Universidad de Cádiz
Seguridad y Competencias Profesionales
Curso 2010/2011

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

18 de enero de 2011

Índice general

Índice de figuras

Índice de cuadros

Historial de Cambios

Fecha	***Cambios***
18 de enero de 2011	Primera versión del documento.

Compromiso de la dirección

La dirección de Bodegas San Dionisio, S.A. se compromete a proveer de los recursos necesarios para la ejecución de la presente Política de Seguridad y concienciar a todo el personal de la empresa de la importancia del cumplimiento de los procedimientos definidos en el documento.

Firmado:

El Director General

En Jerez de la Frontera, a 16 de diciembre de 2010

1. Introducción

1.1. Descripción de la Organización

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*, establecidos en el Anexo II de la consejería de Agricultura y pesca del 13 de mayo de 2010 [1].

1.1.1. Estructura organizativa de la compañía

Las Direcciones

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

Las direcciones son los siguientes, como se puede ver en la figura 1.1:

- Dirección de Administración.
- Dirección Comercial.
- Dirección de Producción.
- Dirección de GI/TI (Gestión de la Información y Tecnologías de la información).
- Dirección Financiera.

Las funciones de las direcciones 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. La figura 1.2 muestra el organigrama.

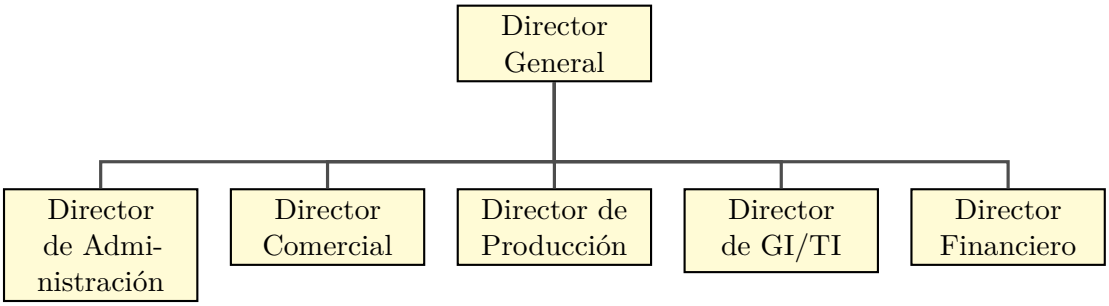

Figura 1.1.: Organigrama de Direcciones de la Empresa

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[1] 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.La figura 1.2 muestra el organigrama.

[1]La figura del comptroller se ilustra más adelante, al explicar las funciones de los miembros de la Dirección Financiera

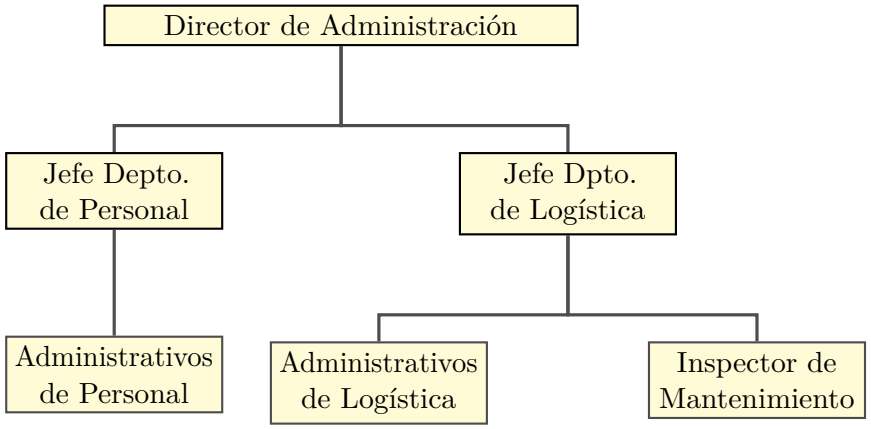

Figura 1.2.: Organigrama de la Dirección de Administración

- 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

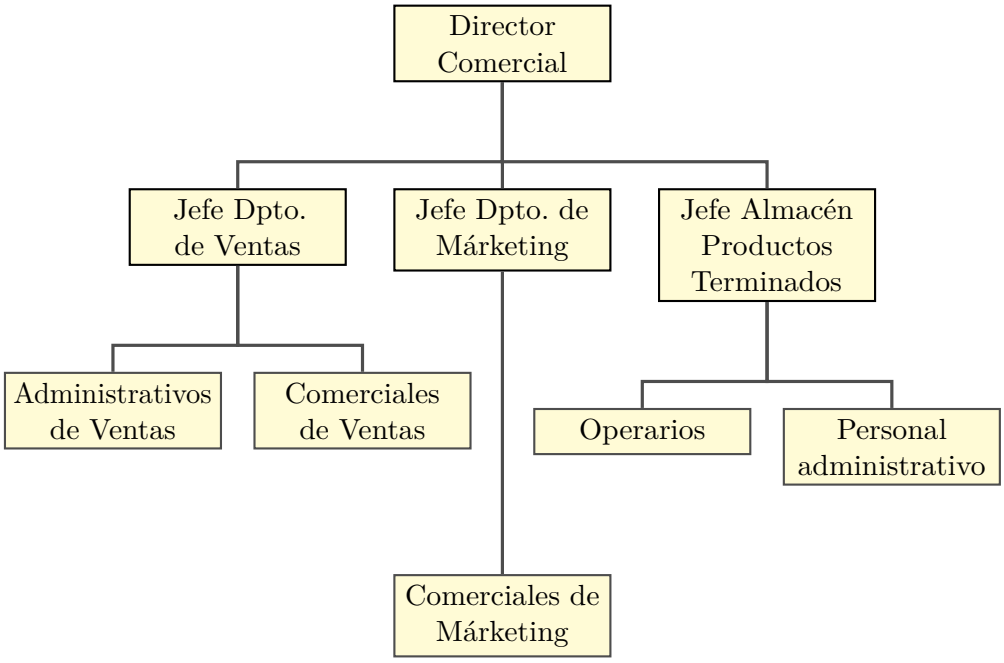

Figura 1.3.: Organigrama de la Dirección Comercial

cumpliendo con la normativa vigente de salud pública y protección al consumidor. Puede ver el organigrama en las figuras 1.4 y 1.5.

Esta dirección 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

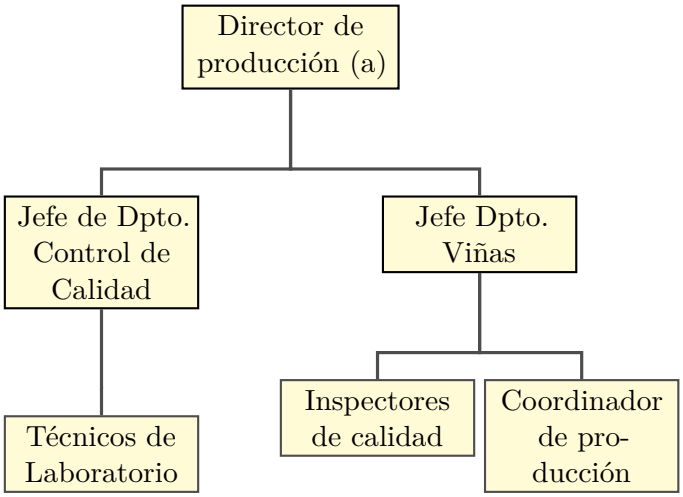

Figura 1.4.: Organigrama de la Dirección de Producción (a)

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 GI/TI

Esta compañía le da mucha importancia estratégica al flujo de datos e información de la empresa, y ha decidido que el área de GI/TI va a tener una dirección. La figura 1.6 muestra su organigrama.

Esta dirección consta de dos depatamentos: TI (Tecnología de la Información) e GI (Gestión de la Información).

- El departamento de TI 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.

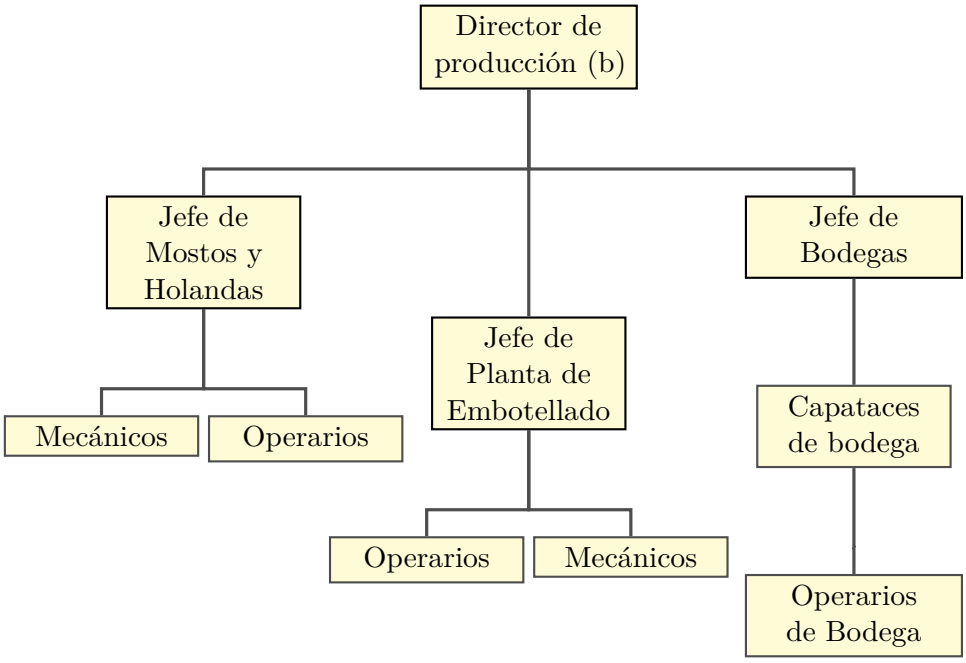

Figura 1.5.: Organigrama de la Dirección de Producción (b)

- 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 GI está compuesto por un Jefe de GI, 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»[2] que representan dichas métricas.

