Universidad de Cádiz
Seguridad y Competencias Profesionales
Curso 2009/2010

Política de Seguridad de Tecnologías de la Información de Bodegas San Dionisio, S.A.

Leopoldo Jesús Gutiérrez Galeano
Lidia Lebrón Amaya
Luis Nadal de Mora
Rafael Sánchez Martínez
Jesús Soriano Candón

17 de octubre de 2010

Índice general

Índice de figuras

Índice de cuadros

Historial de Cambios

Fecha	***Cambios***
17 de octubre de 2010	Primera versión del documento.

Compromiso de la dirección

En este capítulo (no numerado) se escribirá una carta formal firmada y sellada por los miembros relevantes de la dirección de la compañía y por el Responsable de Seguridad, en la que se relaciona la seguridad con las metas de la organización, se valida la versión actual de la política y se compromete a proveer los recursos necesarios para su ejecución.

1. Introducción

Nota del profesor: este guión es únicamente orientativo, y no se obliga a seguir este mismo orden y división en secciones ni a utilizar LaTeX. Sin embargo, se recomienda que el formato usado, sea cual sea, contenga la información recogida en este esquema. Es posible que no todo sea necesario, particularmente en organizaciones de menor tamaño.

Se recomienda hacer referencia y seguir las recomendaciones de las normas UNE-ISO/IEC 27002:2009 [1], UNE-ISO/IEC 27001 [2] (disponible a través de NORWEB en biblioteca.uca.es), UNE 71501 [3] y el resto del material del Campus Virtual. En particular, la norma UNE 71501-3 da ciertas guías sobre el contenido que debería tener una política de seguridad de TI de una organización.

1.1. Descripción de la Organización

Nombre de la organización, a qué se dedica, de qué activos (a alto nivel: locales, edificios, etc.) dispone, cuál es su organigrama, etc.

La organización para la que se diseña esta política de seguridad de denomina Bodegas San Dionisio, S.A.

Bodegas San Dionisio, S.A. se dedica a la producción y comercialización de vinos y brandis dentro de la zona de producción y crianza conocida como *Marco de Jerez*. Para ello, utiliza los métodos tradicionales de producción del Marco, estando adherida a todos los estándares de calidad requeridos por el *Consejo Regulador de la Denominación de Origen Jeréz-Xérès-Sherry*.

1.1.1. Estructura organizativa de la compañía

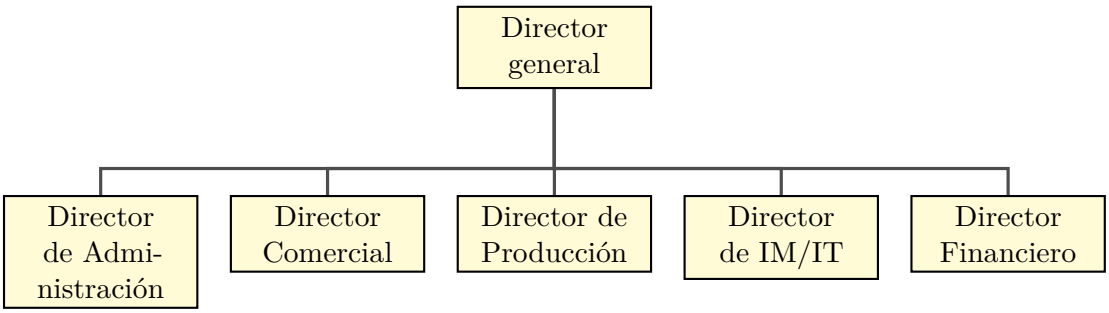
Los Directorados

La organización de la empresa se sustenta en una estructura de directorados y departamentos. El Director General y el resto de los Directores constituyen el Comité de Dirección ejecutiva, que se reúne quincenalmente.

Los directorados son los siguientes:

- Dirección de Administración.
- Dirección Comercial.

- Dirección de Producción.
- Dirección de IM/IT.
- Dirección Financiera.



Las funciones de los directorados y sus departamentos, se detallan en los siguientes apartados.

