Sistema de Gestión Integrado

POLÍTICA DE SEGURIDAD

Documento de uso interno

CONTROL DE VERSIONES

Revisión	Fecha	Motivo del Cambio
0.1	24/02/2017	Tras la integración con la ISO 9001, se convierte la Política de seguridad en manual de gestión, y se crea este documento para recoger las medidas concretas de seguridad.
1.1	29/05/2017	Revisión, corrección de errores

Realizado y revisado Miguel Gómez Laguna Fdo. Fecha 29/05/2017	Aprobado Comité de Gestión Fdo. Fecha 6/06/2017

Contenido

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1. Gestión de Activos

1.1.1. Responsabilidades asociadas a los activos

Para gestionar correctamente los activos el Responsable de Seguridad mantendrá un inventario actualizado de los activos importantes.

En este inventario se registrará quién es el propietario del activo. Esta responsabilidad será asignada al responsable del área ó departamento de SPAI INNOVA donde esté ubicado física o lógicamente el activo.

1.1.2. Clasificación de la información

La clasificación de la información será de acuerdo con la siguiente escala:

Confidencial	Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización
Uso Interno	Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
Pública	Información sin ninguna necesidad de restringir el acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización.

Existirá una relación de cada tipo de documento existente en SPAI INNOVA con la clasificación que le corresponde (Confidencial/Uso Interno/Público). El personal de SPAI INNOVA tendrá conocimiento de esta clasificación de manera que sepan en todo momento el tipo de información que utilizan, sin necesidad de establecer un marcado de la misma, no revelando así a fuentes externas la clasificación de la información. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el Responsable de Seguridad y con su colaboración si es necesaria.

La clasificación de la información se desarrolla en el Anexo II del presente documento.

1.2. Seguridad de la Gestión de los Recursos Humanos

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

La contratación de personal pasa por un proceso de selección en el que deben revisarse las referencias y antecedentes siempre que sea posible.

En las condiciones de la relación laboral deberán quedar reflejadas las responsabilidades del empleado en materia de seguridad de la información. Esta responsabilidad continuará durante un tiempo establecido tras la finalización del contrato.

Se requerirá la firma de un acuerdo de confidencialidad para todos los empleados para evitar la divulgación de información secreta.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede. Se realizarán periódicamente seminarios para que el personal conozca los procesos y tareas que deben realizar en materia de seguridad.

Los empleados que infrinjan las normas de Seguridad pueden ser sancionados por un proceso disciplinario de acuerdo con el convenio general.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

1.3. Seguridad Física y del Entorno

Para que una seguridad lógica sea efectiva es primordial que las instalaciones de SPAI INNOVA mantengan una correcta seguridad física para evitar los accesos no autorizados así como cualquier otro tipo de daño o interferencia externa.

1.3.1. Áreas Seguras

- SPAI INNOVA tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.
- La totalidad de las oficinas de SPAI INNOVA cuentan con las barreras físicas necesarias para asegurar los recursos que éstas alberguen.
- Los lugares donde se ubican el servidor y el cableado estarán cerrados bajo llave y sólo tendrán acceso las personas autorizadas y los proveedores de servicios cuando vayan acompañados por alguien autorizado.
- Las ventanas y puertas deberán permanecer cerradas cuando las instalaciones estén vacías.
- Las instalaciones de SPAI INNOVA están dotadas de dispositivos de extinción de incendios marcados por la legislación vigente en esa materia. En este sentido, se dispone de extintores y salidas de emergencia debidamente señalizados.
- Se prohíbe expresamente al personal comer y beber cerca de los servidores y equipos informáticos. Así mismo, se tendrá especial cuidado con el manejo de cualquier producto que pueda verterse sobre activos de información.
- Para la prevención de fugas de agua e inundaciones será necesaria la revisión periódica de la grifería, sanitarios y demás instalaciones que puedan causar daños de este tipo.

1.3.2. Seguridad de los equipos

- Los equipos informáticos son un activo importante del que depende la continuidad de las actividades de la organización, por lo que serán protegidos de manera adecuada y eficaz.
- Tanto los puestos de usuario como los servidores están protegidos contra posibles fallos de energía u otras anomalías eléctricas, para ello se han instalado equipos de alimentación ininterrumpida.
- Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado de forma para que mantengan la confidencialidad, integridad y sobre todo la disponibilidad de la información. Para ello deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación. También será necesario adoptar las medidas de precaución necesarias en caso de los equipos deban abandonar las instalaciones para su mantenimiento.
- La eliminación de equipos sólo se llevará a cabo por el Responsable de Seguridad o personal en el que éste delegue.

