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

10 de noviembre de 2010

Índice general

Índice de figuras

Índice de cuadros

Historial de Cambios

Fecha	***Cambios***
10 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 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

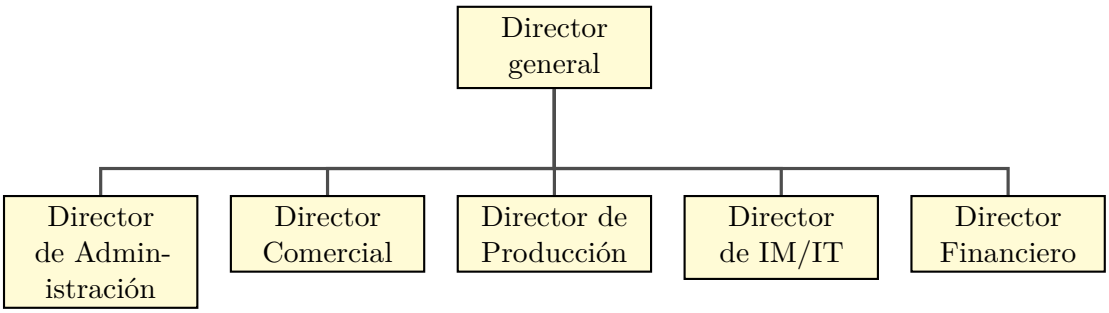
Los Directorados

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*.

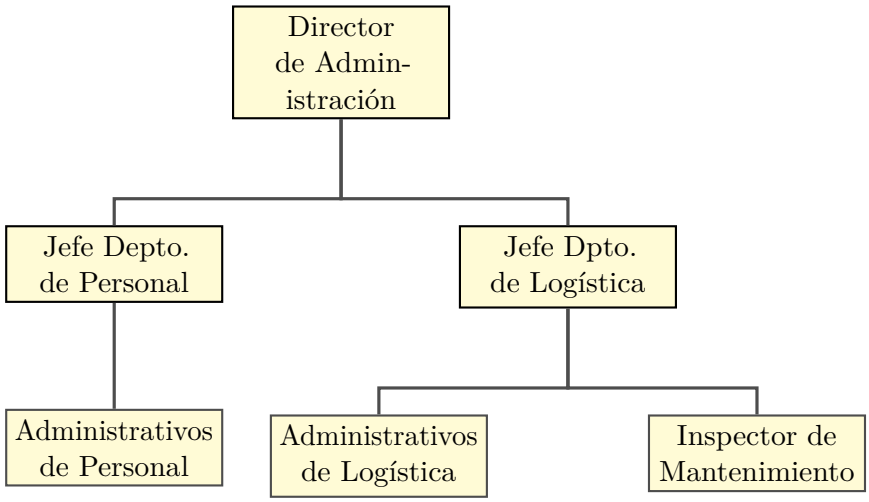
El *departamento de personal* tiene un jefe y varios administrativos, que se encargan de las siguientes funciones:

- 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.