Dirección de Administración

La dirección de administración se ocupa de los asuntos relativos al personal de la empresa, y a la logística de compras y mantenimiento de las instalaciones.

Se divide en dos departamentos: *Personal* y *Logística*.

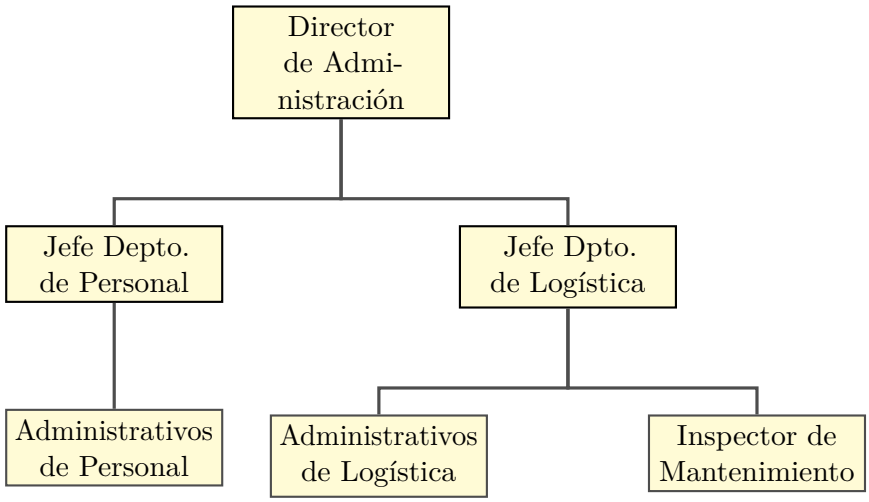
El *departamento de personal* tiene un jefe y varios administrativos, que se encargan de las siguientes funciones:

- Realización de las nóminas.
- Ejecución de los procesos de contratación y despidos.
- Ejecución de los procesos disciplinarios.
- Coordinación de las políticas de ascensos.

El *departamento de logística* tiene un jefe,varios administrativos, y un inspector de mantenimiento, que se encargan de la ejecución de los procedimientos de adquisición de materiales y servicios necesarios para el funcionamiento de la empresa, función que incluye:

- Búsqueda del precio más ventajoso y negociación con proveedores.
- Control de los plazos de terminación y renovación de contratos de servicios y obras.
- Inspección para asegurarse que los servicios y materiales adquiridos cumplen las condiciones estipuladas en los contratos.

- Revisión de facturas recibidas, y envío a Comptroller para su pago, si procede.

