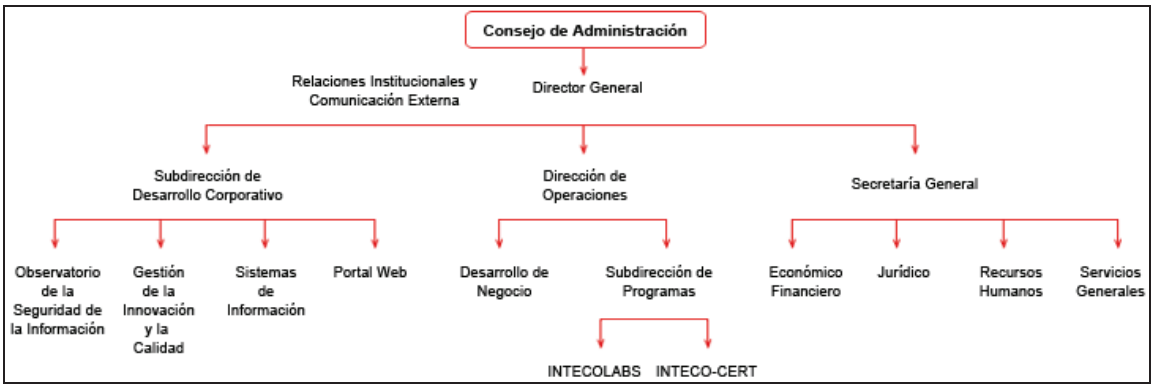

Figura 2. ORGANIZACIÓN DE INTECO

La misión de INTECO es aportar valor e innovación a los ciudadanos, a las Pyme, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en España, promoviendo además una línea de participación internacional.

La visión de INTECO es conseguir sus objetivos mediante:

- El compromiso de profesionales altamente cualificados, comprometidos con sus proyectos y capaces de generar valor e innovación continuamente.

- La dinamización del sector TIC, generando nuevos negocios y oportunidades para clientes, proveedores y profesionales.

- La igualdad de oportunidades para todo el tejido empresarial español, especialmente la PYME, actuando como suministro de último recurso en materia de innovación TIC allá donde sea necesario.

- El soporte a los ciudadanos, que son la clave para que el desarrollo de las nuevas tecnologías tenga un impacto social positivo.

Los valores que promueve INTECO son los siguientes:

- Transparencia con la sociedad, los clientes, y los agentes del sector TIC.

- Búsqueda de la excelencia, tanto en el comportamiento de los profesionales como en la ejecución de los proyectos.

- Compromiso con el servicio público, pues es la razón de ser de una sociedad anónima participada por el Estado.

- Mantenimiento del espíritu innovador en todos los proyectos que se aborden, maximizando el valor ofrecido a los clientes.

Coordina distintas iniciativas públicas en torno a la seguridad de las TIC, que se materializan en la prestación de servicios por parte del Observatorio de la Seguridad de la Información, el Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información (INTECO-CERT) cuya finalidad es servir de apoyo preventivo y reactivo en materia de seguridad en tecnologías de la información y la comunicación tanto a entidades como a ciudadanos, con su Catálogo de Empresas y Soluciones de Seguridad TIC, y la Oficina de Seguridad del Internauta (OSI). La Gerencia de Innovación y Calidad tiene entre sus competencias el soporte a la gestión del SGSI (Sistema de Gestión de Seguridad de la Información.

2.2. Requerimientos de seguridad de la empresa y de la seguridad de la información

Dentro de los puntos estratégicos con los que está comprometida la empresa, se tienen: seguridad, accesibilidad, calidad TIC y formación; sus objetivos se resumen así:

- Seguridad: la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados; al tiempo que garanticen un cumplimiento estricto de la normativa legal en materia de TIC.

- Accesibilidad: la promoción de servicios de la Sociedad de la Información más accesibles, que supriman las barreras de exclusión, cualquiera que sea la dificultad o carencia técnica, formativa, etc., incluso discapacidad, que tengan sus usuarios, y que faciliten la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información.

- Calidad TIC: la promoción de servicios de la Sociedad de la Información que cada vez sean de mayor calidad, que garanticen unos adecuados niveles de servicio, lo cual se traduce en una mayor robustez de aplicaciones y sistemas, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios.

- Formación: la formación de universitarios y profesionales en las tecnologías más demandadas por la industria.

Los grupos de interés de la empresa son: Personas, Proveedores, Clientes, Sociedad, Profesionales, PYMES, Alianzas y AA.PP (Administración Pública).

Los valores corporativos de INTECO son: Compromiso, Excelencia, Transparencia e Innovación.

2.3. Definición del alcance y límites del SGSI

2.3.1 Declaración

El Sistema de Gestión de Seguridad de la Información para INTECO comprende las áreas de la Subdirección de Desarrollo Corporativo, por ser una de las que mas está relacionada directamente con la misión y visión de la empresa. Esta subdirección está formada por las siguientes áreas: Observatorio de la Seguridad de la Información, Gestión de la Innovación y la Calidad, Sistemas de Información y Portal WEB.

El SGSI también comprenderá servicios de apoyo, los cuales incluyen la gestión de las áreas de Recursos Humanos, Jurídica, Económico Financiera y la que realiza funciones de Sistemas, aunque no está especificada claramente en el organigrama de la empresa.

Igualmente comprende los servicios, procesos y activos correspondientes a las áreas mencionadas y que son necesarios para garantizar la disponibilidad de los servicios que la empresa presta, tanto a nivel interno como externo; sin desmejora de cualquier otro componente de la seguridad como lo son la confidencialidad y la integridad de la información y de los valores corporativos de INTECO: Compromiso, Excelencia, Transparencia e Innovación.

2.3.2 Objetivos

- Garantizar la seguridad de los servicios de la Sociedad de la Información, protegiendo los datos personales de los interesados, su intimidad, la integridad de su información y evitando ataques que pongan en riesgo los servicios prestados; al tiempo que se cumpla estrictamente con la normativa legal en materia de TIC.

- Garantizar la accesibilidad de los servicios de la Sociedad de la Información, suprimiendo las barreras de exclusión que tengan sus usuarios, y facilitando la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información.

- Garantizar la calidad de los servicios de la Sociedad de la Información, ofreciendo unos adecuados niveles de servicio, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios.

