DOCUMENTO DE SEGURIDAD
Según RLOPD

EMPRESA: **Benitez y Asocidos para la Gestion S.L.**
Fecha de actualización: 12/05/2011

DOCUMENTO DE SEGURIDAD

EMPRESA: Benitez y Asociados para la Gestion S.L.
Fecha de actualización: 12/05/2011

1. ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Benitez y Asociados para la Gestion S.L., incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

NIVEL ALTO: Se aplicarán a los ficheros o tratamientos de datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas;
- derivados de actos de violencia de género.

NIVEL MEDIO: Se aplicarán a los ficheros o tratamientos de datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito);
- de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social;
- que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas;
- de los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

NIVEL BASICO: Se aplicarán a cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la unica finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesoria, que no guarden relación con la finalidad del fichero;
- en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

Ficheros	**Automatizado**	**Nivel de seguridad**
Fichero manual de clientes y p	No	Bajo
Fichero Manual de RRHH	No	Bajo
Datáfono	Si	Bajo

En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

2. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO.

IDENTIFICACIÓN Y AUTENTICACIÓN

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales.

Ficheros Automatizados

Normativa de identificación y autenticación de los usuarios con acceso a los datos personales de la empresa:

Nombre y apellidos	**Usuario**	**Departamento**
Benitez y Asociados para la Gestion S.L.	Empresa	Empresa
José Vicente Benitez Baute	Vicente	Administración

A cada usuario se le asigna una contraseña genérica para entrar por primera vez a los diferentes ficheros automatizados para los que se le ha autorizado previamente por el responsable. Cuando entra en la aplicación ésta le obligará a cambiar la contraseña por una personal. Dicha contraseña la custodia el usuario.

El usuario deberá modificar su contraseña personal al menos cada 6 meses, transcurrido este plazo sin realizar el cambio la contraseña quedará invalidada.

Las contraseñas deberán cumplir los siguientes requisitos mínimos:

- Mínimo de 6 caracteres alfanuméricos.
- Combinar números y letras.
- Combinar mayúsculas y minúsculas.

En los ficheros de nivel medio y alto que se especifican en el anexo I está limitada la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

CONTROL DE ACCESO

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados, especificando nivel de acceso y limitando los permisos en los ficheros automatizados y guardando bajo llave los manuales.

Exclusivamente el responsable del fichero y el encargado de tratamiento están autorizados para conceder, alterar o anular el acceso sobre los datos y los recursos, conforme a los criterios establecidos por el responsable del fichero.

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cuando se produzcan cambios en los usuarios, bajas o nuevas incorporaciones.

De existir personal ajeno al responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

NIVEL ALTO: REGISTRO DE ACCESOS

Ficheros Automatizados

En los accesos a los datos de los ficheros de nivel alto que se especifican en el anexo I de este documento, se registrará por cada acceso la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se almacenará también la información que permita identificar el registro accedido.

Los datos del registro de accesos se conservaran durante al menos dos años.

El responsable de seguridad revisará al menos una vez al mes la información de control registrada y elaborará un informe especificando el resultado de las revisiones realizadas y los problemas detectados.

No será necesario el registro de accesos cuando:

- el responsable del fichero es una persona física,
- el responsable del fichero garantice que sólo él tiene acceso y trata los datos personales,
- se haga constar en el documento de seguridad.

GESTIÓN DE SOPORTES Y DOCUMENTOS

Los soportes que contienen datos de carácter personal pueden permitir identificar el tipo de información que contienen, ser inventariados y son almacenados en un lugar de acceso restringido al que solo tienen acceso las personas con autorización según se especifica en el anexo I.

El inventario de soportes se especifica en el anexo V.

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos en correos electrónicos, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del fichero o aquel en que se hubiera delegado, con un documento firmado por éste, autorizando la salida de los soportes y documentos correspondientes o la entrega de los soportes móviles necesarios para el desempeño de las funciones del usuario (portátil, teléfono, capturadotes, etc.).

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

Los soportes que vayan a ser desechados, deberán ser previamente destruidos o eliminados de forma que no sea posible el acceso a la información contenida en ellos o su recuperación posterior.

En el traslado de la documentación se adoptarán las siguientes medidas de seguridad para evitar la sustracción, pérdida o acceso indebido a la información:

- Los portátiles y el resto de dispositivos móviles con datos personales estarán protegidos por claves de acceso siguiendo los procedimientos de asignación y control estipulados en este documento.

- La documentación en papel se trasladará en sobres cerrados.