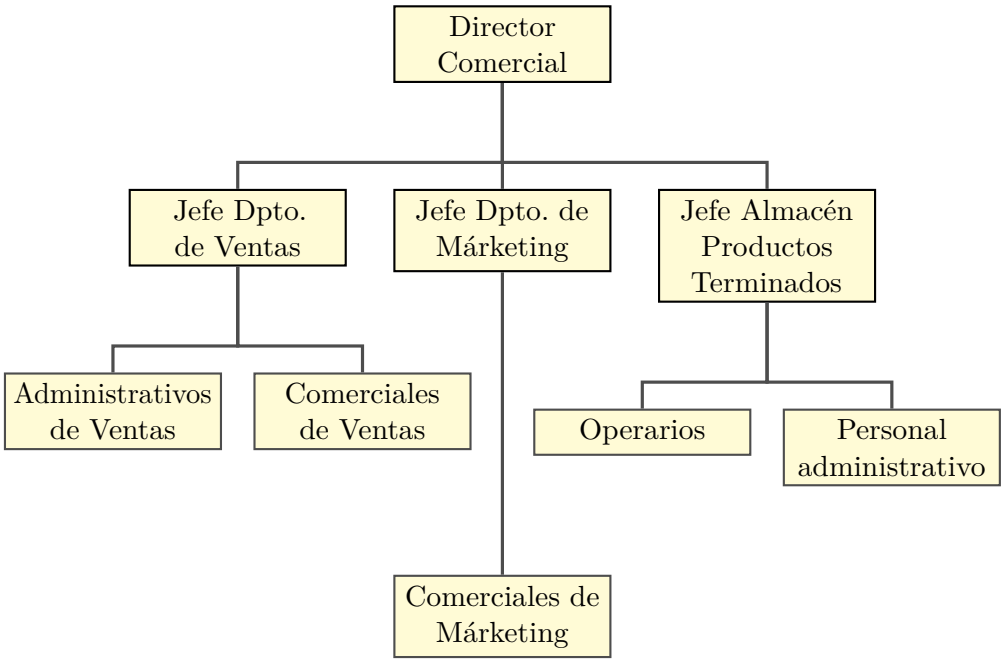


Dirección Comercial

La Dirección Comercial es responsable de planear y ejecutar la estrategia de ventas de la empresa. La encabeza el Director comercial, y tiene tres departamentos: el Departamento de Ventas, el departamento de Márketing, y el almacén de productos terminados.

- El **departamento de ventas** se encarga de la captación de clientes y pedidos de ventas. Se trata de un equipo de vendedores y administrativos. Las exportaciones son manejadas por una empresa intermediaria, por lo que esta compañía no tiene relaciones con el extranjero. Los clientes de la compañía son de los siguientes tipos:
  - Establecimientos de hostelería
  - Tiendas al por menor.
  - Grandes superficies.
  - Compañías distribuidoreas de alimentación.
  - Personas particulares.
- El **departamento de márketing** se encarga del diseño e ejecución de las campañas publicitarias, y trabaja en coordinación con el departamento de ventas y el financiero para el diseño de ofertas y promociones. También se encarga de asistir en la búsqueda de formas innovadoras de presentación y composición de los productos, en coordinación con la Dirección de Producción.
- El **almacén de productos terminados** dispone de un gran almacén donde están disponibles los productos antes de su salida vía pedidos, y tiene encomendadas las siguientes funciones:
  - Almacenamiento y control del stock de productos terminados.

- Preparación y despacho de pedidos. La compañía no tiene flota de transporte propia.



Dirección de Producción

La dirección de producción se encarga de la fabricación de los productos que la compañía tiene a la venta, siguiendo los procedmimentos establecidos por los comités técnicos, y cumpliendo con la normativa vigente de salud pública y protección al consumidor.

Este directorado tiene tres departamentos: Control de Calidad, Viñas, Planta de Molturación y Mostos, Envejecimiento, y Embotellado.

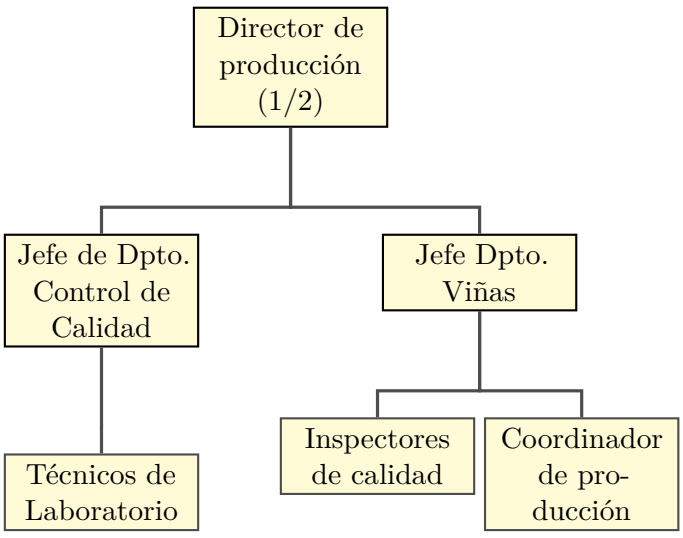
- El **Departamento de Control de Calidad** se encarga de la realización de las pruebas y cálculos pertinentes para asegurarse de que los productos terminados e intermedios que se están fabricando se realizan según los procedimientos estipulados, de que sus propiedades cumplen los niveles de calidad acordes a su categoría. Lo componen un Jefe de Control de Calidad, y varios técnicos de laboratorio.