[2]Dashboard: Conjunto de indicadores gráficos que muestran el estado, normalmente actualizado, de los valores calculados para las métricas que la Dirección determina que van a servir como indicadores del buen o mal funcionamiento de una organización. Normalmente el contenido y procedimimento de recolección de datos y valoración de estas métricas se revisan anualmente, y un departamento relacionado con la gestión de información se encarga de que esta expresión gráfica se muestre lo

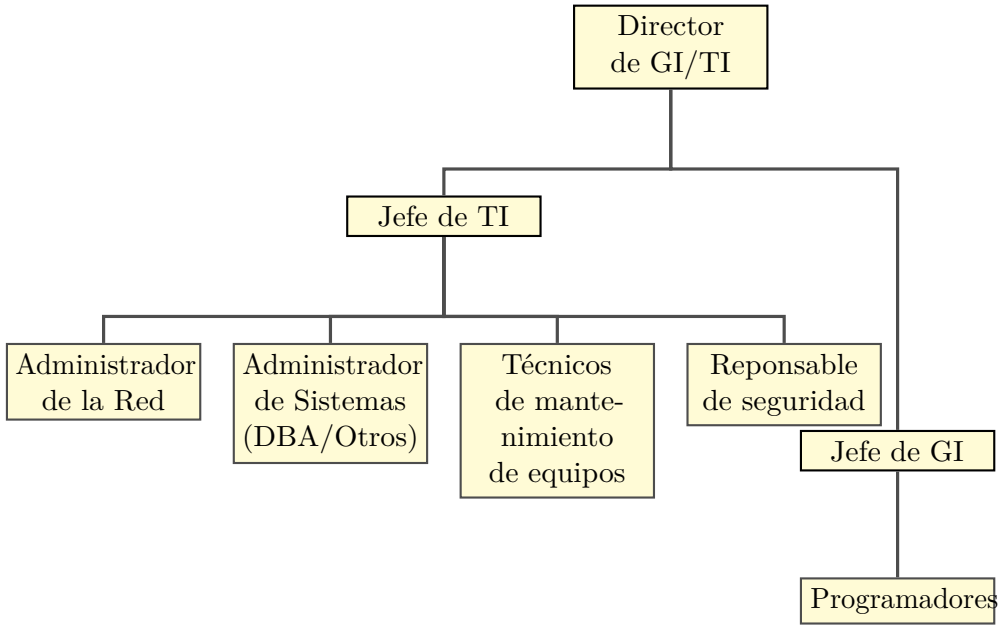

Figura 1.6.: Organigrama de la Dirección de GI/TI

- 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.

más actualizada y fiel a le realidad como sea posible. La palabra «dashboard» viene del inglés, y su traducción es «cuadro de mandos». Es una analogía con el cuadro de mandos de un vehículo, que normalmente presenta una serie de indicadores que le dan una idea al conductor del estado del mismo. Por ejemplo, el nivel de aceite, la temperatura, los testigos de luces, etc., se pueden corresponder con espresiones gráficas en un «dashboard» empresarial como «Productividad de la planta X», o «Riesgo actualizado en cash-flow», etc.

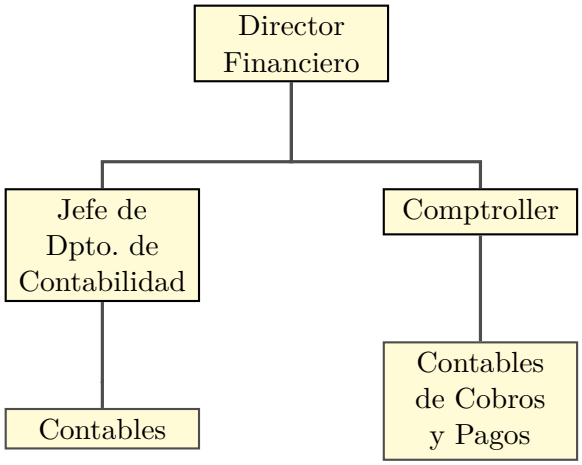

Figura 1.7.: Organigrama de la Dirección Financiera

- 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, la dirección se divide en dos departamentos: uno de **contabilidad**, y otro de **Comptroller**, como se puede observar en la figura 1.7

- 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

El objetivo principal de esta política de seguridad es definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran referidas a la seguridad de los sistemas informáticos. Esta política describe una serie de procedimientos de seguridad que describen cuáles son las actividades que habrían de realizarse en el sistema, en qué momento o lugar, quiénes son los responsables de su ejecución y cuáles son los controles aplicables para supervisar su correcta aplicación.

La política establecida es de obligado cumplimiento para todos los estamentos de la organización: Dirección General, Dirección Administrativa, Dirección de Producción, Dirección Financiera, Dirección Comercial y Dirección de GI/TI.

La política comprende los siguientes aspectos:

- Seguridad de la información tratada por la organización, ya sea de carácter personal o relativa a los proyectos desarrollados en la organización.
- Seguridad de equipos y elementos físicos.
- Control de personal interno y subcontratado.
- Seguridad del Hardware y Software.
- Seguridad en las comunicaciones.
- Continuidad del Negocio.

1.3. Gestión y cambios de la política

La política de seguridad se revisa anualmente en una reunión del Comité de Dirección Ejecutiva junto con el Responsable de Seguridad de la empresa. Estas revisiones tienen como objetivo adaptar la política a las nuevas exigencias de la organización y del entorno tecnológico y legal. Los cambios en la política sólo pueden ser propuestos por alguno de los miembros del comité y/o del responsable de seguridad, y su aprobación se realizará por mayoría de tres quintos en la fecha anual prevista para su revisión. Se utilizará para la realización de solicitud de modificación la plantilla del anexo C on page 69)

Cuando los cambios realizados en la política derivan en cambios procedimentales en la organización, la Dirección de Bodegas San Dionisio, S.A. deberá informar a los departamentos afectados en un plazo inferior a una semana. En caso necesario, se realizarán cursos de formación dentro del horario laboral y se elaborará documentación informativa para los miembros del personal. Cuando los cambios afectan a todos los miembros de la empresa, además de los procedimientos anteriores, se publicará una noticia en la página web de la intranet corporativa, se enviará un correo electrónico a la cuenta de todos los empleados que la posean, y se publicará en los tablones informativos de todos los edificios de la compañía.

1.4. Organización de la Seguridad

Bodegas San Dionisio, S.A. se divide en 6 áreas principales (ver figura 1.1):

- **Dirección**. Esta área se compone únicamente del Director de la empresa. El Director tiene acceso a toda la información de la empresa además de a todos los sistemas informáticos. El responsable de Seguridad de la Empresa ha de asegurarse de que en cualquier momento, el Director puede ejercer esta potestad.

- **Dirección de Administración**. Para poder efectuar sus funciones, el Director de Administración tiene acceso privilegiado al archivo de personal y de proveedores, y acceso de lectura a los archivos pertinentes del cuadro de mandos (Dashboard) del fichero de informes de la empresa.

- **Dirección Comercial**. Para poder efectuar sus funciones, el Director Comercial tiene acceso privilegiado al archivo de proveedores y de clientes, y acceso de lectura a los archivos pertinentes del cuadro de mandos (Dashboard) y la estructura de informes de dirección del fichero de informes de la empresa.

- **Dirección de producción**. Para poder efectuar sus funciones, el Director Comercial tiene acceso privilegiado al archivo de producción, y acceso de lectura a los archivos pertinentes del cuadro de mandos (Dashboard) y la estructura de informes de dirección del fichero de informes de la empresa.

- **Dirección de GI/TI**. Al igual que el Director General, el Director de GI/TI tiene acceso a todos los sistemas informáticos. El responsable de seguridad la información de la Empresa ha de asegurarse de que en cualquier momento, el Director de GI/TI pueda ejercer esta potestad. Con respecto a la información, únicamente no tendrá acceso a aquella que esté clasificada como confidencial por el Director General.

- **Dirección financiera**. Para poder efectuar sus funciones, el Director Financiero tiene acceso agregado al archivo de producción, de proveedores y de clientes. También tiene acceso privilegiado al archivo financiero, y acceso de lectura a los archivos pertinentes del cuadro de mandos (Dashboard) y la estructura de informes de dirección del fichero de informes de la empresa.

