ECOLOGICAL MAILING S.L.

ANEXO I: POLÍTICA DE SEGURIDAD

ISO 27001

ÁGORA CONSULTORES
15/09/2014

v.1.1

1. Política general de seguridad para todos los empleados

Todo personal que trabaje en ECOLOGICAL MAILING S.L o tenga acceso a la información deberá cumplir con las siguientes normas de actuación:

1. Proteger la información confidencial perteneciente o cedida por terceros a ECOLOGICAL MAILING S.L. de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
2. Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
3. Para obtener el acceso a los sistemas de información propios o bajo supervisión de ECOLOGICAL MAILING S.L. será necesario disponer de un acceso autorizado.
4. Será necesario conocer, aceptar y cumplir las presentes políticas antes de poder acceder a los sistemas de información de ECOLOGICAL MAILING S.L.

2. Políticas generales para personal específico

De forma adicional, todo el personal con responsabilidades específicas dentro del ámbito de actuación indicado deberá asegurarse de que se cumplen las siguientes medidas.

- Todo diseño, desarrollo, implementación y operación deberá incorporar mecanismos de identificación, autenticación, control de acceso, auditoría e integridad.
- Se deberán incorporar identificaciones seguras y únicas para la autenticación de usuarios.
- Para un correcto funcionamiento en materia de seguridad deberán compartirse las labores de seguridad entre usuarios, administradores y los encargados directos de la propia seguridad.
- Deberán tomarse todas las precauciones posibles para proteger físicamente los sistemas de robo, destrucción o interrupción.
- Deberá existir un plan de recuperación del sistema para el caso en el que se dé robo, destrucción o interrupción del servicio.
- Deberá asegurarse la confidencialidad de la información almacenada, tanto en formato electrónico como no electrónico.
- Deberá asegurarse que se controla el acceso del personal al CPD.
- Todos los intervinientes en el plan de continuidad de negocio deberán conocer y saber aplicar cuando sea necesario dicho plan.
- El personal del área de operación que deba realizar las copias de seguridad deberá tener conocimiento y saber aplicar los procedimientos de backup.
- El personal del área de operación deberá tener conocimiento de los procedimientos de recuperación de datos de carácter personal, de sanitización de los soportes de datos de carácter personal y del procedimiento de registro entrada/salida de dichos soportes.
- El área de seguridad Informática centraliza los esfuerzos globales de protección de los activos de ECOLOGICAL MAILING S.L a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.
- De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información definidos en el alcance.

3. Política de confidencialidad de la información

Toda persona que tenga acceso a información de ECOLOGICAL MAILING S.L. Deberá considerar que dicha información, por defecto, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información de ECOLOGICAL MAILING S.L. a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos a tal efecto por ECOLOGICAL MAILING S.L.

- Se protegerán, por parte de los usuarios, en la medida de sus posibilidades, la información confidencial a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
- Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior, información confidencial en cualquier tipo de soporte, salvo que esté debidamente autorizado.
- Se utilizará el menor número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.
- El personal en relación a la utilización de agendas de contactos, de las herramientas ofimáticas dispuestas por ECOLOGICAL MAILING S.L. (por ejemplo el Outlook), únicamente introducirá datos personales como nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
- Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada a ECOLOGICAL MAILING S.L. tanto ahora como en el futuro.
- En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
- Asimismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con ECOLOGICAL MAILING S.L.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal desarrolle para ECOLOGICAL MAILING S.L.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo **197 del Código Penal,** que puede dar derecho a exigir compensaciones.

Para garantizar la seguridad de los Datos de Carácter Personal albergados en ficheros automatizados, el personal deberá observar las siguientes normas de actuación, además de las consideraciones ya mencionadas:

- El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros

temporales nunca serán ubicados en unidades locales de disco de los puestos PC del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

- No se albergarán datos de carácter personal en aquellos dispositivos que no estén autorizados para ello.
- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable de dicha información o fichero.
- El propietario de la información se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.

4. Política de control de acceso físico

- El personal no autorizado no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
- Se definen como áreas especialmente protegidas: CPD, zona de procesamiento y manipulado de información (departamento de informática y zona de taller).
- Se limitará el acceso al personal de soporte externo a las áreas especialmente protegidas. Este acceso, como el de cualquier otra persona ajena que requiera acceder a áreas protegidas, se asignará únicamente cuando sea necesario y se encuentre autorizado. Se mantendrá un registro de todos los accesos de personas ajenas.
- Se acompañará a los visitantes en áreas protegidas y se registrará la fecha y hora de su entrada y salida. Se mantendrá un registro protegido para permitir auditar todos los accesos.
- Se prohíbe el consumo de alimentos o bebidas en los CPD´s. No es recomendable en el resto de ubicaciones, salvo en las zonas habilitadas para ello.