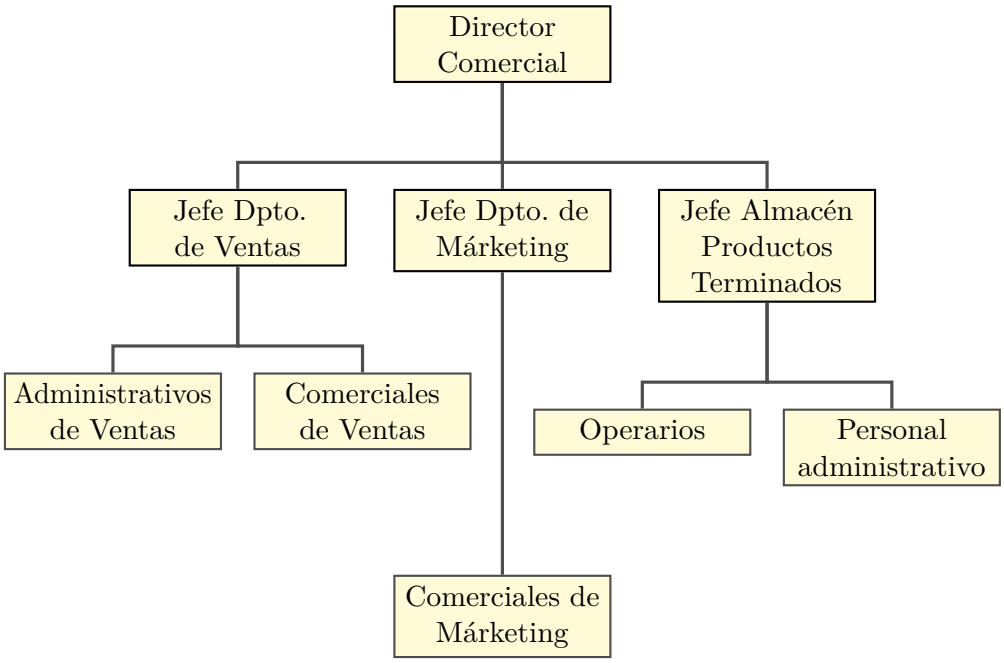


Dirección Comercial

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.

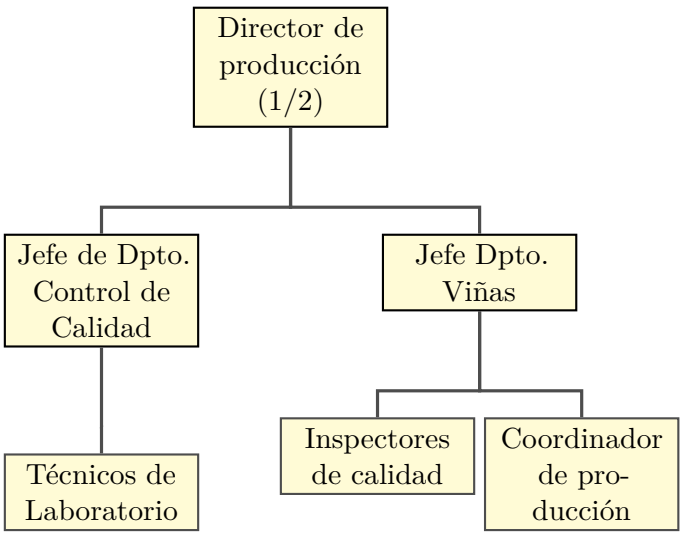
- El **Departamento de Control de Calidad** se encarga de la realización de las pruebas y cálculos pertinentes para asegurarse de que los productos terminados e intermedios que se están fabricando se realizan según los procedimientos estipulados, de que sus propiedades cumplen los niveles de calidad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

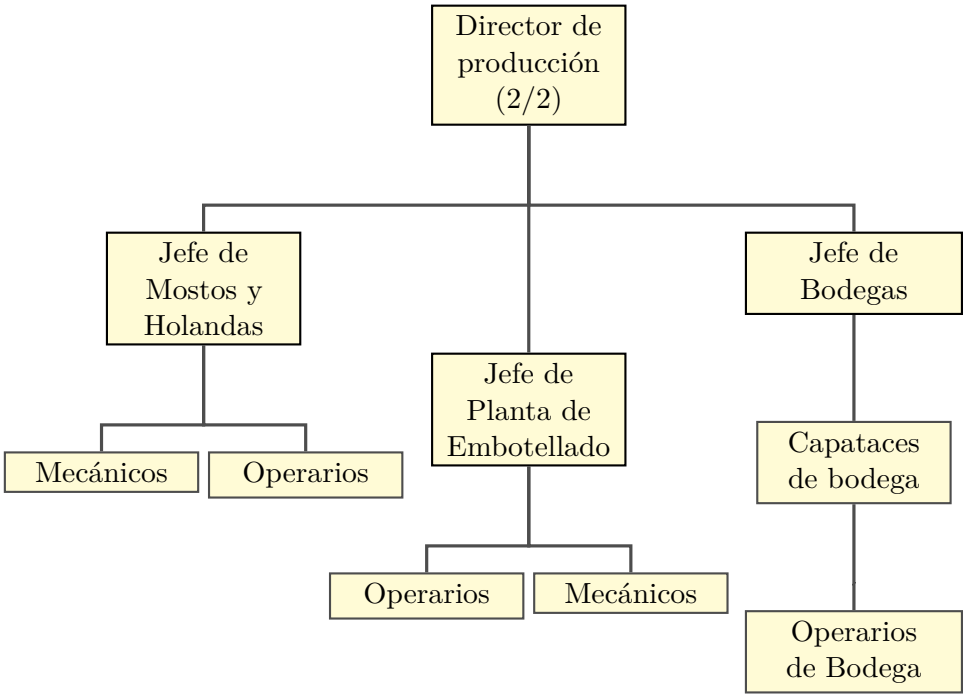
- El **Departamento de Viñas** se encarga de la relación con las fincas productoras de uva que pretenden vender o ya han vendido su producción a la bodega. Estas viñas autorizan a los *inspectores de calidad* de viñas a realizar visitas periódicas a las viñas para asegurarse que la producción contratada 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.