Los directores son responsables de coordinar con el responsables de seguridad de la información y el administrador de sistemas, los privilegios de los que va a disfrutar cada miembro de la organización, dependiendo de qué funciones realicen en cada momento dentro de la compañía, y siguiendo siempre el principio del menor nivel de acceso necesario para el desempeño de su trabajo, tomando como guía lo estipulado en el apartado 2.1.1 Personal autorizado en los ficheros.

Los administradores de sistemas son responsables del correcto depliegue de los controles de seguridad para los distintos sistemas de la empresa, y en lo relativo a la seguridad de los sistemas, han se seguir las guías, normas, especificaciones, y órdenes producidas por el responsable de seguridad de la información la compañía. No obstante, la continuidad del negocio y la efectiva asignación de recursos de la empresa es también importante para la compañía, por lo que un administrador de sistemas está obligado a notificar al Director de GI/TI cuando considere fundadamente que la aplicación de cierta norma de seguridad pudiera afectar a alguno de estos aspectos mencionados. En todo caso, el criterio del Director de GI/TI prevalecerá sobre el administrador de sistemas y el del responsable de seguridad.

Los Administradores de Sistemas efectuarán el despliegue de procedimientos de auditorías, que serán analizados periódicamente por el reponsable de seguridad, y éste último informará trimestralmente al director de GI/TI de los eventos producidos en ese espacio de tiempo para que tomen las medidas pertinentes.

2. Política de seguridad de la información

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.

2.1.1. Personal autorizado en los ficheros

A los efectos de esta política, se establecen tres niveles de autorización para el acceso a los ficheros: Básico, Agregado y Privilegiado. El Responsable de Seguridad, junto con el Director de GI/TI, contando con el asesoramiento técnico de los administradores de sistemas, deberán interpretar la mejor correspondencia entre la definición de estos niveles

políticos, y los niveles de seguridad ofrecidos por los distintos sistemas que sirvan de soporte de acceso a los datos.

- El **nivel básico** consiste en la lectura y/o modificación de registros individuales de los sistemas, con una capacidad muy básica de búsqueda, restringida al dominio de los pasos del proceso de negocio en el que el miembro se ve involucrado. Por ejemplo, un administrativo de personal recibiría acceso de búsqueda por persona de los registros individuales de nóminas, vacaciones, expedientes, o cualificaciones de personas individuales.
- El **nivel agregado** consiste en el acceso a informes que realicen algún tipo de cálculo estadístico sobre los datos, o de listas de items que la persona pudiera utilizar para la realización de dichos cálculos por su cuenta. El nivel agregado implica nivel básico.
- El **nivel privilegiado** consiste en tener acceso a toda la información que pueda producir un sistema, o acceso a los datos en formato original (por ejemplo, acceso directo a la base de datos que hay detrás de un sistema), o tener privilegios para otorgar accesos a otros miembros. El nivel privilegiado implica nivel agregado.

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. Esta tabla no incluye los privilegios especiales otorgados en la sección 1.4, que deberán ser tenidos también en cuenta a la hora del diseño de los privilegios de acceso individuales.

Personal autorizado	**Básico**	**Agregado**	**Privilegiado**
Fichero de personal	Adm. de Personal		Director de Administración, Jefe de Personal
Fichero de proveedores	Adm. de Logística	Inspector de Mantenimiento, Jefe de Logística	Director de Administración
Fichero de clientes	Adm. Ventas, Comerciales Ventas, Adm. Terminados	Jefe de Ventas, Jefe de Marketing, Comerciales de Marketing, Jefe Productos Terminados	Director Comercial

Continúa en la siguiente página

Continúa de la página anterior			
Fichero financiero	Contables	Jefe Contabilidad, Comptroller	Director Financiero
Fichero de producción	Tecnicos Laboratorio, Capataces, Operarios	Inspector Calidad, Coordinador Producción, Jefes en Dirección de Producción	Director Producción
Fichero de informes	Directores		Miembros de GI

Cuadro 2.1.: Aplicaciones

2.2. Análisis de riesgos y sensibilidad

En este punto, inicialmente se clasifican los tipos de activos, 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., además de los criterios de valoración utilizados.

2.2.1. Activos

[S] Servicios

Código	**Descripción**
[int]	Interno (usuarios y medios de la propia organización)
[www]	World Wide Web
[email]	Correo electrónico
[file]	Almacenamiento de ficheros
[ftp]	Transferencia de ficheros

Cuadro 2.2.: Servicios

[D] Datos/Información

Código	**Descripción**
[vr]	Datos vitales: Fichero Financiero, Fichero de Producción
Continúa en la siguiente página	

Continúa de la página anterior	
[com]	Datos de interés comercial: Fichero Comercial y de Proveedores
[int]	Datos de gestión interna: Fichero de Personal y de Informes
[source]	Código fuente
[exe]	Código ejecutable
[log]	Registro de actividad

Cuadro 2.3.: Datos/Información

[SW] Aplicaciones (software)

Código	**Descripción**
[app]	Servidor de aplicaciones
[file]	Servidor de ficheros
[dbms]	Sistema de gestión de bases de datos
[av]	Antivirus
[os]	Sistema operativo
[backup]	Sistema de backup
[mail]	Servidor de correo
[printer]	Servidor de impresión
[domain]	Servidor controlador de dominio

Cuadro 2.4.: Aplicaciones

[HW] Equipos informáticos (hardware)

Código	**Descripción**
[host]	Servidores
[pc]	Equipos de trabajo
[network]: [switch]	Conmutadores
[network]: [router]	Encaminadores
[network]: [firewall]	Cortafuegos
Continúa en la siguiente página	

Continúa de la página anterior

Cuadro 2.5.: Equipos informáticos

[COM] Redes de comunicaciones

Código	**Descripción**
[LAN]	Red local
[Internet]	Internet
[vpn]	Red privada virtual

Cuadro 2.6.: Redes de comunicaciones

[SI] Soportes de información

Código	**Descripción**
[electronic]: [disk]	Discos
[electronic]: [san]	Almacenamiento en red
[electronic]: [disquette]	Disquetes
[electronic]: [cd]	CD
[electronic]: [dvd]	DVD
[electronic]: [tape]	Cintas magnéticas

Cuadro 2.7.: Soportes de información

[AUX] Equipamiento auxiliar

Código	**Descripción**
[power]	Fuentes de alimentación
[ups]	Sistemas de alimentación ininterrumpida
[ac]	Equipos de climatización
[cabling]	Cableado
[robot]: [tape]	Robots de cintas

Cuadro 2.8.: Equipamiento auxiliar

[L] Instalaciones

Código	Descripción
[building]	Edificio

Cuadro 2.9.: Instalaciones

[P] Personal

Código	Descripción
[ui]	Usuarios internos
[op]	Operadores
[adm]	Administradores de sistemas
[com]	Administradores de comunicaciones

Cuadro 2.10.: Personal

2.2.2. Amenazas

[N] Desastres naturales

Código	Nombre	Descripción
N.1	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
N.2	Daños por agua	Inundación: posibilidad de que el agua acabe con los recursos del sistema.

Cuadro 2.11.: Amenazas de desastres naturales

[I] De origen industrial

Código	Nombre	Descripción
I.1	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.
I.2	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.
I.3	Contaminación mecánica	Vibraciones, polvo, suciedad,...
I.4	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta,...
Continúa en la siguiente página		

Continúa de la página anterior		
I.5	Avería de origen físico o lógico	fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
I.6	Corte del suministro eléctrico	Cese de la alimentación de potencia.
I.7	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,...
I.8	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.
I.9	Interrupción de otros servicios y suministros esenciales	Otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante,...
I.10	Degradación de los soportes de almacenamiento de la información	Como consecuencia del paso del tiempo.
I.11	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.

Cuadro 2.12.: Amenazas de origen industrial

[E] Errores y fallos no intencionados

Código	Nombre	Descripción
E.1	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.
E.2	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.
E.3	Errores de monitorización (log)	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,...
E.4	Errores de configuración	Introducción de datos de configuración erróneos.
E.7	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.
E.8	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
E.9	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.
E.10	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.
E.14	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.

Continúa en la siguiente página

Continúa de la página anterior		
E.15	Alteración de la información	Alteración accidental de la información.
E.16	Introducción de información incorrecta	Inserción accidental de información incorrecta.
E.17	Degradación de la información	Degradación accidental de la información.
E.18	Destrucción de información	Pérdida accidental de información.
E.19	Divulgación de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
E.20	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
E.21	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
E.23	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
E.24	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
E.28	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica,...
Continúa en la siguiente página		

Continúa de la página anterior

Cuadro 2.13.: Amenazas de errores y fallos no intencionados

[A] Ataques intencionados

Código	Nombre	Descripción
A.4	Manipulación de la configuración	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
A.5	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.
A.6	Abuso de privilegios de acceso	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
A.7	Uso no previsto	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.
A.8	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
A.9	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.