5. Política de Uso apropiado de los recursos

Los recursos que ECOLOGICAL MAILING S.L pone a disposición del personal, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados.

Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Queda terminantemente prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Los equipos y/o aplicaciones que no estén especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de ECOLOGICAL MAILING S.L. o bajo supervisión de ECOLOGICAL MAILING S.L.

- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores inmorales u ofensivos.
- Introducir voluntariamente cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. El personal contratado por ECOLOGICAL MAILING S.L. tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.
- Intentar acceder a áreas restringidas de los Sistemas de Información.
- Intentar distorsionar o falsear los registros “log” de los Sistemas de Información.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
- Albergar Datos de Carácter Personal en ubicaciones que no estén autorizadas.
- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del Usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

6. Política de protección frente a malware

- Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.
- El software antivirus se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
- El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática, de los ficheros de definición de virus tanto en los ordenadores personales como servidores, así como de bloqueo frente a la detección de virus informáticos.

7. Política de Intercambio de información

- Los usuarios no deben ocultar o manipular su identidad bajo ninguna circunstancia. Salvo en los casos en los que se permita el uso de usuarios anónimos.
- La distribución de información ya sea en formato digital o papel se realizará mediante los dispositivos facilitados por ECOLOGICAL MAILING S.L. ECOLOGICAL MAILING S.L. se reserva, en función del riesgo identificado, la implementación de medidas de control, registro auditoría sobre estos dispositivos de difusión.
- En relación al intercambio de información, se considerarán no autorizadas las siguientes actividades:
- Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.

- Uso de dispositivos de almacenamiento externos (USB, CDs, DVDs…) sin previa autorización por parte de ECOLOGICAL MAILING S.L.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o bromas de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de ficheros a terceras partes no autorizadas de material de la Organización o material que es de alguna u otra manera confidencial.
- Transmisión o recepción de ficheros que infrinjan la Ley de Protección de Datos de Carácter Personal o directrices de ECOLOGICAL MAILING S.L.
- Transmisión o recepción de juegos y/o aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet como grupos de noticias, juegos u otras que no estén directamente relacionadas con el negocio.
- Todas las actividades que puedan dañar la buena reputación de ECOLOGICAL MAILING S.L. están prohibidas en Internet y en cualquier otro lugar. Esto se refiere también a actividades realizadas por empleados de ECOLOGICAL MAILING S.L. para su propio beneficio económico o de terceras partes, y a actividades de naturaleza política.
- Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo podrá ser realizada por personal autorizado y con el debido permiso.
- Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales donde está ubicado el fichero, dicho tratamiento deberá ser autorizado expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
- La transmisión de datos de carácter personal de nivel alto, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

8. Política de uso del correo electrónico

- Se considerará al correo electrónico como una herramienta más de trabajo provista al empleado con el fin de ser utilizada conforme al uso para el cual está destinada. Esta consideración facultará a ECOLOGICAL MAILING S.L. a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad del empleado y su derecho a la intimidad.
- El sistema de correo electrónico de ECOLOGICAL MAILING S.L. no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
- Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).
- No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
- No se permitirá la transmisión vía correo electrónico de información confidencial de ECOLOGICAL MAILING S.L. salvo que la comunicación electrónica esté bien cifradas y el envío este expresamente permitido.

9. Política de Conectividad a internet

- Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al objetivo de negocio de ECOLOGICAL MAILING S.L. o al cumplimiento de su trabajo diario.
- El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporado en la misma.
- La utilización de otros medios de conexión a Internet deberán ser previamente autorizados y estar sujetos a las anteriores consideraciones sobre el uso de Internet.
- Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al de ECOLOGICAL MAILING S.L. en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
- Únicamente se permitirá la transferencia de datos de o a Internet en conexión con actividades del negocio. La transferencia de ficheros no relativa a actividades de negocio (por ejemplo la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia, etc.) estarán prohibidas.

10. Política de Responsabilidades de usuario

- Cada usuario es responsable de su identificador y todo lo que de él se derive, por lo que es imprescindible que este sea únicamente conocido por el propio usuario, no deberá revelarse a nadie sin autorización expresa del responsable de seguridad.
- Los usuarios no deberán utilizar ningún identificador de otro usuario aunque dispongan de la autorización del propietario.
- Los usuarios deberán seguir las siguientes directivas en relación a la gestión de las contraseñas:
- Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad.
- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- Cambiar las contraseñas temporales en el primer inicio de sesión (“login”).
- Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- Notificar de acuerdo con lo establecido en la gestión de incidentes de la seguridad, cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.
- Los usuarios deberán velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Se establecerán las siguientes políticas de escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo:
- Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- No dejar desatendidos los equipos asignados a funciones críticas, y bloquear su acceso cuando sea estrictamente necesario.