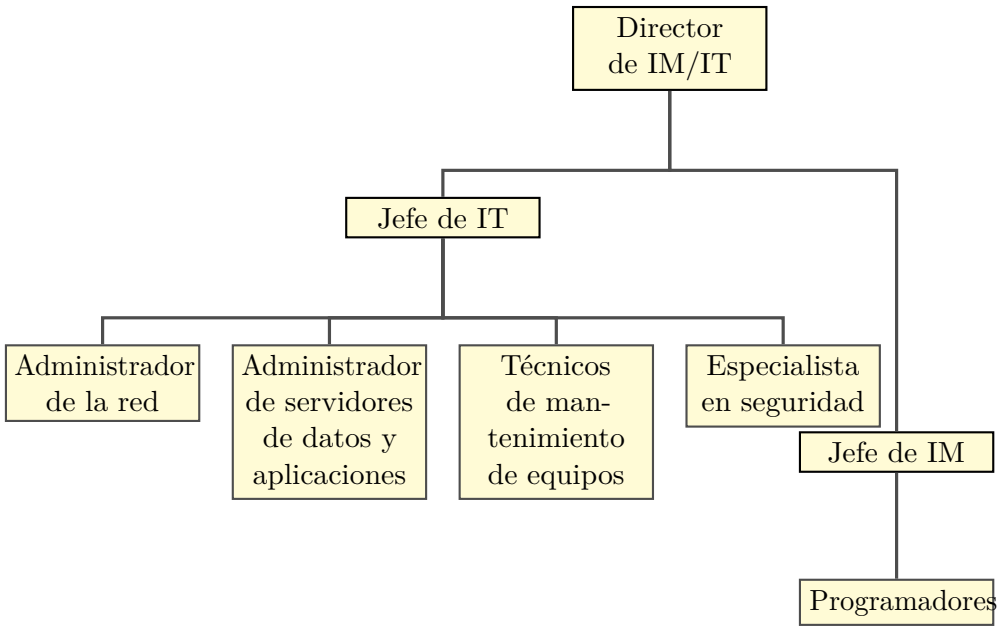
Dirección de IM/IT

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:

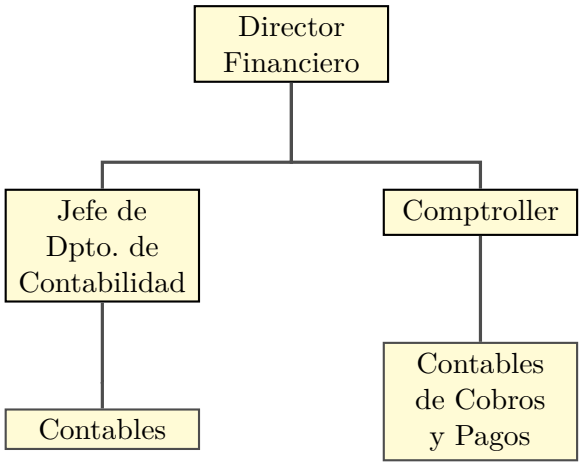
- Mantener fielmente y actualizada la información relativa al estado financiero de la empresa.
- Realizar las operaciones necesarias para el cumplimento de las normas en relación con las Haciendas locales y estatales.
- Realizar análisis de costes y beneficios que ayuden al resto de los Directores a 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 27), del software y hardware (capítulo 5 on page 25) 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	Interceptación 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	Inestanqueidad
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,ademñas de las salidas de emergencia.

3.3. 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.

3.3.1. Normativa de Seguridad contra incendios

La normativa de seguridad contra incencios 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.

3.3.2. Normativa de Compativilidad Electromagnética

La normativa de seguridad contra incencios se rige según:

- UNE-EN50081
- UNE 20-726-91 (CEN/CENELEC EN55022)
- UNE-EN50082-1
- CEN/CENELEC EN55024

3.3.3. 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.

