

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

6 de noviembre de 2010

Índice general

Historial de Cambios	VII
Compromiso de la dirección	IX
1. Introducción	1
1.1. Descripción de la Organización	1
1.1.1. Estructura organizativa de la compañía	1
1.2. Objetivos y alcance de la política	8
1.3. Gestión y cambios de la política	8
1.4. Organización de la Seguridad	9
2. Política de seguridad de la información	11
2.1. Información recogida	11
2.2. Análisis de riesgos y sensibilidad	12
2.2.1. Codificación de amenazas	12
2.2.2. Personal autorizado en los ficheros	15
2.3. Conformidad con la legislación vigente	16
3. Política de seguridad física	17
3.1. Activos	17
3.2. Seguridad del edificio	17
3.2.1. Normativa de Seguridad contra incendios	18
3.2.2. Normativa de Compatibilidad Electromagnética	18
3.2.3. Normativa Eléctrica	18
3.3. Seguridad dentro del almacén	18
3.4. Seguridad del centro de datos	18
3.4.1. Seguridad de acceso	18
3.4.2. Seguridad interna	19
3.5. Seguridad del lugar de trabajo	19
4. Política de control del personal	21
4.1. Proceso de contratación	21
4.2. Proceso de despido	21
4.3. Formación y concienciación del personal	21
4.4. Medidas disciplinarias	21
4.5. Personal temporal y subcontratado	21

5. Política de seguridad en software y hardware	23
5.1. Identificación y autenticación	23
5.2. Registro de accesos	23
5.3. Protección ante software malicioso	23
5.4. Uso aceptable de los equipos	23
5.5. Gestión de soportes	23
6. Política de seguridad de las comunicaciones	25
6.1. Infraestructura y topología de la red	25
6.2. Seguridad de las conexiones al exterior	25
6.3. Seguridad de la información transmitida	25
6.4. Seguridad en el teletrabajo	25
7. Política de continuidad del negocio	27
7.1. Introducción	27
7.2. Copias de seguridad	27
7.3. Recuperación de activos	27
A. Presupuestos de material	29
A.1. Software	29
A.2. Hardware	29
A.3. Infraestructuras	29
A.4. Servicios	29
B. Otros anexos	31
Bibliografía	33

Índice de figuras

Índice de cuadros

Historial de Cambios

<i>Fecha</i>	<i>Cambios</i>
6 de noviembre 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 L^AT_EX. 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 Jerez-Xérès-Sherry*.

1.1.1. Estructura organizativa de la compañía

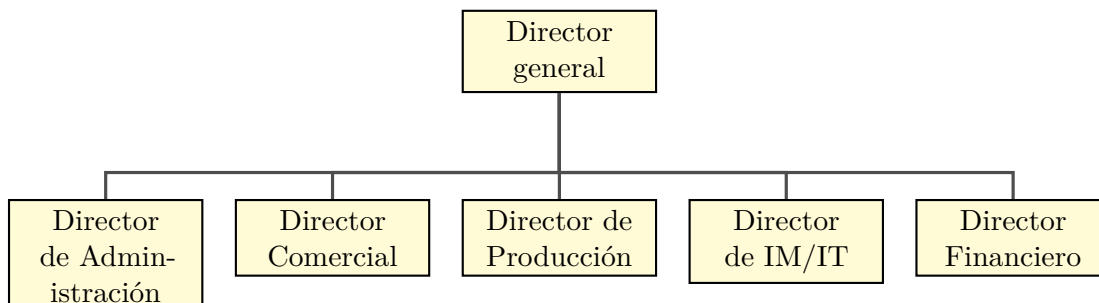
Los Directorados

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*.