- Proteger tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner y fax), como los equipos de duplicado (fotocopiadora, fax y scanner).
- La reproducción o envío de información con este tipo de dispositivos, queda bajo la responsabilidad del usuario.
- Retirar, sin retraso injustificado, la información confidencial, una vez impresa.
- Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
- Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.
- En caso de identificarse incidentes o debilidades relacionadas con la seguridad de la información, se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una esta supuesta debilidad o incidente de seguridad.

11. Política de utilización de Equipos de usuario

Sobre el equipamiento informático asociado al puesto del personal se establecerán las siguientes políticas:

- Todos los puestos de usuario con conectividad a recursos informáticos de ECOLOGICAL MAILING S.L. estarán controlados por ECOLOGICAL MAILING S.L.
- Ningún dato de carácter personal será almacenado en equipos de usuario ni soportes de información.
- Ningún usuario intentará por ningún medio transgredir el sistema de seguridad y las autorizaciones, ni dispondrá de herramientas que puedan realizarlo dentro de los sistemas de la organización. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.
- Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo. Cuando se termina la jornada de trabajo se recomienda apagar el equipo.

12. Política de Identificadores de usuario y contraseñas

- El personal que accede a los Sistemas de Información de ECOLOGICAL MAILING S.L. dentro de su ámbito de trabajo, es responsable de asegurar que los datos, y las aplicaciones y recursos informáticos, sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados e implantados.
- El personal está obligado a utilizar los recursos de ECOLOGICAL MAILING S.L. y los datos contenidos en ellos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales.
- Para obtener el acceso a los Sistemas de Información, el personal debe disponer de un acceso autorizado (identificador de usuario y contraseña) sobre el que como usuarios de sistemas de información deben observar los siguientes procedimientos de actuación:
- Ningún usuario recibirá un identificador de acceso a los sistemas de ECOLOGICAL MAILING S.L. hasta que no acepte formalmente la Política de Seguridad vigente.

- Todos los usuarios con acceso a un sistema de información, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña.
- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- La longitud mínima de la contraseña deberá ser de 6 caracteres.
- Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos.
- Es recomendable utilizar las siguientes directrices para la selección de contraseñas:
- No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo el nombre.
- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.
- La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por el usuario.
- No se debería utilizar el identificador de usuario como parte de la clave secreta.
- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada tres meses. En caso contrario, se le podrá denegar el acceso y deberá contactar con el Centro de Atención a Usuarios para la obtención de una nueva.
- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
- Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- En relación a datos de carácter personal, exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
  Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con el Centro de Atención a Usuarios para notificar la incidencia.

13. Política de uso del Software

- Todo el personal que accede a los Sistemas de Información de ECOLOGICAL MAILING S.L. debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
- Todo el personal, no expresamente autorizado, tiene prohibido instalar cualquier tipo de programa, incluidos los estandarizados.
- Se prohíbe el uso de software no validado por ECOLOGICAL MAILING S.L.
- También está prohibido borrar cualquiera de los programas instalados, salvo si se tiene autorización expresa para ello.

14. Política de uso de Recursos de red

- El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación previa validación del acceso.
- Las conexiones externas se realizarán requiriendo la autenticación previa del usuario, por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
- No se deberá conectar a ninguno de los recursos de ECOLOGICAL MAILING S.L. ningún tipo de equipo de comunicaciones (tarjetas, móviles, tabletas, módems, etc.) que posibilite conexiones alternativas no controladas a la red corporativa.
- Nadie deberá conectarse a la Red Corporativa a través de otros medios que no sean los definidos.

15. Política de Teletrabajo

El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la activación de las siguientes políticas:

- No se permite la utilización de equipamiento no controlado por ECOLOGICAL MAILING S.L. para las actividades de teletrabajo.
- Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.
- Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
- Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
- Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

16. Política sobre Propiedad intelectual

- Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
- Los empleados únicamente podrán utilizar material autorizado por ECOLOGICAL MAILING S.L. para el desarrollo de sus funciones.
- Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los Sistemas de Información de ECOLOGICAL MAILING S.L.
- Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.
- ECOLOGICAL MAILING S.L. únicamente autorizará el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

17. Política de Incidencias

- Todo el personal deberá ponerse en contacto con el responsable de seguridad en caso de que detecte cualquier incidencia relacionada con la información o los recursos de ECOLOGICAL MAILING S.L.
- Cualquier usuario podrá trasladar sugerencias y/o debilidades, que pueda tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas.
- Se deberá notificar, mediante la aplicación de Mejora Continua, de cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
- El responsable de seguridad centraliza la recogida, análisis y gestión de las incidencias recibidas.

Aprobado:

……