3.4. Energía del edificio

Se dispone de un sistema de alimentación ininterrumpida tanto para las estaciones de trabajo del personal, como para los equipos de telefonía y soporte de red del edificio. Lo que se pretende con esta medida es asegurarnos la continuidad en el desarrollo de las actividades del personal mientras se soluciona el problema. Con este sistema podremos asegurar continuidad en el desarrollo de las actividades del personal durante el tiempo que se tome para restablecer el fluido eléctrico. Estos sistemas de alimentación ininterrumpida serán revisados periódicamente por parte del personal de mantenimiento.

3.5. 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.

3.6. Seguridad del centro de datos

El Centro de Proceso de Datos se encuentra en un edificio junto con el departamento de informática cuyo personal lo gestiona. Las medidas de seguridad aplicada al edificio de este edificio serán las mismas que hemos mencionado en aparatados anteriores, aunque por su especial relevancia y características, se aplicarán medidas adicionales.

Entre las medidas adicionales se encuentran:

- El acceso a las dependencias de equipos sólo nestará permitido al personal directamente implicado mediante tarjeta de identificación personal.
- El acceso a los equipos almacenados en los racks estará protegido mediante cerradura custodiada por el responsable de la sala.
- El almacenamiento del soporte lógico será mediante armario ignífugos preferiblemente en otra sala distinta del local de equipos.

3.6.1. 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 autentificación 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.

3.6.2. Seguridad interna

La entrada a nuestro centro de datos consta de una puerta ignifuga 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.

3.7. Seguridad del lugar de trabajo

Como medidas de seguridad dentro del lugar de trabajo tomaremos las mismas especificadas en el apartado de la seguridad del edificio. Además tendremos en cuenta las siguientes medidas dentro de este entorno.

- Está prohibido el acceso al lugar de trabajo con envases que contengan líquidos.
- Los equipos informáticos estarán protegidos mediante una contraseña que será asiganada por el departamento de sistemas así como la entrada a la BIOS del equipo.
- Dependiendo del área en el que se encuentra el personal tendrán o no acceso a ciertas carpetas que contienen la información de los diferentes departamentos, para ello tendrán asiganados diferentes perfiles con diferentes permisos establecidos por el de partamento de sistemas.
- Los equipos informáticos del personal no dispondrán de grabadoras y tendrán los puertos usb deshabilitados, esto se toma como medida de seguridad para que no pueden extraer información del sistema.Si se da el caso de alguna excepción serán los del departamento de informática los encargados de darle ese permiso momentáneo.
- El personal debe estar al corriente de las normas de utilización de sus puestos de trabajo.
- Queda prohibida la utilización de equipos ajenos a la institución.
- El acceso al interior de los equipos estará protegido mediante un precinto de seguridad.

4. Política de control del personal

4.1. Indicaciones a eliminar

En el presente apartado de la guía, se establecerán aquellas medidas que inciden de forma esencial sobre el personal a:

- El uso que hacen de los sistemas de información.
- El manejo de incidencias de seguridad.
- Las normas de seguridad a aplicar.

Por tanto, se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores.

Todas las funciones y responsabilidades deben comunicarse a los usuarios involucrados en su ejecución, de una forma clara y asegurando su recepción y entendimiento. Se prestará especial atención al tratamiento de datos de carácter personal.

4.2. Objetivos

El objetivo de la política de control de personal es reducir los riesgos de errores humanos, robos, fraude, o mal uso de las instalaciones y servicios, relativos a los sistemas de información de la compañía.

Una de las principales amenazas de toda organización es el acceso de usuarios no autorizados (internos o externos) que puedan consultar, modificar, borrar e incluso robar información a la que no deberían acceder.

4.3. Ámbito de aplicación

La política de control del personal es de aplicación a todos los empleados o personal de contrata externa, que puedan llegar a manejar activos de Bodegas San Dionisio, S.A.que incluyan información incluida en el ámbito de aplicación de la política de seguridad de Bodegas San Dionisio, S.A..

4.4. Declaración de la política de control del personal

La protección de los activos ha de producirse en el proceso de reclutamiento del personal, ha de incluirse en el Reglamento de Régimen Interno (RRI) de Bodegas San Dionisio, S.A., han de incluirse en las descripciónes de puestos de trabajo, y ha comprobarse su cumplimiento durante el tiempo de contratación del empleado.

Para asegurar el cumplimiento de los objetivos de esta política, se han de seguirse los siguientes procedimientos e instrucciones en su ámbito de aplicación, detallados en las siguientes secciones.