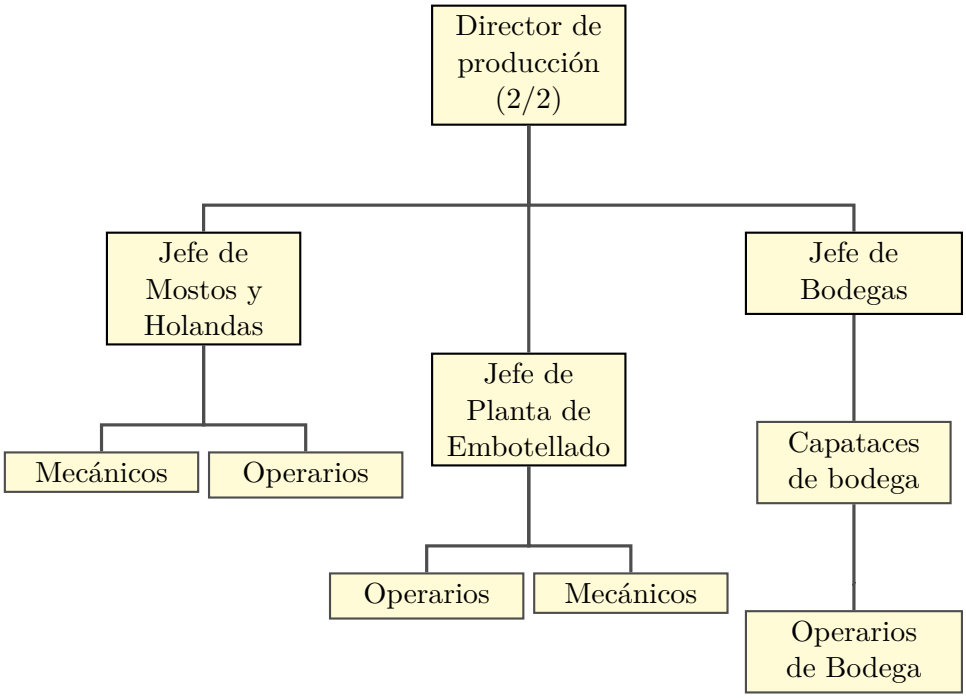
- El **Departamento de Viñas** se encarga de la relación con las fincas productoras de uva que pretenden vender o ya han vendido su producción a la bodega. Estas viñas autorizan a los *inspectores de calidad* de viñas a realizar visitas periódicas a las viñas para asegurarse que la producción contratada va a estar disponible y con unos niveles de calidad determinados en el momento de la vendimia. El *coordinador de producción* se encarga de informar al Jefe de Viñas de cualquier desviación en el volúmen de producción de uva esperado, así como estar enterado de las fluctuaciones de los precios de la uva.

- En la **planta de mostos y holandas** se realiza la recepción de la uva, su prensado para la extracción del zumo de la uva y su fermentación para la consecución del vino jóven o mosto. En esta planta también se realiza la destilación del alcohol para la elaboración el brandy a partir del mosto. A este alcohol obtenido se denomina la «holanda». Consta de un jefe de planta y varios operarios y mecánicos.

- La etapa de envejecimiento está controlada por el **Jefe de Bodega**. Los mostos y holandas se introducen en barriles para su envejecimiento. Esta etapa sigue unos procesos de mezclas y reposos realizados pos los operarios de las bodegas, de cuyas actividades informan a los capataces en forma de pequeños documentos llamados «estadillos».

- Por fin, la **planta de embotellamiento** realiza el embotellado de los productos envejecidos, según las indicaciones del director de producción. Los productos terminados se encaminan al almacén de productos terminados.