1.4. Gestión de comunicaciones y operaciones

1.4.1. Procedimientos Operativos y Responsabilidades

SPAI INNOVA controlará el acceso a los servicios en redes internas y externas y se asegurará de que los usuarios no ponen en riesgo dichos servicios. Para ello deberá establecer las interfaces adecuadas entre la red de SPAI INNOVA y otras redes, los mecanismos adecuados de autenticación para usuarios y equipos, y los accesos para cada usuario del sistema de información.

Para evitar un uso malicioso de la red de SPAI INNOVA existirán mecanismos para cubrir los servicios en red a los que se puede acceder, los procedimientos de autorización para establecer quién puede acceder a que recursos de red y los controles de gestión para proteger los accesos a la red.

Todos los trabajadores autorizados para el manejo de información automatizada deberán estar registrados como usuarios del sistema de información. Cada vez que accedan al sistema de información deberán validarse con su nombre de usuario, que será único e intransferible, y su contraseña personal.

Para asegurar la operación correcta y segura de los sistemas de información, los procedimientos de operación estarán debidamente documentados y se implementarán de acuerdo a estos procedimientos. Estos procedimientos serán revisados y convenientemente modificados cuando haya cambios significativos en los equipos o el software que así lo requieran.

1.4.2. Gestión de los Servicios Suministrados por Terceros

SPAI INNOVA al contratar un servicio externo para gestionar activos de información introduce en el proceso nuevas vulnerabilidades, ya que los recursos se exponen a posibles daños, pérdidas o filtraciones de información. Por todo ello será necesario tomar una serie de precauciones que aseguren el perfecto uso de la información de SPAI INNOVA.

Antes de contratar un servicio externo para la gestión de la información, SPAI INNOVA identificará los riesgos que esta situación conlleva y elaborará un acuerdo en el que se traten las siguientes cuestiones: qué aplicaciones se mantienen en SPAI INNOVA por su especial criticidad, la aprobación de los propietarios de la aplicación, qué implicaciones tiene el contrato para los planes de continuidad del negocio, las normas de seguridad y cómo se medirá su eficacia, quiénes son los responsables y qué procedimientos especiales se seguirán para monitorizar las actividades importantes de seguridad, quién y cómo manejará las incidencias de seguridad y mediante qué procedimientos se informará a SPAI INNOVA de esas incidencias.

1.4.3. Protección frente a código malicioso y código móvil

Queda totalmente prohibida la instalación de otro software que no sea el permitido y necesario para el desarrollo del trabajo por parte del personal de SPAI INNOVA.

Todo software adquirido por la organización sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera, vigilando los diferentes tipos de licencias.

Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado por la Dirección.

El Responsable de Seguridad supervisará la instalación de las herramientas informáticas adecuadas para la protección de los sistemas contra virus, gusanos, troyanos, etc. y los usuarios deberán seguir las directrices que se les indiquen para proteger los equipos, aplicaciones e información con los que trabajan.

1.4.4. Copias de Seguridad

Los datos deben ser guardados en un directorio de la red para asegurar que se realizan copias de seguridad habitualmente.

Habrá procedimientos para la realización de copias de seguridad que se archivarán para recuperar los datos en caso de incidencia. Estas copias estarán claramente identificadas y se guardarán en sitio seguro, preferiblemente fuera de las instalaciones de la organización.

También se desarrollarán procedimientos para recuperar los datos a partir de las copias de seguridad. Hay que asegurarse periódicamente de que la información se guarda correctamente y permite recuperar un nivel mínimo de servicio en caso necesario.

Si se corrompe la información en operación, hay que comprobar el software, el hardware y las comunicaciones implicadas antes de utilizar las copias de seguridad, para asegurarse de que no se pueda corromper la información contenida en ellas también.

1.4.5. Gestión de la seguridad de la red

Todos los equipos informáticos (estaciones de trabajo y el servidor...) que estén o sean conectados a la red, o aquellos que en forma autónoma se tenga y que sean propiedad de SPAI INNOVA deberán estar sujetos a las normas y procedimientos de instalación que emite el departamento de Informática y que han sido ratificados previamente por la Dirección.

Los elementos de red (switch, router, etc.) permanecerán fuera del acceso del personal no autorizado para evitar usos malintencionados que puedan poner en peligro la seguridad de del sistema.

1.4.6. Gestión de Soportes

Los usuarios aplicarán las mismas medidas de seguridad a los soportes que contengan información sensible que a los ficheros de donde han sido extraídos.