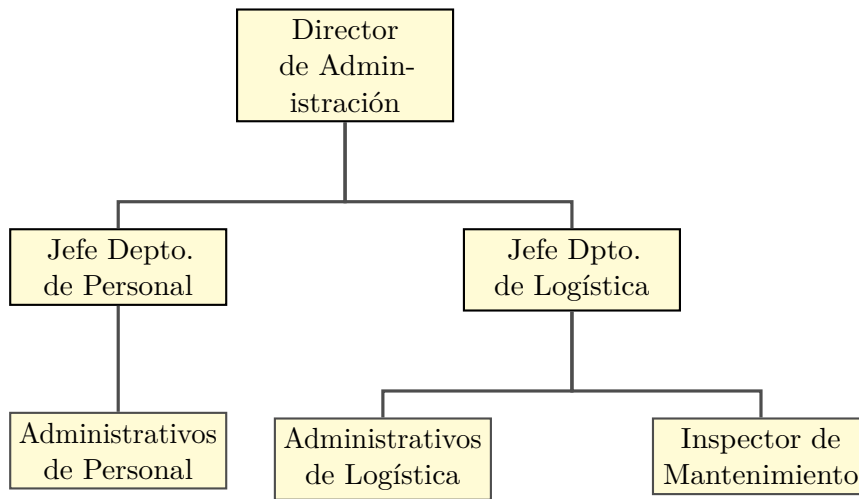
El *departamento de personal* tiene un jefe y varios administrativos, que se encargan de las siguientes funciones:

- 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.

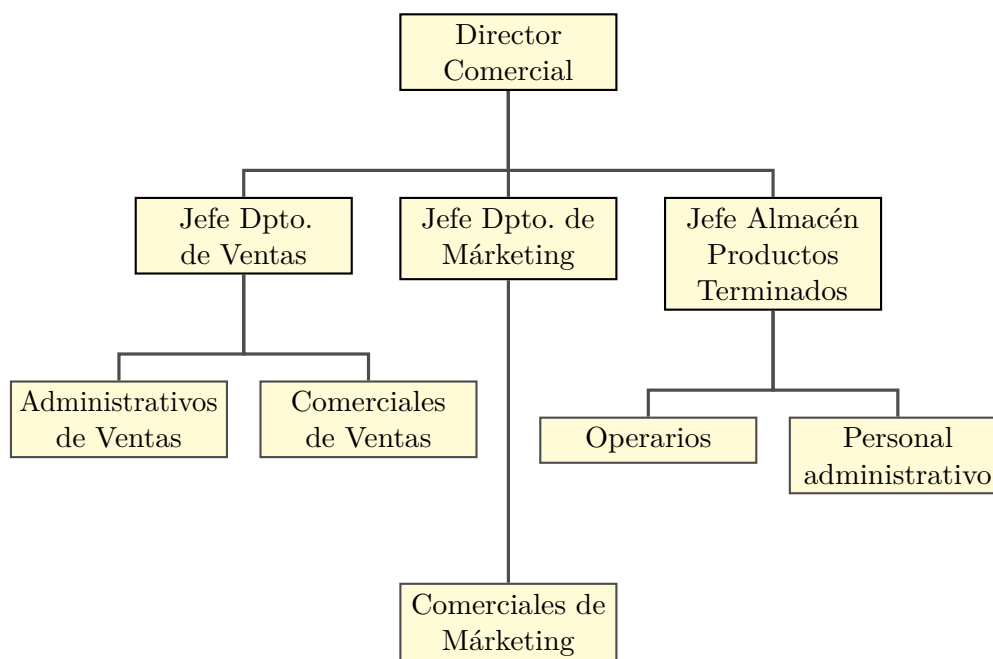


Dirección Comercial

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 distribuidoras 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.