Continúa en la siguiente página

Continúa de la página anterior		
A.10	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.
A.11	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
A.12	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina monitorización de tráfico.
A.13	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado.
A.14	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.
A.15	Modificación de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
A.16	Introducción de falsa información	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.
A.17	Corrupción de la información	Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.
A.18	Destrucción la información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.
A.19	Divulgación de información	Revelación de información.
Continúa en la siguiente página		

Continúa de la página anterior		
A.22	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
A.24	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
A.25	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
A.26	Ataque destructivo	Vandalismo, terrorismo, acción militar,...
A.27	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.
A.28	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...
A.29	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
A.30	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

Cuadro 2.14.: Amenazas de ataques intencionados

2.2.3. Dimensiones

Nombre	**Descripción**
[D] Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
[I] Integridad de los datos	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
Continúa en la siguiente página	

Continúa de la página anterior	
[C] Confidencialidad de los datos	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
[A_S] Autenticidad de los usuarios del servicio	Aseguramiento de la identidad u origen.
[A_D] Autenticidad del origen de los datos	Aseguramiento de la identidad u origen.
[T_S] Trazabilidad del servicio	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.
[T_D] Trazabilidad de los datos	Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Cuadro 2.15.: Dimensiones

2.2.4. Criterios de valoración

Para valorar los activos se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Hay que tener muy en cuenta que:

- Se use una escala común para todas las dimensiones, permitiéndo comparar riesgos.
- Se use una escala logarítmica, centrada en diferencias relativas de valor, que no en diferencias absolutas.
- Se use un criterio homogéneo que permita comparar análisis realizados por separado.

Valor		**Criterio**
10	Muy alto	Daño muy grave a la organización
7-9	Alto	Daño grave a la organización
4-6	Medio	Daño importante a la organización
1-3	Bajo	Daño menor a la organización
0	Muy bajo	Daño irrelevante a efectos prácticos
Continúa en la siguiente página		

Continúa de la página anterior

Cuadro 2.16.: Criterio de valoración

2.2.5. Amenazas, dimensiones y valoraciones por activo

En este punto se detalla mediante una serie de tablas, una por cada tipo de activo, las amenazas que podrían afectarle a cada activo, las dimensiones y se realiza una valoración que se corresponde con la media de las valoraciones de todas las dimensiones.

[S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requieren una serie de medios.

Activo	**Amenazas**	**Dimensiones**	**Valoración**
[int]	[E.1] [E.2] [E.9] [E.14] [E.20] [A.6] [A.11] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D]	8
[www]	[E.1] [E.2] [E.20] [A.6] [A.11] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[email]	[E.2] [E.9] [E.14] [E.20] [A.6] [A.11] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D]	7
[file]	[E.1] [E.2] [E.9] [E.14] [E.20] [A.6] [A.11] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[ftp]	[E.2] [E.14] [E.20] [A.6] [A.11] [A.12] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10

Cuadro 2.17.: Amenazas, dimensiones y valoraciones por servicios

[D] Datos/Información

Elementos de información que, de forma singular o agrupados de alguna forma, representan el conocimiento que se tiene de algo. Los datos son el corazón que permite a la empresa prestar sus servicios. Son en cierto sentido un activo abstracto que será almacenado en los servidores.

Activo	Amenazas	Dimensiones	Valoración
[vr]	[E.1] [E.2] [E.7] [E.9] [E.14] [E.15] [E.16] [E.18] [E.19] [E.20] [A.6] [A.11] [A.14]	[D] [I] [C] [A_S] [A_D]	10
[com]	[E.1] [E.2] [E.7] [E.9] [E.14] [E.15] [E.16] [E.18] [E.19] [E.20] [A.6] [A.11] [A.14]	[D] [I] [C] [A_S] [A_D]	8
[int]	[E.1] [E.2] [E.7] [E.9] [E.14] [E.15] [E.16] [E.18] [E.19] [E.20] [A.6] [A.11] [A.14]	[D] [I] [C] [A_S] [A_D]	10
[source]	[E.1] [E.2] [E.4] [E.14] [E.18] [E.19] [E.20] [A.6] [A.11]	[D] [I] [C] [A_S] [A_D]	10
[exe]	[E.1] [E.2] [E.4] [E.8] [E.14] [E.18] [E.19] [E.20] [A.8]	[D] [I] [C] [A_S] [A_D]	9
[log]	[E.2] [E.3] [E.4] [E.15] [E.18]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	8

Cuadro 2.18.: Amenazas, dimensiones y valoraciones por datos/información

[SW] Aplicaciones (software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

Activo	Amenazas	Dimensiones	Valoración
[app]	[E.2] [E.8] [E.20] [A.8]	[D] [I] [C] [A_S] [A_D]	10
Continúa en la siguiente página			

Continúa de la página anterior			
[file]	[E.2] [E.4] [E.18] [E.19] [A.6]	[D] [I] [C] [A_S] [A_D]	10
[dbms]	[E.2] [E.4] [E.15] [E.16] [E.18] [E.19] [E.20] [A.6] [A.8] [A.11] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[av]	[E.2] [E.8] [E.20] [A.8]	[D] [I] [C] [A_S] [A_D]	10
[os]	[E.2] [E.4] [E.20] [A.6] [A.8] [A.20] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[backup]	[E.2] [E.4] [E.18] [E.19] [A.6]	[D] [I] [C] [A_S] [A_D]	10
[mail]	[E.2] [E.4] [E.20] [A.6] [A.8] [A.20] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[printer]	[E.2] [E.4] [E.20] [A.6] [A.8] [A.20] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
[domain]	[E.2] [E.4] [E.20] [A.6] [A.8] [A.20] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10

Cuadro 2.19.: Amenazas, dimensiones y valoraciones por aplicaciones

[HW] Equipos informáticos (hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Activo	**Amenazas**	**Dimensiones**	**Valoración**
[host]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.4] [I.5] [I.6] [I.7] [E.4] [E.23] [A.7] [A.8] [A.11]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10
Continúa en la siguiente página			

Continúa de la página anterior			
[pc]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23] [A.7] [A.8] [A.11]	[D] [I] [C] [A_S] [A_D]	8
[network]: [switch]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.4] [E.9] [E.23]	[D] [I] [C] [A_S] [A_D]	9
[network]: [router]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.4] [E.9] [E.23]	[D] [I] [C] [A_S] [A_D]	9
[network]: [firewall]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.4] [E.9] [E.23]	[D] [I] [C] [A_S] [A_D]	9

Cuadro 2.20.: Amenazas, dimensiones y valoraciones por equipos informáticos

[COM] Redes de comunicaciones

Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

Activo	**Amenazas**	**Dimensiones**	**Valoración**
[LAN]	[E.2] [E.4] [E.9] [E.23] [A.7] [A.8] [A.11] [A.12] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D]	10
[Internet]	[E.2] [E.4] [E.9] [A.7] [A.8] [A.12] [A.14] [A.24]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	6
[vpn]	[E.2] [E.4] [E.9] [A.7] [A.8] [A.11]	[D] [I] [C] [A_S] [A_D] [T_S] [T_D]	10

Cuadro 2.21.: Amenazas, dimensiones y valoraciones por redes de comunicaciones

[SI] Soportes de información

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Activo	Amenazas	Dimensiones	Valoración
[electronic]: [disk]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	10
[electronic]: [san]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	10
[electronic]: [disquette]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	9
[electronic]: [cd]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	9
[electronic]: [dvd]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	9
[electronic]: [tape]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [I] [C] [A_S] [A_D]	10

Cuadro 2.22.: Amenazas, dimensiones y valoraciones por soportes de información

[AUX] Equipamiento auxiliar

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Activo	Amenazas	Dimensiones	Valoración
[power]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D]	8
[ups]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.4] [E.23]	[D]	8
[ac]	[N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D]	10
[cabling]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D]	8
Continúa en la siguiente página			

Continúa de la página anterior			
[robot]: [tape]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D]	8

Cuadro 2.23.: Amenazas, dimensiones y valoraciones por equipamiento auxiliar

[L] Instalaciones

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

Activo	**Amenazas**	**Dimensiones**	**Valoración**
[building]	[N.1] [N.2] [I.1] [I.2] [I.3] [I.5] [I.6] [E.23]	[D] [A_S] [A_D]	10

Cuadro 2.24.: Amenazas, dimensiones y valoraciones por instalaciones

[P] Personal

En este epígrafe aparecen las personas relacionadas con los sistemas de información.

Activo	**Amenazas**	**Dimensiones**	**Valoración**
[ui]	[A.19] [A.29] [A.30]	[D]	8
[op]	[A.19] [A.29] [A.30]	[D]	7
[adm]	[A.19] [A.29] [A.30]	[D]	6
[com]	[A.19] [A.29] [A.30]	[D]	6

Cuadro 2.25.: Amenazas, dimensiones y valoraciones por personal

2.3. Conformidad con la legislación vigente

De acuerdo con la Ley Orgánica de Protección de Datos, se han desarrollado los documentos de seguridad que se adjuntan a la política, uno por cada fichero, en base a la normativa descrita en el reglamento de dicha ley.