Los soportes (tanto papel como lógicos) que contengan información sensible deben permanecer en cajones o armarios cerrados bajo llave. Cuando alguna persona autorizada deba utilizarla para realizar alguna gestión relacionada con las labores propias de la empresa, ésta se hará responsable del buen cuidado de los soportes. No los dejará encima de su mesa cuando abandone su puesto de trabajo ni los colocará en cualquier otro lugar donde una persona sin autorización pueda verlos o apropiarse de ellos.

Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas. Algunos procedimientos de destrucción que se consideran adecuados son la incineración, el triturado o vaciamiento de los soportes para que sean usados en otra aplicación dentro de SPAI INNOVA.

Siempre será necesario registrar la eliminación de soportes que contengan información sensible para mantener una pista de auditoría.

1.4.7. Intercambio de Información

Se establecerán procedimientos para proteger la información que se intercambie a través de cualquier medio de comunicación (electrónico, verbal, fax, etc.).

1.4.8. Seguimiento

Según se considere necesario, se establecerán los mecanismos necesarios que permitan detectar actividades de proceso de información no autorizadas. Esto implicará realizar tareas para llevar a cabo controles e inspecciones de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y los procedimientos operativos así como para recomendar cualquier cambio que se estime necesario.

1.5. Control de Accesos

1.5.1. Requisitos del negocio para el control de accesos

La información debe estar protegida contra accesos no autorizado.

Cada responsable de departamento o área definirá las necesidades de acceso a la información a dos niveles, para el conjunto del departamento o área y las de cada usuario dentro del conjunto. Sólo se facilitará el acceso a la información necesaria para el trabajo a desarrollar.

En el caso de que visitantes o personal no autorizado acceda a las instalaciones o a la información de SPAI INNOVA deberá ir siempre acompañado por un miembro responsable de SPAI INNOVA que controlará en todo momento que la seguridad de los recursos está garantizada.

1.5.2. Gestión de accesos de los usuarios

El Responsable de Informática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos, así como el acceso lógico especializado de los recursos (servidores, enrutadores, bases de datos, etc.) conectados a la red.

Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

1.5.3. Responsabilidades del usuario

Los puestos de trabajo del personal deben estar despejados de papeles y otros medios de almacenamiento de la información para reducir los riesgos de acceso no autorizado así como otros posibles daños. Éstos deberían guardarse en espacios cerrados adecuados, especialmente fuera del horario laboral.

De igual forma, es necesario configurar los equipos informáticos para que éste quede bloqueado cuando el usuario no se encuentra en su puesto de trabajo de forma que sea necesario introducir una contraseña para acceder a los datos que se almacenan en el terminal.

También deben protegerse los puntos de entrada y salida de correo, las máquinas de fax y las impresoras que no se encuentren atendidas por alguna persona de SPAI INNOVA.

1.5.4. Control de acceso a la red

No se permitirá el acceso a la red, a los sistemas, aplicaciones o información a ningún usuario que no esté formalmente autorizado para ello.

En el caso de proveedores de servicios o entidades externas, que necesiten acceder a ellos por un motivo justificado, se requiere que firmen acuerdos de confidencialidad con la organización para mantener el mismo nivel de seguridad que si fueran empleados de SPAI INNOVA.

El Responsable de Seguridad controlará las altas y bajas de todos los usuarios.

1.6. Gestión de incidentes

Cualquier empleado que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia.

Se establecerán responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a los eventos en materia de seguridad.

El registro de incidencias servirá de base para identificar riesgos nuevos y para comprobar la eficacia de los controles implantados.

1.7. Continuidad del negocio

Es imprescindible para SPAI INNOVA establecer las pautas de actuación a seguir en caso de que se produzca una interrupción de las actividades del negocio por fallos graves en la seguridad o desastres de cualquier tipo.

Para garantizar la continuidad del negocio en estos casos, SPAI INNOVA establecerá planes de contingencia que permitan la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del negocio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del negocio se documentará, partiendo de los riesgos detectados y de los controles definidos en consecuencia que deberán probarse y actualizarse regularmente para comprobar su idoneidad.

La gestión de la continuidad del negocio se incorporará a los procesos de SPAI INNOVA y será responsabilidad de una o varias personas dentro de la empresa.