2.4. Definición de la Política del SGSI

2.4.1. Declaración

Los servicios que INTECO presta a través de la Subdirección de Desarrollo Corporativo y las áreas de Recursos Humanos, Jurídica, Económico Financiera y Sistemas; la información que permite prestar dichos servicios; las aplicaciones y equipos que los proveen y mantienen; las instalaciones físicas donde residen los Sistemas de Información y el personal vinculado directamente con la prestación de dichos servicios, deben permanecer prácticamente disponibles, sin menoscabo de la

integridad y de la confidencialidad necesaria para que los servicios se mantengan funcionando. Así mismo, como objetivo de acción se velará porque los usuarios de INTECO reciban un servicio seguro, accesible y de calidad.

2.4.2. Objetivos

- Asegurar que los usuarios de INTECO tengan acceso a los servicios que se prestan, incluyendo los procesos, los sistemas y los equipos de cómputo.

- Asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información necesaria para prestar los servicios.

- Garantizar que la información que INTECO maneja o que está contenida en los equipos de terceros, como resultado del servicio que presta, solo sea accedida por su propietario o por personal autorizado.

3. Estructura del Sistema Documental

Los siguientes documentos hacen parte del Sistema de Gestión de Seguridad de la Información de INTECO.

3.1. Alcance, Política y Objetivos del SGSI

3.1. Alcance, Política y Objetivos del SGSI

Versión	Redactado / revisado por	Aprobado por	Fecha aprobación	Fecha publicación
1.0	Comité de Seguridad de la Información	Director General	Enero 2012	Febrero 2012

Referencia en ISO 27001 : 4.2.1 a-b)1,2,3-5 y 5.1.1

El Instituto Nacional de Tecnologías de la Comunicación (INTECO) es una entidad española, cuya misión es aportar valor e innovación a los ciudadanos, a las Pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en el país, promoviendo además una línea de participación internacional.

Con el fin que dichos servicios se presten eficazmente, la Dirección de INTECO está comprometida con el desarrollo de un Sistema de Gestión de la Seguridad de la Información (SGSI), el cual bajo lo establecido en la Norma internacional UNE/ISO-IEC 27001, establece un conjunto de medidas técnicas y organizativas para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Este sistema de gestión cubre toda la información, sistemas de información, activos y personas para los procesos en los siguientes servicios:

- Servicios de la Subdirección de Desarrollo Corporativo, que comprende el Observatorio de la Seguridad de la Información, Gestión de la Innovación y la Calidad, Sistemas de Información y Portal WEB.

- Servicios de apoyo de las áreas de Recursos Humanos, Jurídica, Económico Financiera y Sistemas.

La prestación de estos servicios se realiza en la siguiente ubicación física: Avenida de José Aguado N° 41, 24005, León, donde queda la sede de Inteco; esta ubicación queda incluida en el alcance del SGSI.

La Dirección de INTECO a través del Comité de Seguridad de la Información que preside el Director General, ha decidido impulsar y difundir a todos los niveles de la empresa la siguiente Política:

“Cada Responsable de la información en INTECO, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad, manteniendo una adecuada protección de los activos, impidiendo accesos no autorizados a la información”.

Esta Política se fundamenta en los siguientes principios:

- Proteger los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, para asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

- Incorporar medidas de seguridad en los sistemas de información desde su desarrollo e implementación y durante su mantenimiento, con el fin de reducir los riesgos de error humano y sucesos de origen natural.

- Garantizar la seguridad continua de la información:

  - Mantener la Política de Seguridad de INTECO actualizada, con el fin de asegurar su vigencia y nivel de eficacia.
  - Sensibilizar al personal de INTECO con relación a su responsabilidad frente a la utilización de contraseñas.
  - Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
  - El Comité de Seguridad de la Información revisará anualmente la Política, con el fin de mantenerla actualizada. Igualmente efectuará las modificaciones que sean necesarias en razón a posibles cambios que puedan afectar su definición, como cambios tecnológicos, impacto de los incidentes de seguridad, etc.

- Garantizar la seguridad de los servicios de la Sociedad de la Información, protegiendo los datos personales de los interesados, su intimidad, la integridad de su información y evitando ataques que pongan en riesgo los servicios prestados; al tiempo que se cumpla estrictamente con la normativa legal en materia de TIC.

- Garantizar la accesibilidad de los servicios de la Sociedad de la Información, suprimiendo las barreras de exclusión que tengan sus usuarios, y facilitando la integración progresiva de todos los colectivos de usuarios, de modo que todos ellos puedan beneficiarse de las oportunidades que ofrece la Sociedad de la Información.

- Garantizar la calidad de los servicios de la Sociedad de la Información, ofreciendo unos adecuados niveles de servicio, un compromiso en la disponibilidad y los tiempos de respuesta, un adecuado soporte para los usuarios, una información precisa y clara sobre la evolución de las funcionalidades de los servicios.

3.2. Procedimientos y mecanismos de control

Se establecen los siguientes procedimientos y mecanismos de control ya sean automáticos (preferiblemente) o manuales:

- Controlar las versiones de documentos, que garanticen que se mantiene un registro actualizado de las versiones de todos los documentos que se han aprobado y que se identifican los cambios y el estado de la versión vigente de los mismos.

- Controlar las fechas de documentos, que garanticen que documentos no puedan ser publicados con fechas pasadas, o que sean seleccionadas fechas pasadas para revisar documentos.

- Controlar las publicaciones de documentos, que garanticen que no se publiquen nuevas versiones de documentos que aún no hayan sido aprobadas.

- Desarrollar un procedimiento para definir y/o modificar procedimientos dentro de los procesos de INTECO establecidos en el alcance del SGSI, junto con los documentos soporte de los mismos.

- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.

- Controlar que las versiones vigentes de los documentos aplicables se encuentran siempre disponibles y que permanecen legibles y fácilmente identificables.

- Prevenir el uso no intencionado de documentos obsoletos.

- Establecer los controles necesarios para la identificación, almacenamiento, protección, recuperación, retención y disposición de los registros.

3.3. Descripción de la metodología de evaluación de riesgos seleccionada

La metodología seleccionada para la evaluación de riesgos es MAGERIT, esta metodología fue elaborada por el Ministerio de Administraciones Públicas con el fin de ayudar a todas las administraciones públicas del Estado español a mejorar diversos aspectos y puede ser aplicada a cualquier organización.

Las fases para su implementación son las siguientes:

1. Toma de datos y procesos de información: va de la mano con el alcance definido para el SGSI, y se deben tener en cuenta los procesos que lleva a cabo la organización y analizar los riesgos que puedan interferir en los procesos críticos; también se debe precisar a qué nivel de detalle se debe llegar.