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, para más información consultar la sección 2.2.1

3.2. Seguridad del edificio

En este apartado se recogen las medidas de seguridad 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, siguiendo las indicaciones de ISO 17799 [2] y apartado 3.3.1 de la normativa de seguridad contra incendios.
- Extintores: repartidos por los diversos edificios, se colocarán en sitios visibles y de fácil acceso.Siguiendo las indicaciones de ISO 17799 y apartado 3.3.1 de la normativa de seguridad contra incendios. Según Norma ISO 17799, se instalará un extintor cada 125 m^2. 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 Compatibilidad 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 (CPD) 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 estará permitido al personal directamente implicado mediante tarjeta de identificación personal, según norma ISO 7816-11.

- 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, situada en otro edificio independiente alquilado para tal fin. Con el armario ignifugo se cumple la protección contra el fuego con homologación según norma Europea EN-1047-1 y protección contra el robo según norma Europea EN-1143-1

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 departamento 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. Finalidad

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 65)
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. Dicho plan aplica a la escala de nuestra organicación las recomendaciones establecidas en la publicación del 800-50 del NIST (*National Institute of Standards and Technology, Technology Administration*, del Departamento de Comercion de los Estados Unidos de Norteamérica) [3].

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 oficinas 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

Las faltas derivadas del incumplimiento de alguna de las medidas descritas en el presente documento se pueden clasificar en leves, graves y muy graves.

Se considerará falta leve:

1. Dejar la contraseña personal escrita a la vista de los demás o comunicación de la misma a otros empleados.
2. Instalación de software no autorizado sin permiso.
3. Instalación de hardware no autorizado sin permiso.
4. Uso del correo electrónico para fines lúdicos.
5. Almacenamiento de información no autorizada (música, fotos...) en los equipos.

Se considerarará falta grave:

1. Intento de acceso a objetos restringidos del sistema o instalaciones de la misma índole.
2. Acceso a webs restringidas o de contenido peligroso.
3. No comunicación del conocimiento de ataques perpetrados contra el sistema o la organización.
4. La reincidencia en las faltas leves, aunque sean de distinta naturaleza, dentro de un trimestre, cuando hayan mediado sanciones.

Se considerarará falta muy grave:

1. Suplantación de la identidad de otro empleado.
2. Destrucción, manipulación o hurto de equipos o sistemas de la empresa.
3. Robo de información.
4. Ataque a los sistemas de información de la empresa o a los de los clientes.
5. Interceptación de información transmitida a través de la red de la organización.
6. Acceso a zonas físicas restringidas.
7. La reincidencia en falta grave, aunque sea de distinta naturaleza, dentro del mismo trimestre, siempre que hayan sido objeto de sanción.

Las sanciones que la empresa podrá aplicar, según la gravedad y circunstancias de las faltas cometidas, serán las siguientes:

1. Faltas leves:
   - Amonestación verbal.
   - Amonestación por escrito.
   - Suspensión de empleo y sueldo un día.
2. Faltas graves:
   - Suspensión de empleo y sueldo de uno a diez días.
   - Inhabilitación, por plazo no superior a un año, para el ascenso a la categoría superior.
3. Faltas muy graves:
   - Pérdida temporal o definitiva de la categoría profesional.
   - Suspensión de empleo y sueldo de once días a dos meses.
   - Inhabilitación durante dos años o definitivamente para pasar a otra categoría.
   - Despido.

4.9. Personal temporal y subcontratado

El personal temporal y subcontratado será informado con antelación de la política de seguridad de la empresa, independientemente del tiempo de contratación. Como medida de seguridad adicional, se le otorgarán cuentas de usuario temporales. En el caso de visitas ocasionales o de clientes, estas personas estarán acompañadas en todo momento por personal interno a la organización.

Todos los servicios contratados por la empresa requerirán una cláusula de responsabilidad civil especificada en el contrato. En caso de incidente, la empresa contratada deberá pagar la indemnización fijada para el caso que corresponda. Cuando se trate de personal subcontratado, las sanciones aplicables serán las descritas en la sección 4.8.

5. Política de seguridad en software y hardware

5.1. Identificación y autenticación

La identificación y autenticación a la red corporativa está centralizada. Esto quiere decir que cada empleado tiene su nombre de usuario y contraseña que le permite acceder a:

1. El propio sistema operativo.
2. Los datos organizados en forma de archivos del sistema operativo, como cualquiera producido por herramientas de oficina (Textos, Hojas de cálculo, imágenes, etc.), y que sean accesibles a través del sistema de ficheros del sistema operativo.
3. Correo electrónico corporativo.
4. El acceso a las distintas aplicaciones corporativas puestas a disposición por la compañía, cuyo acceso se prohibe fuera del entorno de seguridad de la red corporativa. El acceso a través de una red privada virtual está autorizado por esta política.

5.1.1. Nombre de usuario

El nombre de usuario se obtiene a partir del nombre del empleado. Por ejemplo: para un empleado llamado Juan Perez Madrid su nombre de usuario será: jperez, que se compone por las iniciales de su nombre seguido de su primer apellido.

En caso de que haya dos empleados con el mismo nombre se puede adoptar cualquier regla que permita identificarlos, por ejemplo: vimmartinez, vicmmartinez, etc.

5.1.2. Contraseña

Las medidas mínimas de seguridad de la contraseña para usuarios del sistema operativo son:

- Tamaño mínimo de 8 caracteres.
- Utilización de caracteres alfanuméricos.
- Caducidad de las contraseñas a los 2 meses.
- Máximo de 3 intentos de acceso. En el caso de fallar 3 veces se bloquea el usuario y se debe contactar con el Administrador de Sistemas para resetear el usuario.

5.2. Registro de accesos

5.2.1. Gestión de privilegios de usuarios

Se seguirán en general las pautas marcadas en el punto 9.1 del estándar ISO 17799, siguiendo un enfoque de sistema de permisos cerrado, donde todo lo que no se permite explícitamente está prohibido. Cada usuario será categorizado en una serie de perfiles en función de su trabajo, cumpliendo con el principio del mínimo privilegio: sólo podrán hacer lo que necesitan para su trabajo.

De forma acorde al punto 9.2 del estándar, se establecerán procesos de alta y baja de los usuarios en los sistemas de información. En particular, cuando un usuario es dado de alta en persona en las oficinas administrativas de la Organización, tras haber presentado pruebas de su identidad, será añadido al directorio LDAP de la organización.

El usuario recibirá un documento escrito con una relación de sus privilegios y su responsabilidad de evitar su uso indebido. Este documento ha de ser firmado por el usuario.

El usuario obtendrá nombres de usuario y claves de acceso seguras para cada aplicación que necesite para cumplir su trabajo. Posteriormente, y en su primer acceso, será de su responsabilidad cambiar las claves.

A la hora de la baja, que habrá de realizarse también en persona y con pruebas de identidad. Se desactivarán todas las cuentas del usuario.

Cada 6 meses se revisará el listado de privilegios de todos los usuarios del sistema, buscando posibles incongruencias o permisos innecesarios y cada 2 meses, por el riesgo mayor que representan, se realizarán listados de los usuarios que posean permisos administrativos de los sistemas.

5.2.2. Acceso al Sistema Operativo.

Las medidas en este aspecto serán las expuestas en el punto 9.5 del ISO 17799. No se podrá iniciar sesión a nivel de sistema operativo de manera remota en principio a ninguna máquina, salvo por aquellas que requieran un mantenimiento continuo. Éstas conexiones remotas deberán hallarse cifradas, empleando el protocolo Secure SHell (SSH).

Toda estación de trabajo, sea cual sea el sistema operativo que soporte, harán uso de los mecanismos existentes de protección por contraseña para el acceso al sistema.

Las contraseñas tendrán una caducidad de 2 meses.

La BIOS de todas las máquinas estarán protegidas con contraseña. Esta será la misma para todas las máquinas y solo serán accesibles por el personal técnico.

El fichero de contraseñas tendrá sus propias medidas de seguridad, de forma acorde al Real Decreto RD994/1999 de la legislación española, recogidas en su propio documento de seguridad. En particular, no será legible para otro usuario que el Administrador de Seguridad.

5.2.3. Acceso a los programas y datos

Sólo los usuarios que lo requieran tendrán acceso a cada aplicación, siguiendo estrictamente un esquema cliente/servidor a través de la red de la empresa

Los usuarios normales nunca tendrán acceso directo a los soportes con la información, sólo a los programas que manejan dicha información.

Las aplicaciones web tendrán limitada su disponibilidad a horario de oficina, para evitar que puedan ser atacadas cuando no se encuentre el personal de seguridad en la empresa.

5.2.4. Registro de entradas

Se harán auditorías de las aplicaciones y sistemas operativos para registrar toda entrada y salida del sistema, ejecución de operaciones de alto impacto y fallos de grave importancia.

Se examinarán todos los intentos fallidos de entrada, realizando estadísticas que pongan en relieve aquellas que puedan dar sospechas de ser maliciosas.

Los usuarios serán notificados de la fecha y hora de su última entrada, quedando obligado a advertir al departamento de informática cualquier anomalía que detecten.