2. Anexo I: Política de uso aceptable

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios. No se considera aceptable:

- La creación o transmisión de material infringiendo las leyes de protección de datos o de propiedad intelectual.
- Instalar, modificar o cambiar la configuración de los sistemas de software (sólo los administradores de sistemas están autorizados a ello).
- El uso de Internet para fines personales (incluido el correo electrónico personal basado en Web) se limitará a los tiempos de descanso autorizados. Cualquier transacción electrónica personal que se realice será bajo la responsabilidad del usuario.
- Facilitar el acceso a las instalaciones o los servicios a personas no autorizadas deliberadamente.
- Malgastar los recursos de la red o los sistemas de manera premeditada.
- Corromper o destruir datos de otros usuarios o violar su privacidad intencionadamente.
- Introducir virus u otras formas de software malicioso adrede. Antes de utilizar cualquier medio de almacenaje de información, se deberá comprobar que esté libre de virus o similares.
- Revelar las contraseñas y los medios de acceso voluntariamente.
- Utilizar los equipos para lucro personal.
- La creación, utilización o transmisión de material ofensivo, obsceno o que pueda causar molestar u ofender.
- Enviar mensajes de correo muy grandes o a un grupo muy numeroso de personas (que pueda llegar a saturar las comunicaciones).
- No verificar que los correos están libres de virus.

Asimismo, los usuarios deberán de tener en cuenta las siguientes medidas de seguridad, durante el tratamiento de la información y el uso de los sistemas de TI:

- Cualquier persona que sospeche u observe una incidencia de seguridad, bien sea física (fuego, agua, etc.), de software o sistemas (virus, desaparición de datos, etc.) o de servicios de soporte (comunicaciones, electricidad, etc.) debe comunicarlo inmediatamente al Responsable de Seguridad para que tome las medidas oportunas y registre la incidencia
- Cada equipo informático de usuario/a estará bajo la responsabilidad de algún usuario/a autorizado/a que tratará de proteger, en la medida de sus posibilidades, la confidencialidad de la información de la empresa y, especialmente de los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o cualquier otra manipulación o uso indebido.
- Cuando la persona responsable de un equipo informático lo abandone temporalmente deberá dejarlo en un estado que impida la visualización de los datos protegidos, por ejemplo, a través de un protector de pantalla. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente. Si el abandono del equipo se produjera debido a la finalización de su turno de trabajo, el usuario o usuaria procederá al cierre completo de la sesión del sistema.
- Se deben retirar de las impresoras y demás periféricos de salida todos los documentos que contengan información de la empresa conforme se vayan imprimiendo.

- Ningún usuario o usuaria podrá utilizar dispositivos extraíbles (CD, DVD, USB, etc.) ni almacenar información en ellos, sin la previa autorización del Responsable de Seguridad.
- Los soportes que contengan información deberán estar claramente identificados con una etiqueta externa que indique (directa o indirectamente) de qué fichero se trata y qué tipo de datos contiene.
- Se deberán guardar los soportes que contengan información en lugar seguro y bajo llave, o en salas, despachos,… con acceso restringido, cuando no sean usados, especialmente fuera de la jornada laboral.
- Ningún usuario o usuaria debe instalar ni ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar cualquiera de los recursos informáticos. En ningún caso podrán instalar copias ilegales o irregulares de programas, ni borrar ninguno de los programas instalados legalmente.
- Queda terminantemente prohibido la modificación de la configuración de cualquier software ya sea sistema operativo o aplicaciones, establecida, por defecto, en el equipo informático por el Responsable de Seguridad, sin su previa autorización.
- El uso del correo electrónico e Internet debe limitarse a las funciones propias del puesto de trabajo.
- No se debe de responder a correos falsos, ni a cadenas de correos para evitar que la dirección de correo electrónico se difunda. Tampoco se deben abrir ficheros adjuntos sospechosos procedentes de desconocidos o que no se hayan solicitado.
- Si se detectan virus en los archivos o correos recibidos o durante la navegación por Internet, hay que ponerlo en conocimiento del Responsable de Seguridad.
- Se asignarán contraseñas a todos los usuarios del sistema como medio de validación de su identidad. El procedimiento de asignación de contraseñas se realiza mediante la entrega personal por parte del Responsable de Informática, que es el encargado de comunicar el usuario y la clave para el acceso a los sistemas.
- La contraseña estará compuesta por un mínimo de 6 caracteres, (combinando caracteres alfabéticos y numéricos) y no se deberá revelar mediante ningún concepto, ni se deberá mantener por escrito o a la vista de terceras personas.
- Es recomendable cambiar las contraseñas con una periodicidad trimestral. Asimismo es necesario que los equipos dispongan de protectores de pantalla que se activen a los diez minutos de inactividad, siendo necesario una contraseña de desbloqueo.
- La contraseña no debe contener el identificador o nombre de usuario de la cuenta, o cualquier otra información personal que sea fácil de conocer (cumpleaños, nombres de hijos, cónyuges, etc.). Tampoco una serie de letras dispuestas adyacentemente en el teclado (123456, QWERTY, etc.).
- No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea. Si alguna de ellas queda expuesta, todas las demás cuentas protegidas por esa misma contraseña también deberán considerarse en peligro.
- No compartir las contraseñas en Internet, por correo electrónico ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que te soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla.