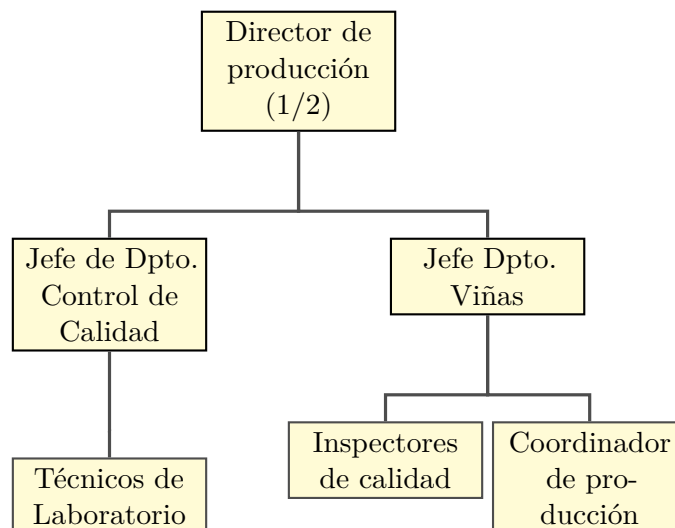
Dirección de Producción

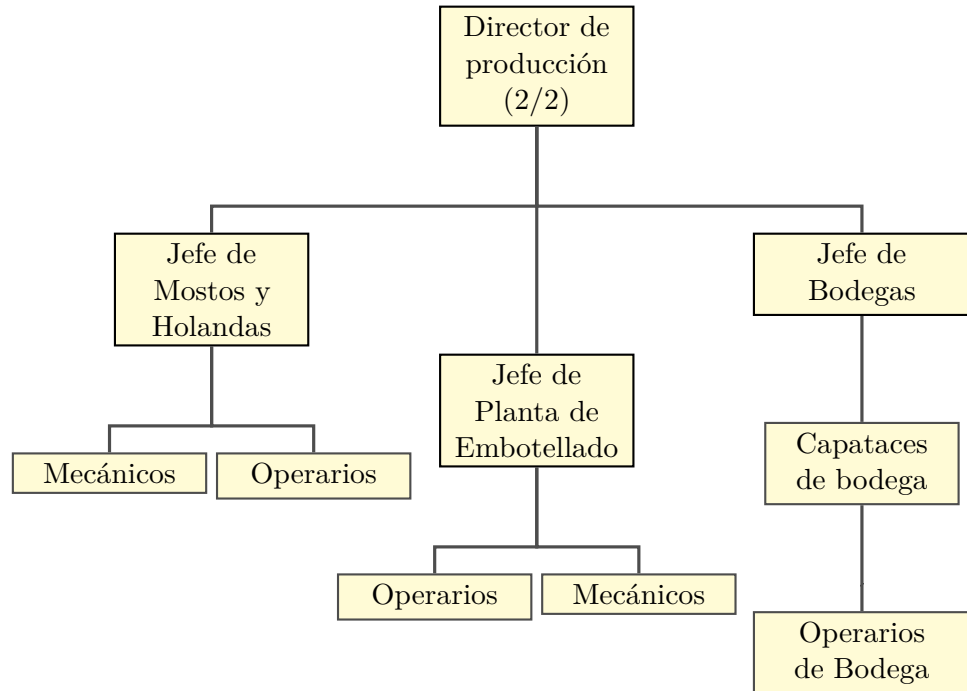
La dirección de producción se encarga de la fabricación de los productos que la compañía tiene a la venta, siguiendo los procedimientos establecidos por los comités técnicos, y cumpliendo con la normativa vigente de salud pública y protección al consumidor.

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 volumen 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 joven o mosto. En esta planta también se realiza la destilación del alcohol para la elaboración del 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 por 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.