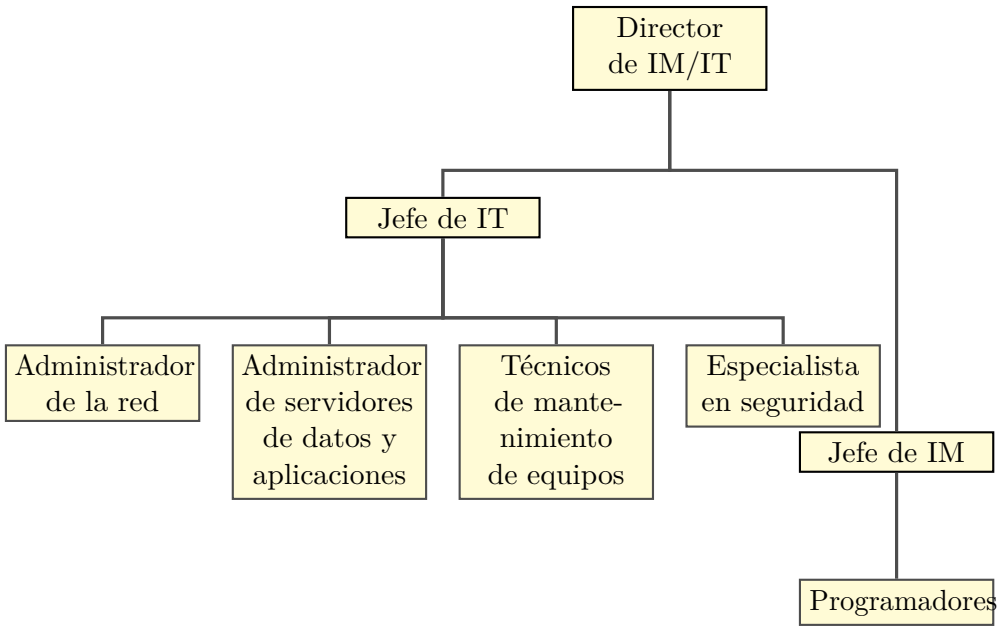
Dirección de IM/IT

Esta compañía le da mucha importancia estratégica al flujo de datos e información de la empresa, y ha decidido que el área de IM/IT va a tener un directorado.

Este directorado consta de dos depatamentos: IT (Information Technology) e IM (Informacion Management).

- El departamento de IT está compuesto de un administrador de redes, un administrador de servidores de aplicaciones y datos, dos técnicos de mantenimiento de equipos, y un especialista en seguridad informática. Las funciones de este departamento son:
  - Instalación, mantenimiento y administración de la infraestructura de red, servidores y comunicaciones de la organización.
  - Instalación, mantenimiento y administración de dispositivos finales (Computadoras, teléfonos móviles, etc.), y su correcta configuración según los servicios requeridos para el tipo de usuario.
  - Contratación de servicios externos para la instalación de infraestructura llegado el caso.
  - Inspección continua de seguridad de la infraestructura de sistemas de información de la empresa.
- El departamento de IM está compuesto por un Jefe de IM, y dos programadores, que cumplen las siguientes funciones:

- Análisis continuado de los procesos de negocio de la empresa, y búsqueda de las herramientas de información adecuadas para la mejora continua de dichos procesos.
- Recolección de los datos necesarios para la correcta valoración de las métricas diseñadas por el comité ejecutivo de dirección y el plan estratégico de la compañía, y mantenimiento del «Cuadro de Mandos» o «Dashboard» que contienen dichas métricas.
- Realización de informes más detallados sobre estos datos recolectados para ayudar a que los mandos de la compañía puedan realizar una supervisión más efectiva.
- Diseño de software, en el caso de que las necesidades específicas de la compañía no pueden ser cubiertas por productos comerciales.