2. Establecimiento de parámetros: se deben identificar los parámetros que se utilizarán durante todo el proceso de análisis de riesgos, los cuales son:

    - Valor de los activos: se asigna una valoración económica a todos los activos de la empresa que se pretenden analizar. En esta valoración se debe tener en cuenta: valor de reposición, valor de configuración, valor de uso del activo, valor de pérdida de oportunidad. Se utiliza una escala de valores: muy alta, alta, media, baja, muy baja; y a cada rango se le asigna un valor económico.

    - Vulnerabilidad: es la frecuencia con la que una organización puede sufrir alguna amenaza en concreto. Se recomienda también la utilización de una escala de valores, que puede ser por ejemplo: frecuencia extrema (una vez al día), alta (una vez cada dos semanas), media (una vez cada dos meses), baja (una vez cada seis meses), muy baja (una vez al año); esta valoración se convierte a número que significa la estimación anual de ocurrencia.

    - Impacto: el porcentaje del valor del activo que se pierde en el caso que sucede un incidente sobre él; en este parámetro también se realiza una estimación por rango de impactos, por ejemplo: muy alto (100%), alto (75%), medio (50%), bajo (20%) y muy bajo (5%).

    - Efectividad del control de seguridad: la influencia que tendrán las medidas de protección ante los riesgos que se van a detectar; es decir, cómo las medidas de seguridad que se implanten, reducirán el riesgo detectado. Se utiliza también una clasificación de niveles: muy alto (95%), alto (75%), medio (50%), bajo (30%), muy bajo (10%).

Se debe tener presente que los parámetros deben ser utilizados tal y como se definan en un principio, durante todo el análisis de riesgos, si se hace una modificación en mitad del proceso, los resultados no serán adecuados.

3. Análisis de activos: identificar cuáles son los activos que posee la empresa y que necesita para llevar a cabo sus actividades; debe ir acorde con el alcance definido. Los activos se pueden clasificar en: físicos, lógicos, de personal, de entorno e infraestructura, intangibles. Se efectuará su valoración de acuerdo a los parámetros descritos anteriormente.

4. Análisis de amenazas: amenazas son aquellas situaciones que podrían llegar a darse en una organización y que resultarían en un problema de seguridad. Se clasifican en:

    - Accidentes: situaciones no provocadas voluntariamente y que generalmente no pueden evitarse. Pueden ser de los siguientes tipos: accidente físico, avería, interrupción de servicios esenciales, accidentes mecánicos o electromagnéticos.

    - Errores: situaciones cometidas de forma involuntaria, por el desarrollo de las actividades propias de la empresa, ya sea por desconocimiento o descuido del personal o terceros. Dentro de estos se pueden encontrar: errores en la utilización de los sistemas, en el desarrollo de aplicaciones, de actualización en los sistemas o aplicaciones, en la monitorización, de compatibilidad entre aplicaciones, inesperados (virus, troyanos, etc.).

    - Amenazas intencionales presenciales: provocadas por el personal de la empresa de forma voluntaria, al realizar acciones que saben que provocan un daño ya sea físico o lógico. Se pueden encontrar las siguientes: acceso físico no autorizado, acceso lógico no autorizado, indisponibilidad de recursos, filtración de datos a terceros.

    - Amenazas intencionales remotas: provocadas por personas ajenas a la empresa y que consiguen dañarla. Se pueden encontrar, entre otras, las siguientes: acceso lógico no autorizado, suplantación del origen en una comunicación, gusanos, denegación de servicio.

5. Establecimiento de vulnerabilidades: vulnerabilidades son aquellos agujeros que se tienen en la seguridad de una empresa y que permiten que una amenaza pueda dañar un activo. Se debe tener claro que, sin vulnerabilidad, la amenaza no puede dañar un activo y que las vulnerabilidades por sí mismas no provocan daños, sino que estos son siempre provocados por las amenazas.

6. Establecimiento de impactos: los impactos son las consecuencias que provoca en la empresa el hecho de que cierta amenaza, aprovechando una vulnerabilidad, afecte un activo. Al analizar los impactos, se deben tener en cuenta los siguientes aspectos: el resultado de la agresión de una amenaza sobre un activo, el efecto sobre cada activo, el valor económico de las pérdidas producidas en cada activo, las pérdidas cuantitativas o cualitativas.

7. Análisis de riesgo intrínseco: el riesgo intrínseco en la metodología utilizada, se toma como el riesgo en la situación actual de la empresa que se analiza. De acuerdo a esto, con los valores analizados en los puntos descritos anteriormente, sólo es necesario multiplicar los valores así: *Riesgo = Valor del activo × Vulnerabilidad × Impacto*

8. Influencia de salvaguardas: las salvaguardas son los controles de seguridad, para este análisis se clasifican en dos tipos: preventivas (reducen las vulnerabilidades) y correctivas (reducen el impacto de las amenazas). En esta fase se trata de encontrar las soluciones de seguridad que existan en el mercado de ambos tipos.

9. Análisis de riesgos efectivo: se estudia cómo se reducen los riesgos con cada una de las salvaguardas identificadas en la fase anterior, es decir, se calcula el riesgo efectivo que tendría la empresa para cada una de las amenazas identificadas. Este cálculo se realiza de la siguiente manera:

Riesgo efectivo = Riesgo intrínseco × Porcentaje de disminución de vulnerabilidad × Porcentaje de disminución de impacto

10. Evaluación de riesgos: consiste en la toma de decisiones por parte de la empresa sobre las medidas de seguridad que debe escoger entre el listado de salvaguardas que permiten reducir los riesgos en aquella. Las organizaciones deben pretender disminuir todos los riesgos que han detectado hasta situarlos por debajo del denominado "umbral de riesgos" y que represente un menor costo.

Como resultado del proceso de análisis y evaluación de riesgos, se tiene lo siguiente:

- Cuáles son los activos y recursos más importantes para la gestión de la empresa y por lo tanto requieren de una atención especial desde el punto de vista de la protección, especificando aquellos considerados de importancia crítica por el peso que tienen dentro del sistema.

- Qué amenazas actúan sobre los activos y recursos a proteger y entre ellas cuales tienen una mayor probabilidad de materializarse (riesgo) y su posible impacto sobre la entidad.

- Cuáles son los activos, recursos y áreas con un mayor peso de riesgo y qué amenazas lo motivan.

- Cuáles son las salvaguardas que permiten mitigar los riesgos en la empresa.

3.4. Informe de evaluación/apreciación de riesgos

De acuerdo a la última fase descrita en el anterior punto, una vez identificados los riesgos que hay que mitigar (riesgos no asumibles) y los objetivos de seguridad que se desea alcanzar, se deberán seleccionar los controles o salvaguardas necesarias. Estas salvaguardas pueden ser controles técnicos, procedimientos operativos, normativas de usuario, cláusulas contractuales, etc. La selección de estos controles se sugiere hacerla a partir de la norma ISO 27002.