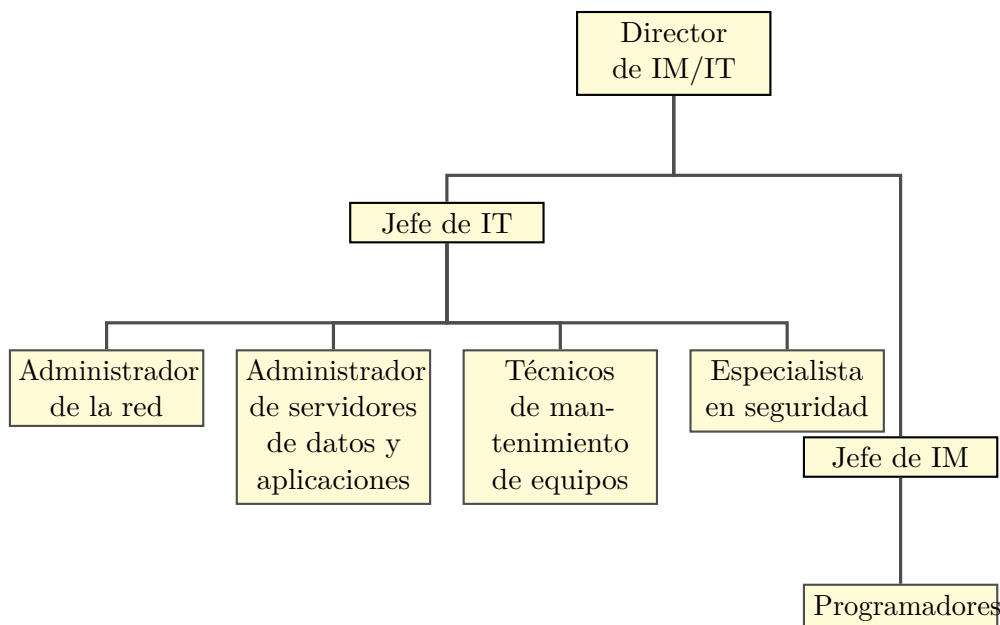
Dirección de IM/IT

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 departamentos: IT (Information Technology) e IM (Information 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

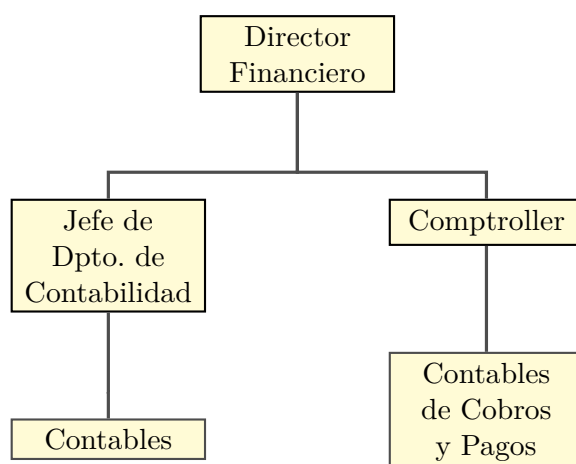
El **Director Financiero** es responsable de las siguientes funciones:

- Mantener fielmente y actualizada la información relativa al estado financiero de la empresa.
- Realizar las operaciones necesarias para el cumplimiento 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 política, 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. Deberá 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 deberán 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 deberán 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.

Habrà 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 25), del software y hardware (capítulo 5 on page 23) y de la seguridad física (capítulo 3 on page 17), entre otros.

2.1. Información recogida

En este punto se describe con qué tipo de información trabaja Bodegas San Dionisio S.A.. En esta empresa, se divide la información en seis ficheros claramente diferenciados, conteniendo cada uno de ellos información de distinto tipo, con los que normalmente trabajan distintos tipos de empleados de la empresa. Los ficheros de la empresa son los siguientes:

- **Fichero de personal:** en este fichero se guarda información sobre los datos personales del personal de la empresa, así como los datos correspondientes a las nóminas.
- **Fichero de proveedores:** se guardan los datos de los proveedores, la información sobre la logística de la empresa y las facturas de las materias primas adquiridas y de su transporte, así como los albaranes.
- **Fichero de clientes:** contiene los datos de los clientes, la gestión de pedidos, información sobre las ventas, la facturación y los albaranes correspondientes al transporte de mercancías.
- **Fichero financiero:** incluyen la información sobre los cobros, pagos, la contabilidad de la empresa, información sobre el IVA y los balances contables.
- **Fichero de producción:** aquí se guarda toda la información sobre la producción de la empresa y sobre las inspecciones de calidad. Estos datos se encuentran en un disco duro compartido, contenidos en hojas de cálculo de Excel, al que solo van a tener acceso las personas implicadas en su realización y lectura.

- **Fichero de informes:** principalmente se guardan los informes de dirección, que se pueden acabar representando como dashboards, etc. Estos informes y los dashboards se encuentran en unas hojas de Excel, dentro de un disco duro compartido, al que solo van a tener acceso las personas implicadas en su realización y lectura.