Dirección Financiera

El **Director Financiero** es responsable de las siguientes funciones:

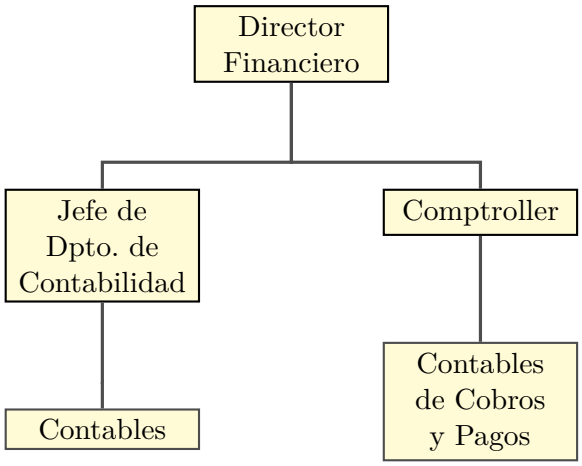
- Mantener fielmente y actualizada la información relativa al estado financiero de la empresa.
- Realizar las operaciones necesarias para el cumplimento de las normas en relación con las Haciendas locales y estatales.
- Realizar análisis de costes y beneficios que ayuden al resto de los Directores a realizar un mejor planeamiento de sus operaciones.

- Avisar a la Dirección de la Empresa de las desviaciones sobre presupuestos financieros y/o de gastos, que pudieran alterar la consecución de objetivos estratégicos de la compañía.

Para ello, el directorado se divide en dos departamentos: uno de **contabilidad**, y otro de **Comptroller**.

- El *departamento de contabilidad* se ocupa de la correcta contabilización de los documentos contables de la empresa, de su custodia según lo estipula la ley, y del cumplimiento de las obligaciones con las haciendas locales y estatales,y del análisis de costes.

- El comptroller se ocupa del análisis del flujo de pagos y cobros, y de que el destino de los recursos de la empresa no se desvíe de la función para la que fueron presupuestados.



1.2. Objetivos y alcance de la política

Aquí se indica qué nivel de seguridad se desea obtener, y se relacionan con los objetivos de la organización. Hay que además limitar el alcance de la polática, para evitar cubrir demasiado terreno, que puede exigir demasiado tiempo.

1.3. Gestión y cambios de la política

Una política de seguridad no es algo estático, sino que se va revisando continuamente. Habrá que describir la forma en que se recogen las propuestas de cambio, se realizan los cambios pertinentes y se difunde de nuevo al resto del personal la última versión de la política, de forma clara e inequívoca.

1.4. Organización de la Seguridad

En esta sección se describe cómo se va a organizar la gestión de la seguridad en la organización a lo largo de todo su organigrama. Deberáa tenerse en cuenta a todos los departamentos, y no sólo al de Informática.

Hay que definir responsabilidades y gestión de los informes de las incidencias. También se deberáan definir a alto nivel los mecanismos que se usarían para comprobar que se llevan a cabo las medidas indicadas en este documento.

En este apartado se deberáan tener en cuenta las medidas explicadas en «Seguridad en el entorno» para limitar el riesgo por ataques internos, tomando en cuenta la matriz de peligrosidad mostrada en las transparencias.

2. Política de seguridad de la información

Este capítulo puede dedicarse a los riesgos que afectan a la información almacenada y obtenida en la organización. Para ello, habrá que describir qué información a nivel abstracto trata la organización y cuál es su nivel de sensibilidad.

Habrá que relacionarla con la Ley Orgánica de Protección de Datos, aunque los documentos de seguridad para la LOPD tendrán que elaborarse por separado de este trabajo. Para los documentos de seguridad se pueden seguir los modelos disponibles en el Campus Virtual.

Este capítulo hará referencia a las medidas implantadas en otros capítulos dedicados a la seguridad de las comunicaciones (capítulo 6 on page 19), del software y hardware (capítulo 5 on page 17) y de la seguridad física (capítulo 3 on page 13), entre otros.

2.1. Información recogida

Descripción a alto nivel de la información que utiliza la organización para llevar a cabo sus fines.

2.2. Análisis de riesgos y sensibilidad

Aquí se haráa un estudio de lo delicada que es la información tratada, y de a qué riesgos se halla sometida, de acuerdo con las tres bases de la seguridad (confidencialidad, integridad y disponibilidad).

2.3. Conformidad con la legislación vigente

Se equiparará la información antes recogida con los requisitos impuestos por la Ley Orgánica de Protección de Datos y otras leyes aplicables, si las hay, y se hará referencia a sus documentos de seguridad, a elaborar por separado.