4.5. Proceso de contratación

4.5.1. Extensible a todo el personal

1. Se valorará la presentación de referencias sobre actitudes del candidato de organizaciones en las que el candidato haya estado prestando servicios previamente, y así se hará saber en los anuncios de ofertas de empleo que publique la empresa. Asímismo se ralizará la comprobación de la autenticidad de las referencias presentadas si el candidato resulta preseleccionado para el puesto.
2. El departamento de personal comprobará la completitud y precisión del Curriculum Vitae del candidato.
3. El departamento de personal confirmará la autenticidad de las certificaciones académicas y personales presentadas por el candidato.
4. Se exigirá el certificado de antecendentes penales a los candidatos.
5. Cualquier persona dentro del ámbito de aplicación de esta norma deberá firmar el acuerdo de confidencialidad del anexo (capítulo B on page 35)
6. En caso de contrataciones a través de ETT´s se asegurará que Bodegas San Dionisio, S.A. tiene acceso a la documentación para la selección aportada por el candidato seleccionado por la ETT, y se incluirá en el contrato con la ETT, que Bodegas San Dionisio, S.A. se reserva el derecho comprobar por su cuenta la exactitud de la documentación aportada.

4.5.2. Extensible al personal con acceso a datos clasificados

1. Además de aplicarse las salvaguardas aplicables al todo el personal,
2. El director tendrá que ser notificado de la contratación, o futura contratación de personal con acceso a datos sensibles dentro de su directorado. El Director se asegurará de que el nuevo empleado es supervisado convenientemente en lo relativo su uso prudente y las precauciones a tomar en el uso de dichos datos. [E.7]
3. El candidato seleccionado firmará un acuerdo de confidencialidad.

4.5.3. Extensible al personal con acceso a datos altamente sensibles

1. Se realizará una investigación sobre el estado financiero del candidato preseleccionado, siempre dentro de los márgenes estipulados por la ley.

4.6. Proceso de despido

1. El Jefe de IT se asegurará de establecer los procedimientos internos para mantener una lista de todas las credenciales para el acceso a sistemas de información otorgadas a los empleados de Bodegas San Dionisio, S.A.

2. EL jefe de IT se asegurará de que existe un procedimiento bien documentado para efectuar la terminación del acceso para las credenciales de cualquier empleado, que dicho proceso puede ser efectuado por más de un miembro del departamento de IT, y que durante el horario regular laboral existe en la empresa algún trabajador capacitado para su realización.

3. Los Jefes de Departamento y Directores se asegurarán que el depido de un empleado se notifica **INMEDIATAMENTE** al Jefe de IT, que diligentemente y sin demora se asegurará de que se realiza el procedimiento citado en el punto 2.

4.7. Formación y concienciación del personal

Se ha establecido un plan de formación y concienciación del personal sobre la seguridad de la información, que está coordinado por el Director de IM/IT, y es ejecutado por el Jefe de IT.

El objetivo de dicho plan es concienciar y formar al personar en lo relativo, entre otros, a los siguientes temas:

- El uso de contraseñas y gestión - incluida la creación, la frecuencia de los cambios, y la protección.
- La protección contra virus, gusanos, troyanos y otros códigos maliciosos - exploración, la actualización de definiciones
- Consecuencias del incumplimiento de las normas de seguridad.
- Correo Electrónico / ficheros anexos desconocidos.
- Uso de la Web y del correo electrónico. Uos aceptables, usos prohibidos.
- La vigilancia de la actividad del usuario.
- Spam.
- Ingeniería social

- Respuesta de incidentes - ¿con quién contactar? ¿Qué hacer?
- La seguridad del ordenador portátil durante un viaje
- La aplicación de los parches de los sistemas sistema, y de los anti-vurus.
- Control de visitantes y el acceso físico a los espacios.
- Seguridad de escritorio. Protectores de pantalla, prevención del shoulder-surfing.

Dicho plan incluirá, entre otros, los siguientes vehículos de distribución de la información:

- Colocación de pósters en las paredes de las ofifinas y lugares de trabajo.
- Implementación de un «banner» de entrada a los sistemas donde se avisa resumidamente a los empleados de sus obligaciones y restricciones en lo relativo a los sistemas de información.
- Obligación del visionado de material audiovisual con el tratamiento de estos temas a todos los empleados.
- Boletín mensual recordatorio con aspectos puntuales de la seguridad de la información.

