Política de Seguridad de la Información y Privacidad

Referencia:	POLI_PoliticaSeguridadInformacion_03
Autor:	Oficina de Seguridad
Versión:	03
Clasificación:	Uso Público

Control del documento

Registro de cambios

Versión	Fecha	Autor	Descripción
00	10/11/2020	Cibergob	Creación del Documento
01	13/11/2020	Comité de Seguridad	Revisión y Aprobación del Documento
02	22/01/2021	Comité de Seguridad	8.1. y 8.5 estructura organizativa y criterios
03	20/01/2022	Comité de Seguridad	5 – Marco normativo

Lista de distribución

"Lista de control de documentos de la Calidad, MA, SST y Seguridad de la información y privacidad", R.1-PR.01
Toda la Documentación aprobada, se encuentra actualizada y al alcance de todos los responsables Informáticamente en la INTRANET de Solitium (https://intranet.gruposolitium.es:8441/index.php/gs/calidad-y-laboral/sistema-de-gestion-de-calidad).

Control de firmas

Aprobado por:	
CARLOS PRAT NAVARRO	ANA BELÉN SANGO
Presidente del Comité de Seguridad	Secretario del Comité

Toda copia impresa sin firma se considera "Copia NO Controlada"

Contenido

1. Objeto

Con el objeto de dirigir y dar soporte a la gestión de la información y de sus servicios, se establece en la presente política las líneas y principios estratégicos que se deberán observar en Solitium para garantizar la calidad de la información y la prestación continuada de los servicios con el objeto de actuar preventivamente ante posibles incidencias y reaccionando con rapidez ante la materialización de las mismas.

Esta política va alineada con los requisitos establecidos dentro de los correspondientes artículos del Esquema Nacional de Seguridad (ENS).

2. Objetivos y misión de SOLITIUM

SOLITIUM adopta un sistema de gestión integrado, en el que se incluye la Seguridad de la información y privacidad por decisión estratégica de la organización que le ayuda a mejorar su desempeño global y proporcionar una base sólida para las iniciativas de desarrollo sostenible.

Su diseño e implementación está influenciado por su entorno, los cambios de ese entorno, sus necesidades cambiantes, sus objetivos particulares, los productos que proporciona, los procesos que emplea, su tamaño y la estructura de la organización.

SOLITIUM, S.L. es un grupo de empresas especializadas en servicios ofimáticos, informáticos y de comunicaciones, soluciones de gestión documental para pymes, gran formato e impresión 3D.

Los principios y misión de la organización, es describir cómo gestionar la seguridad de la información y privacidad y establecer una política de seguridad en el uso de medios electrónicos para conseguir una protección adecuada en SOLITIUM.

3. Objetivos de la Política de Seguridad

La política de seguridad de las tecnologías de la información y comunicaciones de SOLITIUM, en adelante Política de Seguridad de la información y privacidad de SOLITIUM, persigue la consecución de los siguientes objetivos:

a) Garantizar a los usuarios que los datos alojados en SOLITIUM serán gestionados de acuerdo a los estándares y buenas prácticas en seguridad TIC.

b) Aumentar el nivel de concienciación en materia de seguridad TIC allí donde es de aplicación esta Política, garantizando que el personal a su servicio es consciente de sus obligaciones y responsabilidades.

c) Establecer las bases de un modelo integral de gestión de la seguridad TIC en SOLITIUM, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.

d) Hacer patente el compromiso de SOLITIUM con la seguridad de la información y privacidad mediante su apoyo al Comité de Seguridad dotándole de los medios y facultades necesarias para la realización de sus funciones.

e) Definir, desarrollar y poner en funcionamiento los controles metodológicos técnicos, organizativos y de gestión, necesarios para garantizar de un modo efectivo y medible la preservación de los niveles de confidencialidad, disponibilidad e integridad de la información aprobados por SOLITIUM.

f) Garantizar la continuidad de los servicios ofrecidos por SOLITIUM a los usuarios.

g) Crear y promover de manera continua una “cultura de seguridad” tanto internamente, a todo el personal, como externamente a los ciudadanos y proveedores que permita asegurar la eficiencia y eficacia de los controles implantados y aumente la confianza de nuestros ciudadanos.