3. Política de seguridad física

En este capítulo se indicarán las medidas que se usarán para proteger los activos de la organización, de acuerdo con lo indicado en el tema de «Seguridad en el entorno». Las medidas a implantar se basarán en un análisis previo de los riesgos existentes.

Se recomienda consultar «Seguridad física COMO», el estándar UNE-ISO/IEC 272002 [1] y las normas UNE 71501 [3] disponibles en el Campus Virtual. En la norma UNE 71501-3 se recogen algunos de los tipos de riesgos más comunes: entradas no autorizadas, rayos, robos, incendios, accesos no autorizados a estaciones de trabajo, etc.

3.1. Activos

Activos de la organización a nivel físico: locales a proteger, teniendo en cuenta su división en áreas más y menos sensibles.

3.2. Seguridad del edificio

Edificio en general: fluido eléctrico, líneas de teléfono, protección contra entradas no autorizadas, protección contra incendios, etc.

3.3. Seguridad del centro de datos

Protección del centro de datos en que se alojan los servidores: emplazamiento, uso de falso techo/suelo, aire acondicionado, control de acceso y auditorías, etc. Es posible que la protección a incendios o alguna de las medidas a nivel de edificio cambie aquí.

3.4. Seguridad del lugar de trabajo

Protección de la estación de trabajo de cada empleado, evitando accidentes laborales, entradas no autorizadas, robos, volcado de líquidos, etc.

4. Política de control del personal

En este capítulo se deben tratar aquellos riesgos correspondientes con los ataques provenientes de atacantes externos e internos, y la formación de los usuarios, entre otras cosas, de acuerdo con el tema «Seguridad en el entorno».

Además de los recursos situados en el Campus Virtual, deberían tenerse en cuenta las recomendaciones de la guía UNE-ISO/IEC 17799 [1].

4.1. Proceso de contratación

Se describirán las modificaciones necesarias sobre el proceso de contratación para asegurar la seguridad en TI. No es necesario describir el resto del proceso (p. ej. aspectos administrativos).

4.2. Proceso de despido

Como el anterior apartado, pero para cuando alguien deja la organización.

4.3. Formación y concienciación del personal

Especifica qué acciones se llevarán a cabo para que el personal conozca la importancia de la seguridad y sepa qué hacer en cada caso.

4.4. Medidas disciplinarias

Acciones a realizar cuando el personal voluntaria o involuntariamente rodea o va en contra de alguna de las medidas de este documento.

4.5. Personal temporal y subcontratado

Indica cómo se atajarán los problemas de seguridad que supone el acceso de personal externo a la organización a sus facilidades.

5. Política de seguridad en software y hardware

En este capítulo se tratarán los aspectos relacionados con la seguridad del software desarrollado y/o utilizado internamente, y la prevención, detección y diagnóstico del software malicioso. También se tratarán los aspectos relacionados con el hardware de los activos de la organización.

Para los aspectos de desarrollo de software, se puede tomar como guía en la sección de desarrollo las recomendaciones de las transparencias y los informes CWE más relevantes, posiblemente integrándolos en las revisiones periódicas del código, si se desean implantar.

Habrá que analizar los riesgos que supone el software malicioso, y en base a ellos plantear las debidas medidas de prevención, detección y recuperación.

5.1. Identificación y autenticación

Se recogen las distintas medidas a través de las cuales se limitará el acceso a los distintos equipos al personal que los necesite para su trabajo.

5.2. Registro de accesos

En algunos equipos puede ser Ãºtil llevar un control de quién ha accedido, desde dónde, etc.

5.3. Protección ante software malicioso

Medidas para mitigar los riesgos relacionados con el software malicioso.

5.4. Uso aceptable de los equipos

Se recogería cuál es el uso aceptable de los equipos de la organización, dividiéndolos según su aplicación (servidores, estaciones de trabajo y portátiles).

5.5. Gestión de soportes

Medidas a la hora de almacenar y desechar los soportes de almacenamiento.