Los ficheros de registro serán protegidos debidamente a través del uso de los permisos correspondientes sobre el fichero, siendo sólo legibles por los administradores y personal técnico correspondiente.

Se evitara que los archivos sean demasiado grandes, para ello se rotarán los ficheros de auditoría cada semana, manteniendo tres ciclos en el sistema y pasando a copias de seguridad posteriormente.

5.2.5. Responsabilidades

Administrador de Seguridad y personal técnico: bloquear toda cuenta de usuario una vez no se necesite, y crear las cuentas con contraseñas aleatorias seguras. El Administrador tendrá que revisar las incidencias de accesos fallidos, y comunicar cualquier posible ataque al Comité.

Resto personal: mantener las claves en secreto, las nuevas contraseñas deberán cumplir unos niveles mínimos de calidad y serán responsables de cualquier sustracción o pérdida de la tarjeta identificativa sila tuvieran

5.3. Protección ante software malicioso

Para combatir ciertas amenazas como malware..., se tendrá instalado en el servidor un antivirus con su correspondiente licencia, Kaspersky Bussiness Space Security en este caso, de manera que los ordenadores de los empleados se actualizarán por los reponsables de Sistemas o mediante actualizaciones programadas a diario, esto hace que sea más cómodo y que siempre estén actualizados puesto que no estarán instalados de manera local en cada ordenador, llevando así un mayor control evitando así que la obligación de tener los ordenadores actualizados recaiga en el trabajador.

5.3.1. Caracteríaticas del antivirus

Aspectos sobresalientes:

- Protección integrada contra virus, spyware, ataques de hackers y spam.
- Protección proactiva incluso contra los más recientes programas maliciosos
- Cortafuegos personal con IDS e IPS
- Reversión de cualquier cambio malicioso realizado en el sistema
- Protección contra ataques phishing y spam
- Redistribución inteligente de recursos durante el escaneado completo del sistema

5.4. Uso aceptable de los equipos

Todo uso de recursos computacionales por parte de los trabajadores de la empresa debe ser con fines laborales del cargo y funciones para los que fueron contratados. Por tanto, deben cumplir unos determinados requisitos que veremos a continuación.

5.4.1. Uso legal

Los servidores y estaciones de trabajo de Bodegas San Dionisio, S.A. serán utilizados únicamente con fines legales. Por tanto, estará prohibida la transmisión, almacenamiento o distribución de información, datos o material que viole alguna ley o regulación aplicable, como pueda ser software sin licencia, contenido con derechos de autor, material que viole derechos de propiedad intelectual, etc., así como todo material obsceno, difamatorio o que constituya una amenza ilegal.

Asimismo, también serán sancionadas las violaciones al sistema o a la red. Incluyendo aquí acciones como accesos no autorizado, interferencias en el servicio de cualquier usuario del sistema mediante bombas de correo, intentos de sobrecarga o de ataque, etc.

En el siguiente apartado quedarán detalladas las prohibiciones de esta índole.

5.4.2. Uso inaceptable

Queda prohibido las siguientes acciones:

- Cualquier acción que pueda infringir la legislación vigente en el Estado Español.
- Cualquier intento de causar daño a los recursos y servicios computacionales. Incluyendo cualquier actividad negligente que afecte al normal funcionamiento del sistema, como la propagación de virus, caballos de troya, gusanos, bombas de correo, archivos dañinos o cualquier otro software malicioso, ya sea de forma intencionada o no avisando de la existencia de los mismos.
- Intentos no autorizados de acceso a cualquier cuenta o recurso computacional que no corresponda al trabajador.
- Intentar acceder sin autorización a sitios o servicios no autorizados, haciendo uso de herramientas intrusivas, descifre de contraseña, etc.
- Monitorear tráfico de cualquier red o equipo sin el consentimiento del administrador de red o el usuario del equipo monitoreado. Queda prohibido capturar contenido de tráfico no emitido por el equipo que se esté usando, o información sensible de otros usuarios.
- Almacenar, transmitir, divulgar o solicitar información personal de otros usuarios o clientes sin su conocimiento.
- El uso de los equipos o servicios para fines personales, ya sean actividades comerciales, con fines de lucro o de otro tipo.
- Almacenar, difundir, comercializar, exhibir o copiar cualquier tipo de material obsceno, difamatorio o que constituya una amenza ilegal.
- Desarrollo de actividades que produzcan:
  - La congestión de la red.

  - La eliminación o modificación no debida de información del sistema.
  - La violación de la privacidad e intimidad de otros usuarios.
  - El deterioro del trabajo de otros usuarios.

- Revelar a terceros o compartir contraseñas de acceso.
- Conexión, desconexión o reubicación de equipos sin la autorización adecuada.

5.4.3. Otras prohibiciones

- El uso de los recursos computacionales para juegos recreativos.
- Uso de programas no recomendados en las estaciones de trabajo.
- Beber, comer o fumar en zonas no dedicadas a ello o donde no se autoriza.

5.5. Gestión de soportes

Las medidas que se van a tomar para la gestión de los soportes de almacenamiento, se redactan en esta sección. Para la realización de las mismas, se siguen las recomendaciones de la norma UNE-ISO/IEC 17799, indicadas en el punto «8.6 Utilización y seguridad de los soportes de información».

El objetivo principal por el que se sigue la norma indicada en el párrafo anterior es el de evitar daños a los activos e interrupciones de las actividades de la organización. Para ello se establecen los procedimientos operativos adecuados para proteger los documentos, soportes informáticos (tales como CDs, cintas, etc.), datos de entrada o salida y documentación del sistema, de daño, robo y acceso no autorizado.

5.5.1. Gestión de soportes extraibles

Los procedimientos a seguir para la gestión de los soportes informáticos desechables como cintas, discos o resultados impresos, seguiran los siguientes controles:

- Se borrarán cuando no se necesiten más, los contenidos previos de todo tipo de soporte reutilizable del que se desprenda la organización
- Todo soporte del que se desprenda la organización debería requerir autorización y se debería guardar registro de dicho acto para guardar una pista de auditoría.
- Todos los soportes se almacenarán a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes.

5.5.2. Eliminación de soportes

Se eliminarán los soportes de forma segura y sin peligro cuando no se necesiten más. Podría filtrarse a personas externas información sensible si los soportes se eliminan sin precauciones. Para minimizar el riesgo con la eliminación segura de los soportes se establecen los siguientes procedimientos:

- Los soportes que contengan información sensible se almacenarán y eliminarán de forma segura, por ejemplo, incinerándolos, triturándolos o vaciando sus datos para usarlos en otra aplicación dentro de la organización.
- La siguiente lista identifica qué elementos requieren una eliminación segura:
  - Documentos sobre papel.
  - Registros de voz.
  - Papel carbón.
  - Informes.
  - Cintas de impresora de un solo uso.
  - Cintas magnéticas.
  - Discos o casetes extraibles.
  - Soportes de almacenamiento óptico, incluidos los de distribución de software de fabricantes.
  - Listados de programas.
  - Datos de pruebas.
  - Documentación de los sistemas.
- Se registrará la eliminación de elementos sensibles donde sea posible para mantener una pista de auditoría.

5.5.3. Procedimientos de utilización de la información

A continuación se detallan los procedimientos de utilización y almacenamiento de la información de forma coherente con su clasificación para protegerla de su mal uso o divulgación no autorizada, y de acuerdo con su soporte:

- Se etiquetarán todos los soportes para su gestión.
- Existirán restricciones de acceso para identificar al personal no autorizado.
- Se realizará el mantenimiento de un registro formal de recipientes autorizados de datos.
- Se asegurarán de que los datos de entrada, su proceso y la validación de la salida están completos.

- Se protegerán los datos que están en cola para su salida en un nivel coherente con su criticidad.
- Se almacenarán los soportes en un entorno acorde con las especificaciones del fabricante.
- Se marcarán todas las copias de los datos con la dirección de los recipientes autorizados.
- Se revisarán las listas de distribución y de recipientes autorizados a intervalos regulares.

5.5.4. Seguridad de la documentación de sistemas

La documentación de sistemas puede contener una variedad de información sensible. Para proteger la documentación de sistemas de accesos no autorizados se considerarán los siguientes controles y medidas:

- Se almacenarán con seguridad la documentación de sistemas.
- La lista de acceso a la documentación de sistemas se limitará al máximo, y será autorizada por el propietario de la aplicación.
- La documentación de sistemas mantenida en una red pública, o suministrada vía una red pública, se debería proteger adecuadamente.

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.