4.8. Medidas disciplinarias

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

4.9. 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

6.1. Seguridad Comunicaciones

6.1.1. Visión general

La seguridad en la red es uno de los aspectos más importantes dentro de la política de seguridad de una organización que se disponga de dispositivos conectados entre sí y más si se encuentran conectados a internet. Se establecerán medidas de seguridad para asegurar el acceso a la información desde el exterior de la entidad así como restringir los accesos mediante los medios de red por parte de los dispositivos conectados a la red de la empresa.

Se redactarán normas para asegurar el acceso desde el exterior estableciendo un nivel de seguridad perimetral, definición del protocolo escogido para la disposición del servidor web, medidas de seguridad ligadas a conexiones inalámbricas e implantación de VPN.

6.1.2. Objetivos

Esta política está diseñada para proteger los datos de la empresa. Permite asegurar que el acceso a los datos se realice siempre mediante los mecanismos de red establecidos, impidiendo el acceso de posibles intrusos que puedan realizar actividades que atenten contra la privacidad e integridad de los datos de la empresa.

6.1.3. Alcance

Esta política se aplica a todos los medios y dispositivos de red, y por tanto, a todos los empleados que los utilizan. De la misma forma, afectará a los usuarios que accedan de forma remota al las bases de datos.

6.1.4. Arquitectura

La empresa está dividida en tres edificios geográficamente separados entre sí. Estando estos edificios conectados por la red con topología de estrella y mallados a través de una conexión Macrolan de Telefónica como línea de backup. El edificio principal, edificio de oficinas, es el núcleo principal de la estrella, este conecta con los otros dos edificios, almacén/ventas y bodega a través de F.O. SM propietaria de la empresa.

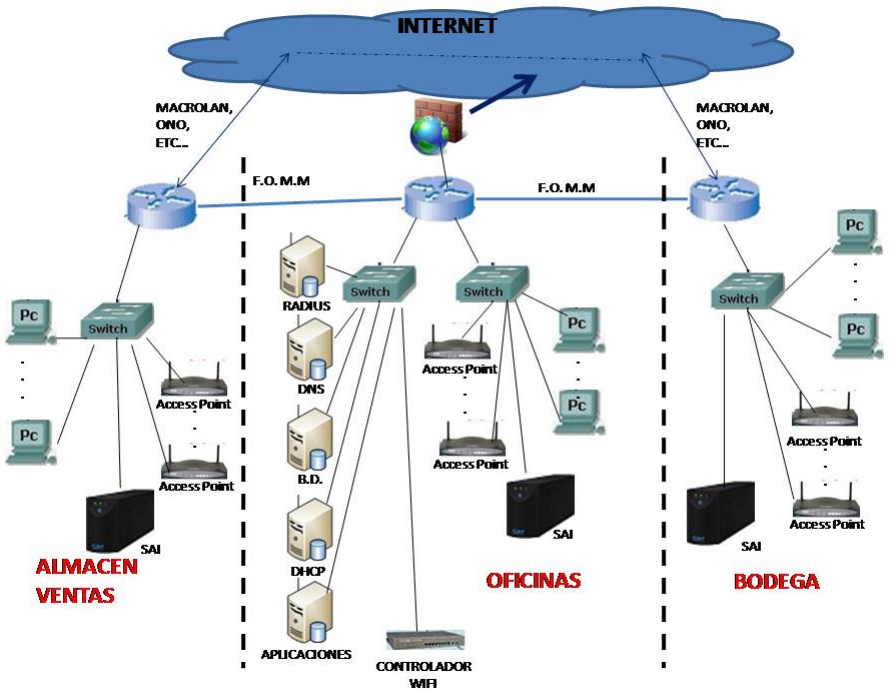


Figura 6.1.: Arquitectura de la red.

La seguridad perimetral se establecerá a través de un servidor proxy. Este será la única puerta de entrada/salida con el exterior.

En el interior, la red estará dividida en las siguientes subredes lógicas (vlan): gestión de red, gestión directivos, gestión administrativa, red de respaldo (macrolan), servicio (máquinas embotellado, etc...) y WIFI. El acceso de una vlan a otra estará restringido así como el acceso a los servidores.

La red WIFI estará cifrada mediante el protocolo WPA2, y los roles de acceso y direccionamiento de cada usuario estará definido en el servidor Radius.