4. Revisión de la Política

Esta política será revisada al menos una vez al año y siempre que haya cambios relevantes en la organización, con el fin de asegurar que ésta se adecua a la estrategia y necesidades de la misma.

La Política será propuesta y revisada por el Comité de Seguridad y aprobada y difundida por SOLITIUM para que la conozcan todas las partes afectadas.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad para resolución de estos, previo informe propuesta de la unidad de protección de datos.

5. Marco Normativo

A los efectos previstos en esta Política, el marco normativo de referencia es el que estipula la legislación vigente en materia de seguridad TIC.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los usuarios, SOLITIUM desarrolla sus actividades de acuerdo a la normativa vigente en dichas materias, de entre las que actualmente cabe destacar por su especial relevancia:

a) Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

b) Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

c) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

d) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

e) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

f) Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

g) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

h) Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

i) Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS).

j) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

k) Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

6. Ámbito de aplicación

Esta Política será de aplicación y de obligado cumplimiento para todos los usuarios de SOLITIUM; a sus recursos y a los procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

7. Principios de seguridad TIC

7.1. Principios básicos de la política de seguridad TIC

La política de seguridad TIC de SOLITIUM se desarrollará, con carácter general, de acuerdo a los siguientes principios:

a) Principio de confidencialidad: los activos TIC deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

b) Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

c) Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los activos TIC y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

d) Principio de trazabilidad: se implantarán medidas para asegurar que en todo momento se pueda determinar quién hizo qué y en qué momento, con el fin de tener capacidad de análisis sobre los incidentes de seguridad detectados.

e) Principio de autenticidad: se deberá articular medidas para garantizar la fuente de información de la que proceden los datos y que las entidades donde se origina la información son quienes dicen ser.

f) Principio de gestión del riesgo y de la seguridad integral: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los activos TIC.

g) Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los activos TIC deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

h) Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información se refiere. De igual forma, se fomentará la formación específica en materia de seguridad TIC de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

i) Principio de prevención, reacción y recuperación: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad TIC.

j) Principio de mejora continua o de la reevaluación periódica: se revisará el grado de eficacia de los controles de seguridad TIC implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico.

k) Principio de seguridad en el ciclo de vida de los activos TIC o líneas de defensa: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

l) Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad del servicio, así como de la responsabilidad de la información. Los roles y responsabilidades de cada una de estas funciones deberán quedar debidamente acotadas y reflejadas documentalmente.

7.2. Requisitos Mínimos de Seguridad

Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación de un Sistema de Gestión de seguridad: La estructura organizativa para la gestión de la seguridad de la información y privacidad será competente para mantener, actualizar y hacer cumplir, la Política de Seguridad de la información y privacidad de SOLITIUM, así como para garantizar el correcto funcionamiento del Sistemas de Gestión de seguridad.

b) Análisis y gestión de los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

c) Gestión del personal: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Profesionalidad: La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida. El personal que atiende, revisa y audita la seguridad de los sistemas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables. Se exigirá, de manera objetiva y no discriminatoria, que los prestadores de servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

f) Protección de las instalaciones: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

g) Adquisición de productos: En la adquisición de productos de seguridad será exigible la certificación de la funcionalidad de seguridad relacionada con el objeto de dicha adquisición, según el criterio del responsable de seguridad y aplicando el principio de proporcionalidad. Para la contratación de servicios de seguridad se estará a lo dispuesto en el principio de profesionalidad.

h) Seguridad por defecto: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. La seguridad de la información y privacidad debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

i) Integridad y actualización del sistema: El sistema informático de SOLITIUM será diseñado y mantenido por el responsable del servicio bajo criterios técnicos, de eficiencia y de seguridad. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. También requerirá autorización formal previa cualquier alteración de la configuración de hardware y software de los equipos o cualquier desinstalación de programas de la plataforma de uso predefinida. Con carácter general, no se instalará software salvo que se disponga de la correspondiente licencia de uso, bien por haberlo adquirido la organización, o bien por tratarse de software libre con una licencia aplicable. En todo caso, será el administrador del sistema quien instale el software una vez se autorice.