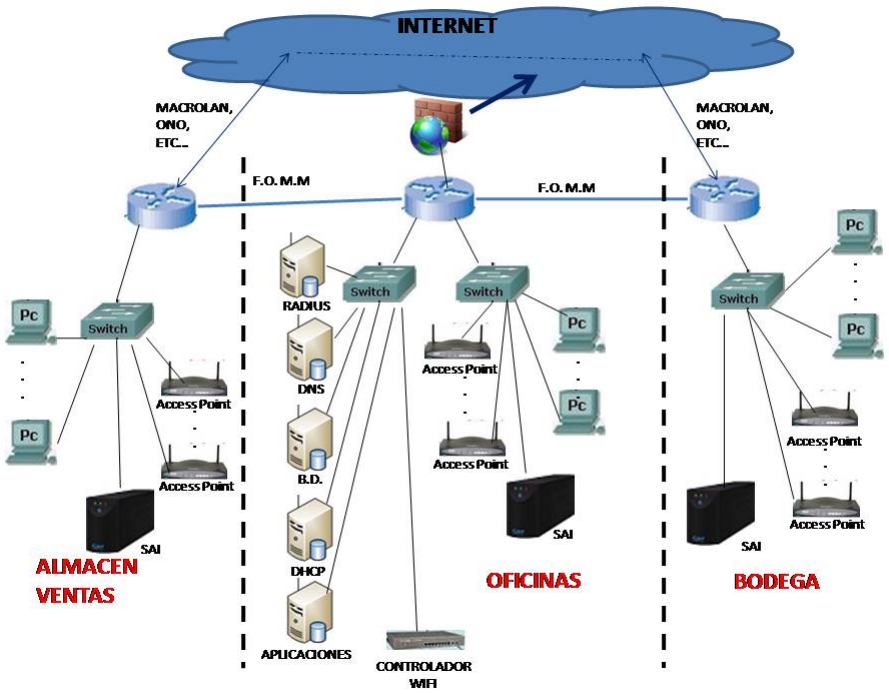

Figura 6.1.: Arquitectura de la red.

6.1.5. Seguridad

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 routers o enrutadores 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 routers 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.

6.1.6. 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.

6.1.7. 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

7.1. Introducción

Como se ha mencionado en la sección 3.6, el CPD consta de espacial relevancia en la organización de Bodegas San Dionisio, S.A., por lo que, en caso de ser necesario, la recuperación de activos se centrará en dicho edificio.

En caso de ataque o desastre, se priorizará la recuperación de ciertos activos, como son:

1. Servidores.
2. Copias de seguridad.
3. Otro hardware.
4. Infraestructuras.

7.2. Copias de seguridad

Se realizarán copias de seguridad periódicamente, trasladando las cintas a la sala destinada a ello, situada en una ubicación distinta a los edificios de los que consta la empresa, para así evitar que se pierdan los backups junto a los datos originales por determinadas causas, como incendios o inundaciones por ejemplo. La sala alquilada para tal fin almacenará estas copias en armarios ignífugos.

Las copias se guardarán con orden cronológico, manteniendo así una estructura lógica de almacenado, facilitando la búsqueda de alguna cinta si fuese necesario.

Las copias de seguridad contendrán los siguientes datos:

1. Ficheros de datos, mencionados en la sección 2.1.
2. Configuración de los sistemas.
3. Registros.

Cubren amenazas de desastres naturales (N.1, N.2), de origen industrial (I.1-I.7, I.11), de errores y fallos no intencionados (E.1,E.2, E.8, E.15, E.17, E.18) y de ataques intencionados (A.4, A.8, A.11, A.15-A.18, A.22, A.25-A.27, A.29). Se debe tener en cuenta que están enfocadas a una futura recuperación de los datos del sistema (o parte de este), por lo que el proceso de copias debe ser confiable. Así como asegurar que si hiciese falta una recuperación, esta fuese rápida y eficiente.

Se ha decidido hacer backups combinando dos tipos de copias, completas y diferenciales. Esta elección se ha tomado teniendo en cuenta la frecuencia de las copias y el método de almacenamiento, los cuales veremos a continuación. Se explicará en cada caso el por qué de la elección del tipo de copia de acuerdo a las necesidades. Para dicha elección se ha de tener en cuenta que las copias diferenciales ofrecen una mayor facilidad en la búsqueda de archivos, pudiendo ser esta más tediosa usando copias progresivas.

7.2.1. Tipos de copias y frecuencia

Se realizarán dos tipos de copias de seguridad, cada uno con un fin distinto:

- Diferenciales: Realizaremos copias diferenciales diariamente, de manera que obtendremos una cinta al día con los datos modificados desde la última copia completa que se haya realizado.
- Completas: Se realizarán distinto tipos de copias completas:
  - Semanales: Cada semana se realizará una copia completa de los datos de esos siete días. Es decir, al cabo de 4 semanas, se habría obtenido una cinta con los nuevos datos generados o modificados de cada semana.
  - Mensuales: Al finalizar cada més se realizará una copia completa de los datos del sistema.

La razón por la que se realiza la copia completa semanal es para evitar que la copia diaria diferencial llegue a ser suficientemente grande, y así el tiempo de realización de la copia no crezca excesivamente. La diferencia de hacer la copia semanal completa y hacer una diferencial más reside en que el siguiente día las copias diferenciales empezarán a hacerse desde esta última copia, por lo que la cantidad de datos que almacenarán no será nunca superior a la de 6 días de modificación o creación de los mismos.

Dichas copias automatizadas se realizarán en un horario en el que no se esté haciendo uso de las instalaciones, para evitar en medida de lo posible que se estén manejando datos al mismo tiempo que se realiza la copia, por lo que sería una opción lógica que se realicen en horario nocturno. Concretamente, se realizarán a las 4:00, a menos que se realice alguna labor de mantenimiento nocturna puntual a dicha hora; en este caso, el responsable de la programación de las copias de seguridad asignará una nueva hora de acuerdo al horario de mantenimiento estimado.

Para mayor seguridad y confidencialidad, los backups se realizarán cifrando la información, de manera que si fuese necesario una recuperación de los datos, el mismo software de cifrado desencriptaría los datos para su correcta restauración en el sistema, sea este o no el encargado de realizar o leer las copias de seguridad con las que se trabajen.

Por otra parte, el software encargado de la realización de las copias verificaría, una vez acabado el proceso, que el backup se ha realizado correctamente, sin ningún tipo de error, obteniéndose una copia fiable de los datos correspondientes.

7.2.2. Almacenamiento

Las copias diarias se alamacenarán en un armario ignífugo dedicado expresamente a ello, dentro de la organización de la empresa, en una sala del edificio de oficinas, con la seguridad necesaria. Se utilizarán 6 cintas para este tipo de copias, una para cada día de la semana, ya que el séptimo día se realizará una copia completa, por lo que la diaría no sería necesaria. Las cintas se reutilizarían en cada ciclo de copias, siendo estas reemplazadas por nuevas cada cierto periodo de tiempo que puedan empezar a deteriorarse por su uso. Este periodo de tiempo será estimado por el responsable del mantenimiento de las copias de seguridad.

Al igual que las copias diarias, las semanales se tratarán con el mismo método, constando este ciclo con 4 cintas que se graban semanalmente. Al final de cada mes se realizará una copia completa, por lo que las cintas podrán ser reutilizadas como se ha explicado anteriormente.

La copia completa mensual se tratará de diferente forma, ya que será trasladada a un edificio ageno a la ubicación actual del equipamiento de la empresa, para evitar la pérdida de los datos originales y copias por catástrofes como incendios, terremotos, inundaciones, etc. Estarán en un lugar con las medidas de seguridad adecuadas y seguras de amenzas como las que hemos nombrado, en una caja fuerte o armario a prueba de fuego.

Todas las copias serán almacenadas siguiendo un orden cronológico, tanto las diarias y semanales en su correspondiente sala, como las copias completas mensuales fuera de las instalaciones principales de Bodegas San Dionisio, S.A. Este orden lógico facilitará la búsqueda de alguna determinada copia de una fecha específica.

Todo el formato físico de copias quedaría correctamente etiquetado. Esto significa que dicha etiqueta estaría cifrada mediante un código interno a la organización. Por ejemplo, se podrían usar 7 caracteres alfanuméricos, de forma que el primero se establezca para indicar a qué departamento pertenecen los datos:

- 1: Departamento Administrativo
- 2: Departamento Comercial
- 3: Departamento de Producción
- 4: Departamento de GI/TI
- 5: Departamento Financiero

el segundo caracter indicaría qué tipo de backup es:

- D: Diario
- S: Semanal
- M: Mensual

y el resto para la fecha en que se ha realizado la copia, también debidamente encriptada, pudiendo usar indistintamente letras o números para referirse al día, mes y año; por ejemplo, el mes de la A (letra 1 del abecedario) hasta la L (letra 12), y el año el número de años que ha trascurrido desde 1990. Así, la etiqueta 5S03J21 correspondería a una copia semanal que contiene datos del departamente financiero, realizada el 03 de octubre de 2011.

Este etiquetado evita la posibilidad de que una persona agena pueda buscar información en los backups o, al menos, que no le sea fácil hacerlo mediante la información visible.

El cifrado de información y de las etiquetas de las copias ayudan a las amenazas E.14, E.16, E.18, E.19, A.4, A.14, A.18 y A.19.

7.2.3. Responsables

El Jefe de TI, con la supervición del Responsable de Seguridad y el Director de GI/TI, delegará un miembro del departamento para realizar las copias de seguridad. El responsable designado elaborará un procedimiento para probar las copias de seguridad y pruebas de restauración de las copias de seguridad, bajo la supervisión del especialista en seguridad informática del mismo departamento. Si dicho responsable no es el administrador de servidores de datos y aplicaciones, este supervisará también el procedimiento mencionado.