La línea de respaldo, que une los edificios satélites (Almacen/Ventas y Bodega) sólo estará activa en caso de que se detecte que la línea principal este cortada. Los router de las distintas sedes usarán para tal fin el protocolo OSPF y solo estarán definidos el enlace primario y el de backup. A sí mismo, solo de definirán en lo router las vlan antes mencionadas.

El servidor Web de la empresa estará situado en la sede central y será propiedad de la misma. Este estará tras el firewall, dentro de la red interna.

Tanto los router como los switch estarán protegidos con contraseñas alfanuméricas y solo serán accesibles mediante SSH o consola. El conocimiento de estas contraseñas será exclusivo del personal que defina el responsable de la Unidad de Informática, máximo responsable de dicho conocimiento.

Las contraseñas serán modificadas una vez al mes, pudiéndose modificar con más frecuencia si el responsable de la Unidad de Informática lo estimara preciso. Este cambio quedará reflejado por escrito indicando la fecha, personal implicado y firma del responsable.

El cableado de red será estructurado, UTP CAT 5 ó superior. No se habilitará ninguna roseta sin cumplir con el protocolo establecido y solo se permitirá una conexión por toma de red, es decir, queda totalmente prohibido conectar hub, switch ó cualquier otro elemento que extienda la red sin consentimiento previo.

Ninguna roseta se cambiara de vlan sin el correspondiente visto bueno del responsable de la unidad, debiendo quedar reflejado por escrito en dicha solicitud la fecha, motivo y firma del responsable.

6.1.5. Habilitación de rosetas

Para la habilitación de una roseta es obligatorio informe del responsable de la unidad indicando el propósito de uso, fecha y firma.

Si una roseta quedara sin uso es responsabilidad del responsable de la unidad el informar al departamento de comunicaciones la desabilitación de dicha roseta. Esto se realizará por escrito indicando la fecha, motivo y firma del responsable.

6.1.6. Conexiones desde el exterior

Todas conexión que se haga desde el exterior de la empresa a cualquier servidor se realizarán mediante VPN (red privada virtual), para los que se usarán los certificados clase 1 emitidos por la empresa

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. Acuerdo de Confidencialidad

Cláusulas adicionales de la comunicación de contrato de duración determinada a tiempo completo por obra o servicio determinado celebrado el día de de entre las partes D. con NIF y D. con DNI como administrador solidario de la empresa Bodegas San Dionisio, S.A., con CIF .

1. Diligencia y Buena Fe.

«El empleado llevará a cabo los servicios correspondientes a la naturaleza de su cargo y funciones con la debida diligencia y conforme a los principios de buena fe, discreción y sujeto en todos los casos, a la Política sobre Confidencialidad establecida por la Empresa, la cual se recoge a modo de Anexo del presente contrato».

«El empleado se compromete igualmente en el momento de la resolución del contrato, cualquiera que sea la causa a entregar a la Empresa inmediatamente todos aquellos elementos o medios que la misma le hubiere proporcionado para el desempeño de su función, sirviendo a título ejemplificativo pero no limitativo la siguiente enumeración: los documentos (incluyendo las copias), cintas de todo tipo, software del ordenador, información y registros, llaves, tarjetas de identidad, tarjetas de crédito, libros y cualesquiera otros elementos propiedad o relativos a la Empresa o de empresas asociadas. Incluyéndose sin limitación, todos los elementos elaborados por el Empleado o que puedan haber llegado a su poder en el curso o como consecuencia de su empleo y que se encuentren en su posesión, poder, custodia o control».

2. Baja Voluntaria.

«El trabajador que desee resolver voluntariamente su contrato de trabajo deberá ponerlo en conocimiento de la Dirección de la misma, cumpliendo con un plazo de preaviso de quince días.
En el supuesto de incumplimiento del plazo previsto, la Empresa podrá proceder al descuento del salario correspondiente al período de preaviso incumplido».

3. Pacto de confidencialidad y Protección de Datos.

Tanto en el desarrollo de la prestación de servicios, como una vez extinguida la misma por cualquier causa, el Empleado deberá mantener estricta confidencialidad y no divulgará, utilizará, expondrá ni publicará Información Confidencial recibida en virtud

del desempeño de su relación laboral con la Empresa como consecuencia e la misma, ya sea referida a la Empresa, otras compañías, clientes o relacionado con la Empresa, salvo que tal divulgación, utilización o publicación le sea requerida por la Empresa debida a motivos de trabajo, o salvo que un directivo de la Empresa expresamente autorice al Empleado por escrito.