6. Política de seguridad de las comunicaciones

Esta sección se dedicará a describir cómo se protegerán las conexiones internas y externas, los datos que recorran la red interna de la organización, y cómo se evitarán las fugas de información hacia el exterior.

6.1. Infraestructura y topología de la red

Hay que describir la red existente a alto nivel, con el equipamiento utilizado. Como mínimo debe describirse la topología a alto nivel, con sus enrutadores, conmutadores y estaciones de trabajo. Normalmente se seguirá un cableado estructurado, si la organización es lo suficientemente grande.

6.2. Seguridad de las conexiones al exterior

Se describirán las conexiones al exterior (internet, PBX) y cómo se protegerán ante accesos no autorizados. Si se estima necesario, pueden tomarse medidas para asegurar la disponibilidad de la conexión (enlaces redundantes, por ejemplo).

Normalmente habrá que establecer un perímetro de seguridad para proteger la red de la organización de las amenazas exteriores.

6.3. Seguridad de la información transmitida

Medidas para evitar que la información transmitida sea bloqueada, interceptada, modificada o falsamente fabricada.

6.4. Seguridad en el teletrabajo

Si en la organización se permite el teletrabajo, habrá que tomar las medidas necesarias para que esto no suponga una amenaza de seguridad.

7. Política de continuidad del negocio

Este capítulo se dedica fundamentalmente a las medidas de recuperación en caso de un ataque o un desastre.

7.1. Introducción

En esta primera sección se puede describir qué partes son especialmente vitales para el funcionamiento continuado de la organización, y que por lo tanto requieren de una mayor inversión de sus recursos.

Habrá que priorizar la recuperación de ciertos activos frente a otros: servidores frente a estaciones de trabajo, datos sensibles frente a información derivada, etc.

7.2. Copias de seguridad

Esta sección se dedica a las copias de seguridad, indicando de qué se harán copias, con qué frecuencia, de qué tipos, usando qué soportes y juegos de copias, etc.

7.3. Recuperación de activos

Planificación para la recuperación de un activo ante un desastre o un ataque. Puede tratarse de una parte de las infraestructuras, hardware, software (con su configuración asociada), o datos.

Para software, por ejemplo, lo usual es mantener documentación actualizada sobre el estado de la configuración de los sistemas, de forma que ante un ataque al software se pueda reinstalar y volver a configurar. Esto requiere señalar quién será responsable de mantener dicha documentación al día, con qué periodicidad será revisada, y quién llevará el control de dichas medidas, entre otros aspectos.

A. Presupuestos de material

Aquí se listarán una serie de presupuestos iniciales para los distintos elementos que puedan utilizarse para llevar a cabo la política.

A.1. Software

Presupuestos del software necesario: cortafuegos, antivirus, etc.

A.2. Hardware

Presupuestos del hardware necesario: equipamiento de red, sistemas de alimentación ininterrumpida, etc.

A.3. Infraestructuras

Presupuestos para los materiales de infraestructuras: detectores de humo, detectores de presencia, cámaras de seguridad, armarios ignífugos, cerrojos de múltiples cilindros, extintores, etc.

A.4. Servicios

Presupuestos para cursos de formación y concienciación (a menos que sean internos), contratación de personal de seguridad, alquiler de cámaras conectadas a una centralita remota, etc.

B. Otros anexos

Se dedicarán más anexos para aquellas listas y materiales que por su extensión rompan el flujo normal del texto de una determinada política, o que se consideren que pueden cambiar con más frecuencia.

Posibles anexos incluyen:

- Formularios a utilizar para gestionar las incidencias
- Normativa y legislación aplicable
- Procedimientos del responsable de seguridad y/o el comité de seguridad

Bibliografía

[1] *Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información*, UNE-ISO/IEC 27002:2009, AENOR.

[2] *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.*, UNE-ISO/IEC 27001:2007, AENOR.

[3] *Tecnología de la Información. Guía para la gestión de la seguridad de TI.*, UNE 71501:2001, AENOR.