2.2. Análisis de riesgos y sensibilidad

En este punto, inicialmente se clasifican los tipos de amenazas a las que puede ser vulnerable la empresa, describiendo a continuación los riesgos a los que se halla sometida la información con la que se trabaja en Bodegas San Dionisio S.A..

2.2.1. Codificación de amenazas

Las posibles amenazas que se pueden llegar a dar, se han clasificado en una serie de tablas según el tipo al que puede pertenecer cada una de ellas. Además, se le ha asignado a cada amenaza un código único que facilita el tipo al que pertenece, evitando redundancia entre distintas amenazas o entre distintos tipos de amenazas.

En la siguiente enumeración se pueden ver los distintos tipos de amenazas existentes y seguidamente las amenazas se clasifican siguiendo el esquema detallado a continuación:

- Errores generales.
- Ataques no intencionados.
- Ataques físicos no intencionados.
- Ataques intencionados.
- Amenazas físicas no intencionadas.
- Amenazas físicas intencionadas.

Errores generales

Código	Descripción
ERG01	Error de configuración
ERG02	Error de software
ERG03	Error de seguridad
ERG04	Error en las actualizaciones
ERG05	Error en la red interna
ERG06	Error general en la red
ERG07	
ERG08	
ERG09	
ERG10	

Ataques no intencionados

Código	Descripción
ATN01	Eliminación o pérdida de información
ATN02	Modificación de información
ATN03	Difusión pública de información
ATN04	Difusión o pérdida de credenciales
ATN05	Bloqueo o cierre de sesión no efectuado
ATN06	Acceso externo no autorizado
ATN07	
ATN08	
ATN09	
ATN10	

Ataques físicos no intencionados

Código	Descripción
AMN01	Volcado de líquidos sobre el equipo
AMN02	Tropiezos por la situación de los aparatos y cables
AMN03	Mantenimiento del edificio: pintura, limpieza, etc.
AMN04	Caídas o vuelques durante el transporte
AMN05	
AMN06	
AMN07	
AMN08	
AMN09	
AMN10	

Ataques intencionados

Código	Descripción
ATI01	Robo
ATI02	Intercepción de datos por medios físicos
ATI03	Sabotaje
ATI04	Vandalismo
ATI05	
ATI06	
ATI07	
ATI08	
ATI09	
ATI10	

Amenazas físicas no intencionadas

Código	Descripción
AFN01	Incendio
AFN02	Inundación
AFN03	Inestabilidad
AFN04	Derrumbe
AFN05	Terremoto
AFN06	
AFN07	
AFN08	
AFN09	
AFN10	

Amenazas físicas intencionadas

Código	Descripción
AFI01	Incendio
AFI02	Inundación
AFI03	Avería física
AFI04	Destrucción física
AFI05	Corte del servicio eléctrico
AFI06	Corte del servicio telefónico
AFI07	Corte del proveedor de servicios de red
AFI08	Ataque terrorista
AFI09	
AFI10	

2.2.2. Personal autorizado en los ficheros

En la siguiente tabla se clasifica para cada fichero de la empresa, qué tipo de personal está autorizado para la lectura, realización o modificación de dichos ficheros:

Nombre / Personal autorizado	Básico	Agregado	Privilegiado
Fichero de personal			
Fichero de proveedores			
Fichero de clientes			
Fichero financiero			
Fichero de producción			
Fichero de informes			

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 especifican las diferentes medidas de seguridad física a tomar para los distintos elementos de la empresa que deben protegerse.

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

En este apartado se recogen las medidas de seguridad que hemos decididos para los diversos edificios,

El protocolo de seguridad en edificios de oficinas seguido trata de evitar:

- Riesgos de incendios. - Riesgos de robos. - Riesgos de inundación.