7.3. Recuperación de activos

En caso de que se sufra un desastre o ataque, la recuperación de activos dependerá del tipo de ataque que haya ocurrido:

- Datos: Si los daños sufridos han sido sobre los ficheros de datos, se podrían tomar varias acciones dependiendo del daño:
  - Si han sido los datos actuales del sistema los que han sufrido el ataque, se tendría que llevar a cabo una restauración o recuperación de los mismos usando para ello las copias de seguridad que se han ido llevando a cabo regularmente, de acuerdo a lo redactado anteriormente. Si el ataque se ha dado durante el último mes, la recuperación de datos se podrá realizar de manera agilizada, ya que se tendría acceso casi inmediato a los datos, que se encontrarían en la sala destinada a ubicar estas copias, en el edificio de oficinas. Por lo que bastaría con recuperar la copia deseada y volcar el contenido en el sistema, recuperando la pérdida o modificación de datos que se ha sufrido.
  - En cambio, si los datos que han sido objeto del ataque son los backups, se habría de actuar de la manera opuesta. Es decir, si se han perdido o deteriorado las copias de seguridad, la recuperación de estas se haría simplemente realizando nuevas copias de los datos del sistema. Las nuevas copias sustituirían a las que han sufrido los daños, quedando almacenadas en el lugar correspondiente y

sin afectar esto a la continua creación de copias de seguridad que debe seguir desarrollándose diariamente.

- Si, desafortunadamente, tanto los datos actual del sistema como las copias de seguridad sufren daños, estaríamos ante un problema más serio. En este caso, la recuperación de los datos sería prácticamente imposible, a no ser que se haya perdido por borrado de memoria y se pueda usar un software de recuperación de datos eliminados. En otro caso, como incendio o inundación por ejemplo, no quedaría más remedio que recopilar de nuevo todos los datos perdidos mediante las mismas fuentes que se obtuvieron originalmente. Por este motivo se almacenan las copias mensuales completas en otro lugar físico, minimizando la posibilidad de que se pierdan los datos originales y las copias de ellos. Sería más probable que esto ocurriera con las copias diarias y semanales, pero la recuperación de estos datos sería más asequible que hacerlo de todos los datos de la empresa, ya que serían los datos modificados o creados dentro del último mes a lo sumo.

- Software: Ante un ataque que provoque daños en el software, se reinstalará el software afectado, volviéndose a configurar haciendo uso de las copias de seguridad, que contienen la configuración de los sistemas de la organización.

  El responsable de mantener actualizada la información de configuración del software será delegado de la misma forma que el responsable de realizar las copias de seguridad, detallado anteriormente, puediendo ser la misma persona la designada a ambas tareas. Dicha información será revisada mensualmente, para quedar archivada si fuese necesario una copia de la configuración al mes en caso de haberse producido cambios en esta, junto con la copia completa mensual. Este periodo de revisión puede estar sujeto a cambios.

- Hardware: Si el ataque o desastre afecta al hardware, la opción posible es la recuperación del equipo afectado mediante adquisición de uno nuevo. Normalmente, esto implicaría la compra del producto y su correspondiente instalación correcta en el sistema, haciendo uso de las copias de seguridad si es necesario recuperar datos o archivos de configuración del sistema almacenados previamente. Es posible que en la empresa se disponga de recambio para ese hardware si se trata de elementos comunes, como podría ser un monitor o un ordenador, con lo que la recuperación no se demoraría demasiado. Sin embargo, si el problema ocurre con hardware un poco más sofisticado o algún recurso de red es posible que este se demore un poco más.

- Infraestructuras: En caso de que la infraestructura del edificio o de alguna sala sufra los daños, el problema sería de distinta índole. Si el problema es de infraestructuras como armarios, puertas, material de seguridad, etc., se llevaría a cabo su arreglo para que la organización siga funcionando normalmente a través de la contratación de especialistas en el sector si fuese necesario. Si el problema es más serio, con daños en la estructura del edificio, habría que estudiarse la posibilidad de abandonar las

instalaciones, ya fuese temporal o definitivamente, o simplemente el arreglo de la zona afectada sin necesidad de desalojo. Si este daño afecta también al hardware, se actuaría como se ha especificado anteriormente.

- Para tener cierta salvaguardia, se contrará un seguro que cubra daños materiales producidos por los siguientes aspectos:
  - Incendio, humo o explosión.
  - Actividades externas a la organización que dañen las instalaciones, como pueden ser actos de vandalismo, robos, atracos, colisión de vehículos, etc.
  - Inundaciones.
  - Daños eléctricos, subidas de tensión o caída de rayos.
  - Rotura de cristales.
  - Activación de medidas automáticas de extinción de incendios.
  - Averías de agua, luz y otras instalaciones de la misma naturleza.
  - Daños a los equipos de la empresa, tanto informáticos como de producción.
  - Daños en las infraestructuras del edificio, tanto muros, techos y suelos, como armarios, puertas, etc.

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.

Producto	**Precio**	**Cantidad**	**Total**
Antivirus con cortafuegos: Kaspersky	520 €	3	520 €
Producto2	Precio2	3	3*Precio2

Cuadro A.1.: Presupuesto Software

A.2. Hardware

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

Producto	**Precio**	**Cantidad**	**Total**
Cinta Magnética SDLT para copias mensuales	62.19	12	746.28
Cinta Magnética DLT para copias semanales	33.59	4	134.36
Cinta Magnética DLT para copias diarias	23.67	6	142.02
Hardware para backups	3182	1	3182

Cuadro A.2.: Presupuesto Hardware

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.

Producto	Precio	Cantidad	Total
Armario ignifugo	2573 €	2	5146 €
Extintor de CO2	38.5 €	17	654.5 €
Señalización extintor	0.50 €	17	8.5 €
Revisión anual extintores	11 €	17	187 €
Detector iónico de humos visibles e invisibles	28 €	13	363 €
Cámara de seguridad infrarrojos	61.47 €	15	922.05 €
Cerradura electrónica para CPD	117 €	1	117 €
Detector de inundaciones	51.90 €	5	259.5 €

Cuadro A.3.: Presupuesto Infraestructuras

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.

Producto	Precio	Cantidad	Total
Seguro	730 (mes)	12	8760
Alquiler sala externa para copias	362 (mes)	12	4344

Cuadro A.4.: Presupuesto Servicios

A.5. Infraestructuras Comunicaciones

Presupuestos para los materiales de infraestructuras de comunicaciones:

Producto	Precio	Cantidad	Total
Router Cisco 7201	11.859,90 €	1	11.859,90 €
Cisco Small Business RVL200 SSL/IPSec VPN Router	173,96 €	2	347,92 €
SMC Networks SMC SMC8624T-V.1-INT SWITCH GIGABIT GESTIONABLE LAYER 2 DE 48 PU	1297,63 €	4	5190,52 €
Continúa en la siguiente página			

Continúa de la página anterior			
Seguro (precio mensual)	1	730	
Access point Cisco 1330	510,00 €	9	4590 €
SAIs MGE UPS Systems Pulsar 2200	2467,00 €	4	9868 €
Firewall Cisco ASA 5505 10-User Bundle	527,64 €	15	527,64 €

Cuadro A.5.: Presupuesto Infraestructuras

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. Plantilla de Solicitud de modificación en la política de seguridad

Bodegas San Dionisio, S.A.

AL COMITÉ DE DIRECCIÓN EJECUTIVA

DE: [Director o Responsable de Seguridad]

Solicitud de modificación en la política de seguridad de la información de Bodegas San Dionisio, S.A.

Descripción de la modificación que se solicita:
Escriba aquí la descrípción

Razón o razones para el cambio que se solicita:
Escriba aquí la razón

Enumeración de referencias legales o de normativas estándar que justifican o obligan la realización del cambio:
Escriba aquí las referencias

Fecha límite para la realización del cambio, en caso de que se requiera:
Fecha

Enumeración de referencias legales o de normativas estándar que justifican o obligan la realización del cambio:
Escriba aquí las referencias

Descripción breve de los cambios organizativos y/o técnicos que supone el cambio. (Se anexa descripición detallada):
Escriba aquí los cambios

Cantidad estimada del coste en Euros que supone el cambio. (Se anexa presupuesto detallado):
Escriba aquí la cantidad

En , a de de .

[NOMBRE Y FIRMA]

Bibliografía

[1] (2010, 5) Orden de 13 de mayo de 2010, por la que se aprueba el reglamento de las denominaciones de origen «jerez-xérès-sherry» y «manzanilla de sanlúcar de barrameda», así como sus correspondientes pliegos de condiciones. BOJA, n. 103 del 28 de Mayo de 2010. Junta de Andalucía. [Online]. Available: http://www.juntadeandalucia.es/boja/boletines/2010/103/d/23.html

[2] *Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.*, ISO/IEC 17799:2000, UNE-ISO/IEC.

[3] *Building an Information Technology Security Awareness and Trining Program*, NIST Special Publication 800-50, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.