Ficheros Automatizados

NIVEL MEDIO: REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

Las salidas y entradas de soportes correspondientes a los ficheros de nivel alto y medio especificados en el anexo I, serán registradas de acuerdo al siguiente procedimiento:

El registro de entrada y salida de soportes se gestionará mediante la aplicación informática de gestión de la LOPD "TGT lopd", en el que constan los siguientes campos:

Registro de entrada: Identificador, la fecha y hora, el emisor, descripción de soportes, el tipo de información que contienen, la

forma de recepción y la persona autorizada responsable de la recepción.

Registro de salida: Identificador, la fecha y hora, el receptor, descripción de soportes, el tipo de información que contienen, la forma de envío y la persona autorizada responsable de la envío.

Ficheros Automatizados

NIVEL ALTO: GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Los soportes de nivel alto especificados en el anexo I, se identificarán mediante un sistema de etiquetado comprensibles y con significado para los usuarios con acceso autorizados, permitiéndoles identificar su contenido y dificultando la identificación para el resto de personas.

La La distribución y salida de soportes que contengan datos de carácter personal de los ficheros de nivel alto especificados en el anexo I de este documento, se realizará cifrando los datos. Igualmente se cifrarán los datos que contengan los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable.

Ficheros Manuales

CRITERIOS DE ARCHIVO

El archivo de los soportes o documentos se realizará de acuerdo con los criterios que en cualquier caso garanticen la correcta conservación de los documentos, la localización y consulta de la información y posibiliten el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Ficheros Manuales

ALMACENAMIENTO DE LA INFORMACIÓN

Los documentos con datos personales se guardarán en muebles, archivadores o habitaciones con llave, teniendo acceso a ellos exclusivamente las personas autorizadas.

NIVEL ALTO: Los elementos de almacenamiento (armarios, archivadores o habitaciones) respecto de los documentos con datos personales, se encuentran en las instalaciones de la empresa cerrados con llave. Estos lugares permanecerán cerrados en tanto no sea preciso el acceso a los documentos.

Ficheros Manuales

CUSTODIA DE SOPORTES

En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamientos indicados en el punto anterior, por estar en proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso a personas no autorizadas.

ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizarán un nivel de seguridad equivalente al exigido para los accesos en modo local.

Ficheros Automatizados

NIVEL ALTO: Los datos personales correspondientes a los ficheros de nivel alto especificados en el anexo I de este documento,

que se transmitan a través de redes públicas o inalámbricas de comunicaciones electrónicas se realizará cifrando previamente estos datos.

RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DE LA UBICACIÓN DEL FICHERO

Tratamientos de datos personales fuera de locales del responsable:

Los ficheros tratados en dispositivos portátiles y sus usuarios se especifican en inventario de soportes especificado en el anexo V de este documento.

Ficheros Manuales

TRASLADO DE DOCUMENTACIÓN

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse las medidas necesarias orientadas a impedir el acceso o manipulación de la información objeto de traslado.

FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Ficheros Manuales

NIVEL ALTO

COPIA O REPRODUCCIÓN

La realización de copias o reproducción de los documentos con datos personales sólo se podrán realizar bajo el control del responsable del fichero correspondiente.

Las copias desechadas deberán ser destruidas imposibilitando el posterior acceso a la información contenida utilizando para ello destructoras de documentos o en su defecto procedimientos similares.

Ficheros automatizados

COPIAS DE RESPALDO Y RECUPERACIÓN

Se realizarán copias de respaldo, salvo que no se hubiese producido ninguna actualización de los datos, como mínimo una vez a la semana.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

El responsable del fichero verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos.

Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

En el Anexo III se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

NIVEL ALTO: En los ficheros de nivel alto especificados en el Anexo III, se conservará una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de donde se encuentran los sistemas informáticos que los tratan, y deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información de forma que sea recuperable.

NIVEL MEDIO: RESPONSABLE DE SEGURIDAD

Se designa como responsable de seguridad José Vicente Benitez Baute que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una exoneración de la responsabilidad que corresponde a Benitez y Asociados para la Gestion S.L. como responsable del fichero de acuerdo con el RLOPD.

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

3. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento: se les entrega un documento con la información correspondiente.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

FUNCIONES Y OBLIGACIONES DE CARÁCTER GENERAL.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar a ;Benitez y Asociados para la Gestion S.L. las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en el apartado de "Procedimientos de notificación, gestión y respuesta ante las incidencias".

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los soportes que los contengan, o a los recursos del sistema de información.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto de aquellos datos que hubiera podido conocer durante la prestación del servicio.

5. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de Benitez y Asociados para la Gestion S.L..

El procedimiento a seguir para la notificación de incidencias será: la incidencia la comunica el usuario del fichero en el que se produce al responsable del fichero o a quien éste le haya delegado sus competencias.