Para conseguir estos objetivos, se ha creado un programa de seguridad integral. A continuación exponemos todos los sistemas y servicios que se han tenido en cuenta para elaborar dicho programa:

En cuanto a riesgos de incendios se refiere se han tomados las siguientes medidas de prevención:

- Detectores de humo.
- Extintores: repartidos por los diversos edificios, se colocarán en sitios visibles y de fácil acceso. Según Norma, se instalará un extintor cada 125 m². Llevarán incorporado un soporte para su fijación y se debe encontrar como máximo a una altura de 170 cm. del suelo. Se indicará en una placa: tipo y capacidad de carga, vida útil y tiempo de descarga.
- Salidas de emergencia: Colocadas en cada uno de los edificios que forman el recinto.
- Señalización: Se han colocado carteles en los sitios donde se encuentran ubicación los equipos de control de incendios, como los extintores, y de primeros auxilios, además de las salidas de emergencia.

Normativas

Todos los aparatos, equipos, sistemas y componentes de las instalaciones de protección contra incendios, cumplirán lo preceptuado en el Reglamento de Instalaciones de Protección contra Incendios, aprobado por Real Decreto 1942/1993

3.2.1. Normativa de Seguridad contra incendios

La normativa de seguridad contra incendios se rige según: - IEC 332-3 sobre propagación de incendios. - IEC 754-2 sobre emisión de gases tóxicos. - IEC 1034-2 sobre emisión de humo.

3.2.2. Normativa de Compatibilidad Electromagnética

La normativa de seguridad contra incendios se rige según: - UNE-EN50081 - UNE 20-726-91 (CEN/CENELEC EN55022) - UNE-EN50082-1 - CEN/CENELEC EN55024

3.2.3. Normativa Eléctrica

Todos los materiales y procedimientos de diseño e instalación relacionados con la parte eléctrica de los proyectos debe cumplir el Reglamento Electrotécnico de Baja Tensión (RBT) e Instrucciones Técnicas Complementarias del Ministerio de Industria y Energía (MIE).

En cuanto a riesgos de robos se refiere se han tomados las siguientes medidas de prevención:

- Instalación de alarmas de seguridad. - Cajas fuertes. - Instalación de cámaras de Vigilancia. - Vigilantes de Seguridad para controlar el acceso al recinto.

En cuanto a riesgos de inundación se refiere se han tomados las siguientes medidas de prevención:

- Detectores de inundación: colocados en los edificios donde se encuentran los ordenadores, tanto en la parte administrativa como en el departamento informático. Además dichos ordenadores nunca estarán colocados a nivel del suelo previniendo así que estos se puedan dañar si entrara agua.

3.3. Seguridad dentro del almacén

Se ha dejado un pasillo peatonal de unos 80 cm, entre los materiales almacenados y los muros del almacén, lo que facilita realizar inspecciones, prevención de incendios y defensa del muro contra los derrumbes. Los pasillos interiores longitudinales y transversales tendran dimensiones más amplias para el correcto manejo de los equipos utilizados. Calcular las estanterías del almacén deberán de tener una capacidad y resistencia adecuada para sostener los materiales por almacenar, en nuestro caso las botellas de vino, también se ha teniendo en cuenta que la altura más apropiada para el posterior trabajo con los equipo de manipulación.

3.4. Seguridad del centro de datos

3.4.1. Seguridad de acceso

Los servidores de la empresa se encuentran en el CPD, que ocupa una habitación dentro del departamento informático. Su entrada está protegida mediante un dispositivo

de autenticación de usuarios. Como la empresa cuenta con un control de picadas, cada trabajador tendrá a su disposición una tarjeta que lo identifica, de manera que según el perfil del empleado tendrá acceso o no a ciertas áreas de la empresa. En el caso del CPD sólo tendrán acceso los informáticos encargados de dicha tarea.

3.4.2. Seguridad interna

La entrada a nuestro centro de datos consta de una puerta ignífuga para evitar riesgos en caso de incendio. También posee un extintor que sigue las normas mencionadas en el apartado 3.2. Esta sala cuenta con falsos suelos y techos por donde irá todo el cableado.

3.5. Seguridad del lugar de trabajo

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

Habrà 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 útil 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.

Habría 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.