3.5. Plan de tratamiento de riesgos

A partir del resultado del análisis de riesgos se debe elaborar un plan de acción, que indique qué decisión se tomará con cada riesgo identificado, la cual puede ser una de las siguientes: reducir, transferir o aceptar el riesgo; dicho plan contendrá lo siguiente:

- Establecimiento de prioridades: se designan aquellos riesgos que tendrán que ser reducidos en primer lugar debido a que son los más elevados para la organización.

- Planteamiento del análisis de coste/beneficio: se estudian, para cada una de las medidas que se pueden implantar, qué coste le supondría a la organización y en qué porcentaje reduciría los riesgos detectados.

- Selección de controles definitivos: después de analizar el coste/beneficio de todos los controles, hay que seleccionar definitivamente los que tendrá que implantar la empresa para reducir los riesgos hasta situarlos por debajo de su umbral de riesgo.

- Asignación de responsabilidades: se asignan los responsables dentro de la empresa de llevar a cabo la implantación de los controles.

- Implantación de controles: se realiza la implantación de los controles de seguridad designados. Los controles que se implanten no son obligatoriamente técnicos, sino que podrían ser controles organizativos o procedimentales.

3.6. Procedimientos documentados de la organización

A continuación se presentan los siguientes procedimientos documentados de la empresa: Procedimiento Regulación de acceso al Sistema Informático y Procedimiento Copias de seguridad

INDICE

Versión	Redactado / revisado por	Aprobado por	Fecha aprobación	Fecha publicación
1.0	Comité de Seguridad de la Información	Director General	Febrero 2012	Marzo 2012

Referencia en ISO 27001: A.11.1., A.11.2., A.11.3., A.11.5., A.11.6.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Redactar el procedimiento para regular el acceso al Sistema Informático de la empresa INTECO.

Para garantizar la protección del Sistema Informático, es necesario definir un procedimiento que establezca las medidas de seguridad, organizativas y técnicas que protejan la información de la empresa y los sistemas que la tratan.

2. Alcance

Este procedimiento va dirigido a todos los usuarios del Sistema Informático, que incluyen tanto los usuarios internos (personal de plantilla) como los usuarios externos (subcontratados).

Entrará en vigencia el día 1º. de marzo del 2012 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Cumplimiento con los requisitos legales y estándares de seguridad

El presente procedimiento proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A:

A.11.1 Requisitos de negocio para el control de acceso
A.11.2 Gestión de acceso de usuario
A.11.3 Responsabilidades de usuario
A.11.5 Control de acceso al sistema operativo
A.11.6 Control de acceso a las aplicaciones y a la información

4. Descripción

4.1 Identificación y autenticación para usuarios del Sistema Informático

Para acceder al Sistema Informático de la empresa, es necesario contar con un usuario, el cual identificará a la persona en el mismo y su estructura debe ser la siguiente: Inicial_nombre_usuario.apellido1_nombre_usuario.apellido2_nombre_usuario. El usuario será autenticado por una contraseña, a partir de esta autenticación, se le asignarán funciones que determinan las actividades que podrá desarrollar dentro del Sistema Informático.

Para que el usuario sea asignado, previamente se debe firmar lo siguiente:

En caso de personal de plantilla, el “Acuerdo de Confidencialidad y Buen Uso de los Sistemas Informáticos”, Anexo 1 de este procedimiento.

En caso de personal subcontratado, además del “Acuerdo de Confidencialidad y Buen Uso de los Sistemas Informáticos”, el representante de la firma contratista debe firmar también el “Convenio de Confidencialidad y No Divulgación”, Anexo 2 de este procedimiento.

Los documentos anteriormente mencionados definen entre otros, el buen uso, disponibilidad y nivel de servicio, así como la responsabilidad y confidencialidad exigida para el mismo.

El Sistema Informático dispone de mecanismos para identificar a los usuarios que acceden al mismo, así como para controlar si están autorizados a acceder a los recursos y el modo (lectura,

modificación, etc.) en que pueden realizar el acceso. Se llevará un registro de asignación y revocación de usuarios, así como de los privilegios concedidos y las fechas correspondientes.

4.2 Contraseñas

Para la gestión y manejo de contraseñas, se debe cumplir lo establecido en la Norma de Contraseñas.

4.3 Puesto de trabajo

Cuando se finaliza la realización de las tareas, se sugiere salir del Sistema Informático desconectándose, de tal manera que nadie pueda trabajar con el usuario/contraseña de otra persona. Es conveniente mantener el protector de pantalla con contraseña y con lapso de activación no superior a cinco (5) minutos. Ante la ausencia temporal, se debe activar el protector de pantalla y no dejar expuestos discos o soportes USB. La sesión de usuario se bloquea automáticamente por inactividad después de 15 minutos. No se debe anotar la contraseña en ningún papel que quede en el puesto de trabajo del usuario.

4.4 Control de acceso a servidores corporativos

El Responsable de Seguridad dará acceso (lectura, escritura, modificación, etc.) a los servidores corporativos de acuerdo a las autorizaciones definidas por los roles asignados a cada usuario. Se llevará registro de auditoria de intentos fallidos de acceso a los servidores. La información de los servidores hace parte del “Acuerdo de Confidencialidad y buen uso de los Sistemas Informáticos”, suscrito por los usuarios.

5. Control

La Empresa realizará auditorias internas periódicas para garantizar el cumplimiento de los controles establecidos en este procedimiento.

6. Penalizaciones

Cuando el Administrador del Sistema Informático detecte incumplimiento en este procedimiento, puede tomar cualquiera de las siguientes medidas:

- Notificar la incidencia al Responsable de Seguridad.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación, de ser necesario.
- Con el permiso del Responsable de Seguridad y la correspondiente justificación, examinar ficheros o dispositivos de almacenamiento del usuario implicado.
- Informar a la Dirección de lo sucedido.

7. Divulgación

Publicado el 30 de marzo de 2012.

8. Revisión

Este documento se revisará anualmente.