- Si un usuario o usuaria tiene sospecha fundada de que su acceso autorizado está siendo o puede ser utilizado por otra persona, estará obligado a cambiar su contraseña para lo cual contactará con el Responsable de Seguridad o Informática, para comunicar la incidencia.
- No se podrá utilizar ningún acceso autorizado de otro usuario o usuaria, aunque lo autorice la persona propietaria.
- Ningún usuario debe intentar acceder a áreas restringidas de los sistemas de información propios o de terceras personas, distintos de los que le hayan sido asignados.

Los equipos portátiles y teléfonos móviles serán asignados por SPAI INNOVA. Existirá un inventario actualizado de los equipos portátiles y móviles. SPAI INNOVA será la unidad encargada de gestionar dicho inventario.

- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de SPAI INNOVA. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas. La sustracción de estos equipos se ha de poner inmediatamente en conocimiento de SPAI INNOVA para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de SPAI INNOVA.
- Los usuarios de estos equipos se responsabilizarán de que no sean usados por terceras personas ajenas a SPAI INNOVA o no autorizadas para ello.
- Los dispositivos móviles requerirán la autenticación de los usuarios para el acceso a los mismos, así como a las aplicaciones instaladas.
- En general, los equipos portátiles no deberán conectarse directamente a redes externas (incluyendo la red o el acceso a Internet del usuario en su domicilio). En casos debidamente justificados y previamente autorizados por SPAI INNOVA se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.
- Se utilizará software adicional que permita la protección de los dispositivos mediante el uso de sistemas antivirus, así como acciones como la localización y borrado remoto, ante la pérdida de los mismos.

3. Anexo II: Clasificación de la información

La clasificación de la información será de acuerdo con la siguiente escala:

Confidencial	Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias serias para la organización
Uso Interno	Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
Pública	Información sin ninguna necesidad de restringir el acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización.

Los empleados conocerán esta clasificación y el tipo documentación con la que trabajan. Para transmitir la información confidencial por cualquier medio se necesita la aprobación expresa del responsable del activo. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el Responsable de Seguridad y con su colaboración si es necesaria.

Cuando un usuario detecte alguna desviación respecto a las medidas de seguridad definidas para cada tipo de documento, o disponga de acceso a información a la que no esté autorizado, deberá de considerarlo como una incidencia de seguridad, y proceder según el procedimiento definido.

Tipo de documento	Clasificación	Descripción	Requisitos de Seguridad	Usuarios Autorizados	Responsable
Documentación de RRHH	C	Información en soporte papel, y mediante documentos automatizados perteneciente a los trabajadores y referente a los servicios de RRHH: nóminas, contratos, curriculums, etc.	Automatizada: Se realizarán copias de seguridad al menos semanalmente por el Responsable de Sistemas. Esta documentación se depositará en el servidor SYNOLOGY, en una carpeta denominada LABORAL, de acceso exclusivo a usuarios autorizados. Además para el acceso a esta carpeta, se requerirá autenticación de los usuarios mediante nombre de usuario y contraseña individual.	Acceso exclusivo a dirección y recursos humanos.	Jefe de Administración
			Soporte papel: La información se archivará en el departamento de Administración, en armarios o archivadores con acceso exclusivo y que dispongan de mecanismos		

			de apertura (llave).		
Documentación Clientes	U.I.	Documentación en papel y digitalizada de los clientes.	Automatizada: Esta información se encuera alojada dentro de la base de datos que maneja el software de Gestión Contable. Dicha base de datos está en el servidor VM-CONTABILIDAD. Se requerirá autenticación de los usuarios mediante nombre de usuario y contraseña individual. La información se respaldará con periodicidad diaria incremental y semanal completa por el Responsable de Sistemas	Todo el personal interno	Jefe de Administración

			Soporte papel: La información se archivará en armarios o archivadores con acceso exclusivo y que dispongan de mecanismos de apertura (llave), en el área de Administración.		
Información Pública / Comercial	P	Contenido web, folletos informativos, trípticos informativos, orientados a clientes y potenciales clientes	De manera automatizada (web, …), será modificada exclusivamente por personal autorizado. Se respaldará la información al menos semanalmente de forma completa por el Responsable de Sistemas. Se encuentra ubicada en el servidor SYNOLOGY. Respecto a los mails de contenido comercial, se encuentras alojados en los equipos de usuarios. Se respaldarán semanalmente de forma completa, por el Responsable de sistemas	Todo el personal	Comercial

			Soporte papel: La información se archivará en armarios o archivadores en el área Comercial.		