El registro de incidencias se gestionará mediante la aplicación informática de gestión de la LOPD "TGT lopd".

Ficheros Automatizados

NIVEL MEDIO: En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros de nivel medio y alto.

NIVEL MEDIO: Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

6. PROCEDIMIENTOS DE REVISIÓN

REVISIÓN DEL DOCUMENTO DE SEGURIDAD

El documento de seguridad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información, en el contenido de la información incluida en los ficheros o como consecuencia de los controles periódicos realizados. En todo caso se entenderá como cambio relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

NIVEL MEDIO:AUDITORÍA

La auditoría externa que verifique el cumplimiento del Título VIII del RLOPD, referente a las medidas de seguridad, según lo indicado en sus artículos 96 y 110 respecto de ficheros automatizados y no automatizados respectivamente, se realizará como mínimo una vez cada dos años.

Con carácter extraordinario deberá realizarse cuando se lleven a cabo modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas, con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado.

El informe analizará la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias.

Los informes de auditoría han de ser analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras y quedará a disposición de la Agencia Española de Protección de Datos, o en su caso de las autoridades de control de las comunidades autónomas.

ANEXO I

DESCRIPCIÓN DE FICHEROS

Actualizado a: 12/05/2011

Nombre de Fichero	Fichero manual de clientes y p
Descripción	Copia de facturas, presupuestos y base de datos de clientes y proveedores.
Nombre comercial	Fichero manual de clientes y proveedores
Responsable de fichero o tratamiento	Empresa
Encargado del tratamiento	Empresa
Nivel	Bajo
Automatizado	No
Usuarios	Empresa,Vicente

Nombre de Fichero	Fichero Manual de RRHH
Descripción	Nóminas, presupuestos y datos de los empleados.
Nombre comercial	Fichero Manual de RRHH
Responsable de fichero o tratamiento	Empresa
Encargado del tratamiento	Empresa
Nivel	Bajo
Automatizado	No
Usuarios	Empresa,Vicente

Nombre de Fichero	Datáfono
Descripción	Gestión de cobro
Nombre comercial	Datáfono
Responsable de fichero o tratamiento	Empresa
Encargado del tratamiento	Empresa
Nivel	Bajo
Automatizado	Si
Usuarios	Empresa,Vicente

La relación de Ficheros y Usuarios se mantiene de forma informatizada en la aplicación de gestión de la LOPD "TGT lopd".

ANEXO II

NOMBRAMIENTOS

Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad.

ANEXO III

AUTORIZACIONES DE SALIDA O RECUPERACIÓN DE DATOS

Adjuntar original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos.

Procedimiento	**Frecuencia**	**Tipo de procedimiento**	**Automatizado**
Envio de datos	Mensual	Extracción de datos	No
Recepción de datos	Mensual	Recuperación de Datos	No

ANEXO IV

DELEGACIÓN DE AUTORIZACIONES

Especificar, en su caso, las personas en las que el responsable del fichero ha delegado Indicar las autorizaciones, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte papel, etc.

Fecha	**Fichero**	**Responsable**	**Delegado**	**Accion**

ANEXO V

INVENTARIO DE SOPORTES

Si el inventario de soportes se gestiona de forma manual recoger en este anexo la información al efecto, según lo indicado en el apartado de "Gestión de soportes y Documentos" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento.

Fecha	12/05/2011					
Tipo de soporte	Nombre	N sr	Ubicacion	Usuario principal	Fichero	Autom
Otros	Datáfono		Mostrador	Empresa	Datáfono	Si
Mobiliario	Archivador		Oficina	Empresa	Fichero manual de clientes y Fichero Manual de RRHH	Si

ANEXO VI

REGISTRO DE INCIDENCIAS

El registro de incidencias se lleva de forma automatizada en la aplicación informática de Gestión de la LOPD "TGT Lopd".

ANEXO VII

ENCARGADOS DE TRATAMIENTO

Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, y que no los comunicarán, ni siquiera para su conservación a otras personas.

El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento esta obligado a implementar.

Ejemplos:

- Asesoría Laboral y/o Fiscal
- Servicios de Informática
- Empresas de mensajería
- Etc.

Nombre del Negocio	**CIF**	**CP**			**responsible**	**dni**
Benitez y asociados para la gestión S.L.	B38421939	38650	Santa Cruz de Tenerife	Asesoría fiscal contable	José Vicente Benitez Daute	42087862R
Laboralia Plus S.L.U.	_____	38631	Santa Cruz de Tenerife	Asesoría Laboral	_____	_____

Provincia **Actividad**

ANEXO VIII

REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

El registro de entrada y salida de soportes se gestiona de forma automatizada a través de la aplicación de gestión de la LOPD "TGT lopd".