ANEXO 1 - ACUERDO DE CONFIDENCIALIDAD Y BUEN USO DE LOS SISTEMAS INFORMATICOS

1. Sólo las personas debidamente designadas podrán ejecutar aquellas operaciones o consultas sobre el Sistema Informático, para las que hayan sido expresamente autorizadas.
2. Acerca del Software: El Software suministrado debe ser utilizado para la realización de las tareas relacionadas con la empresa, y no para uso personal. No debe instalarse ningún software en los equipos de cómputo.
3. No está permitida ninguna conexión de red en el equipo de cómputo que no sea la suministrada por la empresa.
4. Acerca de la Contraseña: Para la gestión y manejo de contraseñas, se debe cumplir lo establecido en la Norma de Contraseñas, la cual hace parte de este Acuerdo.
5. Acerca de la información: La información contenida o publicada en el Sistema Informático es propiedad de la empresa y no deberá ser transferida o divulgada en forma no autorizada.

Con respecto a las obligaciones mencionadas, cualquier incumplimiento será constituido como grave y será objeto de las sanciones consideradas en el contrato respectivo.

Recomendaciones del Uso

a. Ante el olvido de la contraseña, se podrá solicitar una nueva al personal del área de Soporte al Cliente.
b. Cuando se finaliza la realización de las tareas, se debe salir del Sistema Informático desconectándose, para que nadie pueda trabajar con el usuario/contraseña de otra persona.
c. Es conveniente mantener el protector de pantalla con contraseña y con lapso de activación no superior a 5 minutos.
d. Ante la ausencia temporal, se debe bloquear la sesión con contraseña.

_____

Nombre Usuario:
Documento de ID:

Tipo de Usuario: Interno ○
Externo ○

ANEXO 2 - CONVENIO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

En carácter de Representante Legal de la empresa .... y bajo el contrato Número ..... me comprometo a:

- Acceder al Sistema Informático a través de las licencias de uso instaladas por la empresa _____, aceptando el "Convenio de Confidencialidad y de No Divulgación" en los términos que amparan los derechos propietarios.
- Reconocer que la propiedad intelectual de la Información y del software, pertenece a la empresa _____.
- No copiar, traducir, desensamblar, o descompilar el Software instalado en los equipos utilizados a partir del código objeto del mismo, o usar dicho Software para crear obras derivadas.
- No remover de la Información, ningún aviso referente a derechos de autor, marcas o secretos industriales.

Con respecto al personal de mi empresa me comprometo a:

- Capacitar a los mismos en el conocimiento y uso de los Sistemas Informáticos y de la información contenida en estos.
- Hacer firmar y respetar al personal de mi dependencia el "Acuerdo de Confidencialidad y Buen Uso de los Sistemas Informáticos".

Ante el incumplimiento de todo lo mencionado en este convenio, la empresa CONTRATISTA será objeto de la aplicación de las sanciones consideradas en el contrato respectivo.

_____ Representante Legal

_____ Fecha

INDICE

Versión	Redactado / revisado por	Aprobado por	Fecha aprobación	Fecha publicación
1.0	Comité de Seguridad de la Información	Director General	Marzo 2012	Abril 2012

Referencia en ISO 27001: A.10.5.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Garantizar la seguridad de la información contenida en las bases de datos de los Sistemas de Información y en los servidores de la empresa INTECO. El procedimiento establecido para la realización de copias de seguridad y para la recuperación de los datos, deberá garantizar su reconstrucción en el estado en el que se encontraban al tiempo de producirse cualquier tipo de pérdida o destrucción.

2. Alcance

Este procedimiento aplica a todos los servidores de la empresa donde residen las bases de datos y reposa la información corporativa.

Entrará en vigencia el día 1º. de abril del 2012 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Responsables

Este procedimiento aplica a los administradores de Red y de los servidores correspondientes y a los operadores del Centro de Cómputo, por parte de la empresa y a los empleados de la firma de valores que se encarga de la custodia de la información.

4. Cumplimiento con los requisitos legales y estándares de seguridad

El presente procedimiento proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A: A.10.5. Copias de seguridad

5. Descripción

5.1 Métodos de copias

Se definen los siguientes métodos de copias de seguridad a utilizar:

Copia de seguridad normal: toma copia a todos los archivos seleccionados y pone a cada archivo una marca que indica que se ha hecho una copia de seguridad del mismo.

Copia de seguridad incremental: toma copia a todos los archivos creados o modificados desde la última copia de seguridad normal o incremental y pone una marca a los archivos copiados.

5.2 Métodos de rotación de cintas

Se utilizarán 7 juegos de cintas, armados de tal manera que se tendrán 3 copias completas disponibles en cualquier momento: abuelo, padre e hijo. Lo anterior significa que se podrá recuperar información con una antigüedad de 3 semanas.

El juego 1 será usado para realizar una copia completa el primer viernes, el juego 2 una copia completa el segundo viernes y el juego 3 está reservado para el tercer viernes. Los otros 4 juegos (4, 5, 6, 7) son usados para realizar copias normales (incrementales) de lunes a jueves y serán reutilizados cada semana.

Como cada copia se hace por duplicado, se tendrán que disponer de 14 juegos de cintas.

5.3 Rotulado de las cintas

Una vez realizada una copia, se deberá rotular la cinta llenando los siguientes datos en el formato que se indica a continuación:

Identificación: _____

Fecha de la copia: _____

Hora inicio: _____ Hora final: _____

Fecha de vencimiento: _____

Tipo de copia: _____ O/D: _____

Operador: _____

Así mismo se debe diligenciar la Planilla de copias de seguridad (ver Anexo 1).

5.4 Almacenamiento de las copias de seguridad

Cada uno de los 7 juegos de cintas debe ser guardado en el área de Sistemas pero fuera del Centro de Cómputo o lugar donde estén ubicados los servidores, estas cintas deben ser almacenadas en armarios ignífugos que tengan acceso restringido. Los duplicados deberán ser guardados en un lugar externo a la empresa, para lo cual se establecerá un contrato con una empresa de seguridad que ofrezca el servicio de almacenaje y conservación de copias de seguridad.

5.5 Recuperación de las copias de seguridad

Cada tres meses se debe realizar una simulación de recuperación de las copias de seguridad, y dejar registrado el resultado de la simulación, e informando al Administrador de la red si se obtuvo un error en el proceso.

6. Control

La Empresa realizará auditorias internas periódicas para garantizar el cumplimiento de los controles establecidos en este procedimiento.

7. Penalizaciones

Cuando el Administrador del Sistema Informático detecte incumplimiento en este procedimiento, puede tomar cualquiera de las siguientes medidas:

- Notificar la incidencia al Responsable de Seguridad.

8. Divulgación

Publicado el 30 de marzo de 2012.

9. Revisión

Este documento se revisará anualmente.