El término «Información Confidencial», a los fines del presente contrato, comprenderá toda información obtenida de la Empresa, o de los proveedores de ésta, por el Empleado, incluyendo, pero no limitando, a los secretos industriales y comerciales, métodos financieros, sistemas de información confidencial, planes de comercialización asociados con los productos, directos o indirectos de la Empresa, listados de clientes, detalle de clientes de la Empresa (sus requerimientos, posición financiera, los términos del negocio o de cualquier transacción con ellas) y cualquier información con respecto a la cual se manifieste al Empleado que es confidencial.

Es responsabilidad del Empleado mantener esta información fuera del alcance del resto del personal.

Asimismo, y en consideración a que la Empresa recibe y recibirá en el futuro información confidencial o privativa de tercera partes («Información de Terceras Partes») y que tal información se sujetará a la obligación por parte de la Empresa de mantener su confidencialidad y de usarla únicamente para determinados fines, el Empleado deberá mantener tal información en la más estricta confidencialidad y no revelará a ninguna otra persona distinta de los empleados de la Empresa que necesiten conocer tal información para su trabajo dentro de la misma, ni tampoco utilizará la misma, salvo en relación con su trabajo para la Empresa, a no ser que esté expresamente autorizado por escrito por un directivo de la Empresa. Esta obligación se mantendrá incluso después de extinguirse el presente contrato por cualquier causa.

En el supuesto que se solicite o requiera al Empleado revelar información confidencial en virtud de alguna orden judicial, el Empleado deberá notificar tal situación de forma inmediata a la Empresa. El Empleado adoptará todas las medidas solicitadas por la Empresa a fin de defender dicha revelación coercitiva, permitiendo a la Empresa a que le asista legalmente en cualquier procedimiento relativo a dicha revelación coercitiva.

El empleado tomará todas las medidas necesarias a fin de minimizar el riesgo de la divulgación de un secreto o de información confidencial, así como para el almacenamiento adecuado y seguro de dicha información. Asimismo, el Empleado se compromete a mantener y guardar registros adecuados (en la forma de anotaciones, dibujos, bosquejos y de cualesquiera otras que puedan ser requeridas por la Empresa) de toda la Información Confidencial durante el tiempo de su prestación de servicios para la Empresa, que deberán estar disponibles y permanecerán siempre en la sola y única propiedad de la Empresa.

El Empleado no utilizará para sus propios fines que no fueran aquellos de la Empresa cualquier secreto comercial o información confidencial relacionada con la Empresa, de manera tal que sólo podrá utilizar la información confidencial en el ámbito de la relación laboral y en beneficio de la Empresa.

El Empleado no utilizará para sus propios fines que no fueran aquellos de la Empresa cualquier secreto comercial o información confidencial relacionada con la Empresa, de manera tal que sólo podrá utilizar la información confidencial en el ámbito de la relación laboral y en beneficio de la Empresa.

Con independencia de que hayan sido o no clasificados como Información Confidencial, todos los memorándums, notas, listas, medios electrónicos o magnéticos, microfilms, películas, archivos, listado de clientes, proveedores y empleados, correspondencia, documentos, ordenadores y otros discos y cintas, listado de datos, códigos, diseños y dibujos, así como cualquier otro tipo de documento o materia de cualquier naturaleza (y todas las copias de los mismos) realizados o compilados por el Empleado durante la vigencia de su relación laboral la Empresa a los que haya tenido acceso, serán propiedad exclusiva de la Empresa y serán entregados a la Empresa dentro de los diez días siguientes a la finalización de la relación laboral, cualesquiera que sea la causa que produzca la misma o en cualquier otro momento en que la Empresa así lo solicite.

El empleado además se abstendrá de usarlos y revelarlos sin causa justificada sin consentimiento expreso de la Empresa.

Asimismo, por la presente, el Empleado cede a la Empresa cualesquiera derechos que haya podido o que adquiera de la Información Confidencial, reconociendo a la Empresa (o sus cesionarios) como únicos titulares de tales derechos. Junto a lo anterior, conviene que la empresa y sus cesionarios serán los únicos propietarios de cualesquiera secretos industriales, derechos de propiedad intelectual e industrial, Copyright y cualesquiera otros derechos en el mundo entero.

En , a de de .

El trabajdor La Empresa

C. 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

Hola

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.