ANEXO 1 – PLANILLA DE COPIAS DE SEGURIDAD

IDENTIFICACION CINTA	TIPO COPIA (NORMAL/INCR)	FECHA COPIA	HORA INICIO	HORA FINAL	FECHA VENCIM.	ORIGINAL/ DUPLICADO	OPERADOR	OBSERVACIONES

3.7. Registros requeridos para el desarrollo del proceso

Se deben crear y mantener registros que evidencien la conformidad con los requisitos y el funcionamiento del SGSI. Estos registros deben estar debidamente protegidos y controlados; permanecer legibles, fácilmente identificables y recuperables. Se deben tener en cuenta también los registros que sean necesarios por requerimiento legal u obligación contractual de la empresa.

3.8. Declaración de aplicabilidad

De acuerdo a los resultados del análisis de riesgo, se deberán seleccionar los controles a implementar y a excluir, con su correspondiente justificación, se señalan también si hay controles actualmente implementados; también es recomendable mencionar cómo se realizará la implementación, este documento debe ser aprobado por la Dirección General de la empresa.

Referencia en ISO 27001: 4.2.1 h), i), j)

Se sugiere utilizar un formato como el siguiente, en el que se muestran los controles establecidos en el Anexo A de la Norma ISO 27001:

inteco Instituto Nacional de Tecnologías de la Comunicación	SGSI DECLARACION DE APLICABILIDAD	
N. Versión: 1.0		Página ___ de ____

Controles de la Norma ISO 27001			Controles actuales	Justificación para exclusión	Controles seleccionados y razón para su selección				Observaciones
					RL	OC	RN/MP	RAR	
Claúsula	**Numeral**	**Controles y Objetivos de control**							
5. POLITICA DE SEGURIDAD	**5.1**	**Política de seguridad de la información**							
	5.1.1	Documento de política de seguridad de la información							
	5.1.2	Revisión de la política de seguridad de la información							
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**6.1**	**Organización interna**							
	6.1.1	Comité de gestión de seguridad de la información							
	6.1.2	Coordinación de la seguridad de la información							
	6.1.3	Asignación de responsabilidades relativas a la seguridad de la información							
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información							
	6.1.5	Acuerdos de confidencialidad							
	6.1.6	Contacto con las autoridades							
	6.1.7	Contacto con grupos de interés especial							
	6.1.8	Revisión independiente de la seguridad de la información							
	6.2	**Terceros**							
	6.2.1	Identificación de los riesgos derivados del acceso de terceros							
	6.2.2	Tratamiento de la seguridad en la relación con los clientes							
	6.2.3	Tratamiento de la seguridad en contratos con terceros							
7. GESTIÓN DE ACTIVOS	**7.1**	**Responsabilidad sobre los activos**							
	7.1.1	Inventario de activos							
	7.1.2	Propiedad de los activos							
	7.1.3	Uso aceptable de los activos							
	7.2	**Clasificación de la información**							
	7.2.1	Directrices de clasificación							
	7.2.2	Etiquetado y manipulado de la información							
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**8.1**	**Antes del empleo**							
	8.1.1	Funciones y responsabilidades							
	8.1.2	Investigación de antecedentes							
	8.1.3	Términos y condiciones de contratación							
	8.2	**Durante el empleo**							
	8.2.1	Responsabilidades de la Dirección							
	8.2.2	Concienciación, formación y capacitación en seguridad de la información							
	8.2.3	Proceso disciplinario							
	8.3	**Cese del empleo o cambio de puesto de trabajo**							
	8.3.1	Responsabilidad del cese o cambio							
	8.3.2	Devolución de activos							
	8.3.3	Retirada de los derechos de acceso							

inteco Instituto Nacional de Tecnologías de la Comunicación	SGSI DECLARACION DE APLICABILIDAD	
N. Versión: 1.0		Página ___ de ____

Controles de la Norma ISO 27001			Controles actuales	Justificación para exclusión	Controles seleccionados y razón para su selección				Observaciones
					RL	OC	RN/MP	RAR	
Claúsula	**Numeral**	**Controles y Objetivos de control**							
9. SEGURIDAD FÍSICA Y AMBIENTAL	**9.1**	**Áreas seguras**							
	9.1.1	Perímetro de seguridad física							
	9.1.2	Controles físicos de entrada							
	9.1.3	Seguridad de oficinas, despachos e instalaciones							
	9.1.4	Protección contra las amenazas externas y de origen ambiental							
	9.1.5	Trabajo en áreas seguras							
	9.1.6	Areas de acceso público y de carga y descarga							
	9.2	**Seguridad de los equipos**							
	9.2.1	Emplazamiento y protección de equipos							
	9.2.2	Instalaciones de suministro							
	9.2.3	Seguridad del cableado							
	9.2.4	Mantenimiento de los equipos							
	9.2.5	Seguridad de los equipos fuera de las instalaciones							
	9.2.6	Reutilización o retirada segura de equipos							
	9.2.7	Retirada de materiales propiedad de la empresa							
10. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	**10.1**	Responsabilidades y procedimientos de operación							
	10.1.1	Documentación de los procedimientos de operación							
	10.1.2	Gestión de cambios							
	10.1.3	Segregación de tareas							
	10.1.4	Separación de los recursos de desarrollo, prueba y operación							
	10.2	**Gestión de la provisión de servicios por terceros**							
	10.2.1	Provisión de servicios							
	10.2.2	Supervisión y revisión de los servicios prestados por terceros							
	10.2.3	Gestión de cambios en los servicios prestados por terceros							
	10.3	**Planificación y aceptación del sistema**							
	10.3.1	Gestión de capacidades							
	10.3.2	Aceptación del sistema							
	10.4	**Protección contra código malicioso y descargable**							
	10.4.1	Controles contra el código malicioso							
	10.4.2	Controles contra el código descargado en el cliente							
	10.5	**Copias de seguridad**							
	10.5.1	Copias de seguridad de la información							
	10.6	**Gestión de la seguridad de las redes**							
	10.6.1	Controles de red							
	10.6.2	Seguridad de los servicios de red							
	10.7	**Manipulación de los soportes**							
	10.7.1	Gestión de soportes extraible							

Controles de la Norma ISO 27001			Controles actuales	Justificación para exclusión	Controles seleccionados y razón para su selección				Observaciones
					RL	OC	RN/MP	RAR	
Claúsula	**Numeral**	**Controles y Objetivos de control**							
	10.7.2	Retirada de soportes							
	10.7.3	Procedimientos de manipulación de la información							
	10.7.4	Seguridad de la documentación del sistema							
	10.8	**Intercambio de información**							
	10.8.1	Políticas y procedimientos de intercambio de información							
	10.8.2	Acuerdos de intercambio							
	10.8.3	Soportes físicos en tránsito							
	10.8.4	Mensajería electrónica							
	10.8.5	Sistemas de información corporativo/de negocio							
	10.9	**Servicios de comercio electrónico**							
	10.9.1	Comercio electrónico							
	10.9.2	Transacciones en linea							
	10.9.3	Información puesta a disposición pública							
	10.10	**Supervisión**							
	10.10.1	Registro de auditorias							
	10.10.2	Supervisión del uso del sistema							
	10.10.3	Protección de la información de los registros							
	10.10.4	Registros de administración y operación							
	10.10.5	Registro de fallos							
	10.10.6	Sincronización del reloj							
11. CONTROL DE ACCESO	**11.1**	Requisito del negocio para el control de acceso							
	11.1.1	Política de control de acceso							
	11.2	Gestión de acceso de usuario							
	11.2.1	Registro de usuario							
	11.2.2	Gestión de privilegios							
	11.2.3	Gestión de contraseñas de usuarios							
	11.2.4	Revisión de los derechos de acceso de usuario							
	11.3	**Responsabilidades de usuario**							
	11.3.1	Uso de contraseña							
	11.3.2	Equipo de usuario desatendido							
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia							
	11.4	**Control de acceso a la red**							
	11.4.1	Política de uso de los servicios en red							
	11.4.2	Autenticación de usuario para conexiones externas							
	11.4.3	Identificación de los equipos en las redes							
	11.4.4	Diagnóstico remoto y protección de los puertos de configuración							
	11.4.5	Segregación de las redes							
	11.4.6	Control de conexión a la red							
	11.4.7	Control de encaminamiento (router) de red							
	11.5	**Control de acceso al sistema operativo**							
	11.5.1	Procedimientos seguros de inicio de sesión							

Controles de la Norma ISO 27001			Controles actuales	Justificación para exclusión	Controles seleccionados y razón para su selección				Observaciones
					RL	OC	RN/MP	RAR	
Claúsula	**Numeral**	**Controles y Objetivos de control**							
	11.5.2	Identificación y autenticación de usuario							
	11.5.3	Sistema de gestión de contraseñas							
	11.5.4	Uso de los recursos del sistema							
	11.5.5	Desconexión automática de sesión							
	11.5.6	Limitación del tiempo de conexión							
	11.6	**Control de acceso a las aplicaciones y a la información**							
	11.6.1	Restricción del acceso a la información							
	11.6.2	Aislamiento de sistemas sensibles							
	11.7	**Ordenadores portátiles y teletrabajo**							
	11.7.1	Ordenadores portátiles y comunicaciones móviles							
	11.7.2	Teletrabajo							
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION	**12.1**	**Requisitos de seguridad de los sistemas de información**							
	12.1.1	Análisis y especificaciones de los requisitos de seguridad							
	12.2	**Tratamiento correcto de las aplicaciones**							
	12.2.1	Validación de los datos de entrada							
	12.2.2	Control del tratamiento interno							
	12.2.3	Integridad de los mensajes							
	12.2.4	Validación de los datos de salida							
	12.3	**Controles criptográficos**							
	12.3.1	Política de uso de los controles criptográficos							
	12.3.2	Gestión de claves							
	12.4	**Seguridad de los archivos del sistema**							
	12.4.1	Control del software en explotación							
	12.4.2	Protección de los datos de prueba del sistema							
	12.4.3	Control de acceso al código fuente de los programas							
	12.5	**Seguridad en los procesos de desarrollo y soporte**							
	12.5.1	Procedimientros de control de cambios							
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo							
	12.5.3	Restricciones a los cambios en los paquetes de software							
	12.5.4	Fugas de información							
	12.5.5	Externalización del desarrollo de software							
	12.6	**Gestion de la vulnerabilidad técnica**							
	12.6.1	Control de las vulnerabilidades técnicas							
13. GESTIÓN DE INCIDENTES DE	**13.1**	**Notificación de eventos y puntos débiles de la seguridad de la información**							
	13.1.1	Notificación de los eventos de seguridad de la información							
	13.1.2	Notificación de puntos débiles de la seguridad							

Controles de la Norma ISO 27001			Controles actuales	Justificación para exclusión	Controles seleccionados y razón para su selección				Observaciones
					RL	OC	RN/MP	RAR	
Claúsula	Numeral	Controles y Objetivos de control							
INCIDENTES DE SEGURIDAD DE LA INFORMACION	**13.2**	**Gestión de incidentes de seguridad de la información y mejoras**							
	13.2.1	Responsabilidades y procedimientos							
	13.2.2	Aprendizaje de los incidentes de seguridad de la información							
	13.2.3	Recopilación de evidencias							
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**14.1**	**Aspectos de seguridad en la gestión de la continuidad del negocio**							
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio							
	14.1.2	Continuidad del negocio y evaluación de riesgos							
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información							
	14.1.4	Marco de referencia para la planificación de la continuidad del negocio							
	14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio							
15. CUMPLIMIENTO	**15.1**	**Cumplimiento de los requisitos legales**							
	15.1.1	Identificación de la legislación aplicable							
	15.1.2	Derechos de propiedad intelectual (IPR)							
	15.1.3	Protección de los documentos/de la organización							
	15.1.4	Protección de datos y privacidad de la información personal							
	15.1.5	Prevención y uso indebido de los recursos de tratamiento de la información							
	15.1.6	Regulación de los controles criptográficos							
	15.2	**Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico**							
	15.2.1	Cumplimiento de las políticas y normas de seguridad							
	15.2.2	Comprobación del cumplimiento técnico							
	15.3	**Consideraciones sobre las auditorias de los sistemas de información**							
	15.3.1	Controles de auditoria de los sistemas de información							
	15.3.2	Protección de las herramientas de auditoria de los sistemas de información							

RL: Requerimientos legales - **OC**: Obligaciones contractuales - **RN/MP**: Requerimientos del negocio/mejores prácticas - **RAR**: Resultados del Análisis de riesgos

Conclusiones

Un Sistema de Gestión de Seguridad de la información (SGSI) puede definirse como la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

El desarrollo de un SGSI se basa en la norma ISO 27001/2005, la cual especifica los requisitos para establecer, implantar, documentar y evaluar un SGSI y también bajo ella se logra la certificación para las organizaciones que lo deseen. Se basa también en el Ciclo de Deaming (o PHVA), para garantizar la actualización del sistema y la mejora continua, mediante la aplicación de las siguientes fases: Planificar (establecer el SGSI), Hacer (implantar y operar el SGSI), Verificar (monitorizar y revisar el SGSI) y Actuar (mantener y mejorar el SGSI).

Dentro del SGSI se deben tomar decisiones respecto al cumplimiento de políticas, estas deben ser impulsadas por la Dirección de la organización, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la empresa. Así mismo, para poder tener una implantación exitosa del SGSI, los objetivos del mismo deben estar alineados al negocio de la empresa, de lo contrario el valor que agrega no sería muy evidente.

La concientización de la empresa es un apoyo fundamental de esta norma, es por esto que las organizaciones deben buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados.

También es importante el establecimiento de medidas técnicas, organizativas y procedimentales que garanticen la continuidad de las actividades o procesos de negocio, en caso de incidencias graves, es decir el diseño, implantación y mantenimiento del Plan de Continuidad, como parte del Plan de Seguridad de la empresa y como resultado del Análisis y Gestión de Riesgos.

Un SGSI no puede ser implantado por moda sino siempre buscando objetivos claros que agreguen valor a la organización. Toda nueva implementación debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI.

El tener implantado un SGSI certificado bajo la norma ISO 27001 no significar contar con seguridad máxima en la información de la organización, sino que la empresa cumple con los requerimientos y mejores prácticas establecidas en dicha norma, para que su SGSI actual funcione correctamente y además pueda evolucionar hacia la mejora continua.

Anexos

Anexo 1. Norma de contraseñas

INDICE

Versión	Redactado / revisado por	Aprobado por	Fecha aprobación	Fecha publicación

Referencia en ISO 27001: A.11.2.3, A.11.3.1, A.11.5.3.

RESPONSABLE DEL DOCUMENTO:

1. Objetivo

Definir las normas que se deben aplicar en la configuración y uso de las contraseñas de usuarios.

Para garantizar la protección y autenticación de acceso a los sistemas, es importante que las contraseñas cumplan unos requisitos mínimos que garanticen la robustez del sistema.

2. Ámbito de aplicación

De obligatorio cumplimiento para todos los usuarios de la empresa.

Entrará en vigencia el día 1º. de abril del 2011 y permanecerá vigente hasta la próxima versión aprobada de la misma.

3. Cumplimiento con los requisitos legales y estándares de seguridad

La presente norma proporciona cobertura a aspectos recogidos en los siguientes controles de la ISO 27001, Anexo A:

A.11.2.3. Gestión de las contraseñas de usuario

A.11.3.1. Uso de las contraseñas

A.11.5.3. Sistema de gestión de las contraseñas

4. Descripción de la norma

4.1. Todo identificador de usuario que se asigne por la compañía es único y permite la relación única entre el usuario y la persona que representa; así mismo dicho identificador permite exclusivamente el acceso a las funciones establecidas.

4.2. Las contraseñas en todos los sistemas tienen una longitud mínima de 8 caracteres, la cual debe incluir mínimo 2 dígitos, 4 caracteres alfabéticos y un carácter especial; y no debe incluir o ser igual al nombre del usuario.

4.3. El número de intentos sucesivos fallidos en la introducción de contraseña es de cinco (5), después de lo cual será bloqueado el usuario.

4.4. La contraseña debe ser cambiada cada dos (2) meses y no debe usarse ninguna de las anteriores cinco (5) claves.

4.5. Se deberá cambiar la contraseña siempre que exista la sospecha que otras personas puedan tener conocimiento de la misma.

4.6. La contraseña es de uso exclusivo del usuario al cual pertenece.

4.7. Las contraseñas se deberán entregar de forma segura a los usuarios. Los usuarios deben utilizar exclusivamente los identificativos asignados a su persona, manteniendo en secreto las correspondientes contraseñas, y siendo responsables por las transacciones realizadas en el Sistema Informático, con el usuario/contraseña que utiliza.

4.8. En caso de olvido de la contraseña, o bloqueo por acumulación de intentos fallidos de acceso al sistema, se reinicializará la contraseña a través del sistema de desafíos pregunta-respuesta.

4.9. Los usuarios deben seleccionar contraseñas de calidad, de acuerdo a las siguientes recomendaciones:

a. Se debe evitar utilizar la misma contraseña en todos los sistemas disponibles.

b. No utilizar información personal en la contraseña: nombre del usuario o de familiares, ni los apellidos, ni la fecha de nacimiento. Se recomienda la utilización de letras mayúsculas y minúsculas en la contraseña.

c. El usuario es responsable de mantener en secreto su contraseña. Se debe evitar guardar o escribir la contraseña en cualquier papel o dejar constancia de ella.

5. Controles

5.1. La asignación del identificador único para los usuarios se debe realizar mediante un proceso formal denominado Acuerdo sobre el uso de los sistemas de información, donde queda establecida la responsabilidad y obligaciones en el uso de dicho identificador, especialmente que se comprometen a mantener sus contraseñas personales en secreto y las posibles consecuencias de un mal uso.

5.2. Deben implementarse en todos los sistemas de información de la compañía, los mecanismos de autenticación y autorización que garanticen el cumplimiento de los requisitos definidos en

esta norma para las contraseñas de los usuarios: longitud mínima, complejidad, tiempo de bloqueo, caducidad, historial de claves.

5.3. Se debe garantizar que los usuarios cambien las contraseñas iniciales que les son asignadas la primera vez que ingresan al sistema. Las contraseñas temporales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.

5.4. Cuando se introduzca la contraseña en los sistemas, nunca debe aparecer de forma visible y legible en la pantalla.

5.5. Se debe establecer una política de control de accesos en base a las necesidades de seguridad de la compañía, dicha política debe ser revisada periódicamente.

5.6. Debe existir un procedimiento formal para dar de alta y baja a los usuarios, con el fin de garantizar y cancelar los accesos a todos los sistemas y servicios de información existentes en la compañía.

5.7. Auditar los sistemas para garantizar que se cumplen los controles recogidos en esta norma. En el supuesto de que no se aplique alguno de los controles, se deberán justificar y documentar estas excepciones. Se deberá mantener un registro donde queden recogidas todas las excepciones, a disposición de las auditorias.

Bibliografía

Asociación Española de Normalización y Certificación – AENOR. (2007). *ISO/IEC 27001:2005 Sistemas de Gestión de la Seguridad de la Información. Especificaciones,*

Ministerio de Administraciones Públicas. (2006). *MAGERIT Versión 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*

Documentos y Webs:

INTECO-CERT. (2010). *Curso de Sistemas de Gestión de la Seguridad de la Información según la norma UNE-ISO/IEC 27000.*

http://www.inteco.es

Índice de figuras