j) Protección de la información almacenada y en tránsito. En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil. También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por SOLITIUM.

k) Prevención ante otros sistemas de información interconectados: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

l) Registro de actividad: Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

m) Incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

n) Continuidad de la actividad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

o) Mejora continua del Sistema de Gestión de seguridad: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información y privacidad será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

8. Organización de la seguridad TIC

8.1. Responsabilidad general

La preservación de la seguridad TIC será considerada objetivo común de todas las personas al servicio de SOLITIUM, siendo estas responsables del uso correcto de los activos de tecnologías de la información y comunicaciones puestos a su disposición.

En caso de incumplimiento de las directrices y normativas de seguridad indicadas en la presente política y las obligaciones derivadas de ellas, SOLITIUM se reserva el derecho de aplicar el régimen disciplinario establecido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Por su importancia dentro de la implementación de la seguridad, quedan desarrolladas en la presente política algunas de las funciones de los órganos que SOLITIUM estima necesarios para la correcta gestión de la seguridad.

La estructura organizativa de SOLITIUM en materia de Seguridad se revisa cada dos años. Una vez revisada, SOLITIUM celebra un Comité de Seguridad Extraordinario donde se ratifica la nueva organización de la seguridad (Presidente, vocales, secretario, responsable de seguridad, de la información y del servicio ...).

8.2. Comité de Seguridad

1. Se crea el Comité de Seguridad de SOLITIUM, como órgano colegiado de carácter transversal para la coordinación y gobierno en materia de seguridad.

2. El Comité estará formado por un presidente, un secretario y una serie de vocales que representan las unidades de SOLITIUM.

3. Serán funciones propias del Comité:

    a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad TIC.

    b) Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y planes estratégicos definidos.

    c) Elevación de propuestas de revisión del marco normativo de seguridad TIC al órgano competente para su reglamentaria tramitación.

    d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad TIC.

    e) Supervisión y aprobación del nivel de riesgo y de la toma de decisiones en la respuesta a incidentes de seguridad que afecten a los activos TIC.

    f) Definición y aprobación del modelo de relación con los Comités de Seguridad TIC de las entidades incluidas en el ámbito de aplicación de la Política.

4. El Comité se reunirá al menos una vez por semestre y se regirá por esta política.

5. El Comité nombrará entre sus miembros un grupo de respuesta a incidentes TIC, llamado “Comité de Crisis”, cuya función será la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos de SOLITIUM.

6. Las labores de soporte y asesoramiento al Comité serán realizadas por el Responsable de Seguridad TIC y la Oficina de Seguridad TIC.

8.3. Responsable de Seguridad

1. El nombramiento del Responsable de Seguridad será potestad del Comité de Seguridad de SOLITIUM.

2. La persona Responsable de Seguridad tendrá las siguientes funciones, dentro de su Departamento:

    a) Definición y seguimiento de las actuaciones relacionadas con la seguridad TIC de los activos de información de la Entidad y la gestión del riesgo.

    b) Asesoramiento y soporte sobre temas de Seguridad.

    c) Coordinación en materias de seguridad TIC.

    d) Propuesta y seguimiento de programas de formación y concienciación.

    e) Reporte al Comité de Seguridad de un informe periódico sobre el estado de la Seguridad TI y las actividades relacionadas.

    g) Asunción de las funciones incluidas en los artículos 10, 27.3, 34.6, Anexo II (apartado 2.3) y Anexo III (apartados 2.1.b y 2.2.b) del Real Decreto 3/2010, de

8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

f) Asunción de las funciones incluidas en el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

8.4. Oficina de Seguridad

1. La Oficina de Seguridad estará compuesto por técnicos de las diferentes unidades de SOLITIUM, si bien se puede convocar a aquellas personas que la Oficina estime necesarias para el desarrollo de los trabajos encomendados.

2. En esta Oficina de Seguridad estará también el Responsable de Seguridad de SOLITIUM que tendrá funciones sobre la revisión y elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad TIC.

3. La Oficina de Seguridad TIC tendrá las siguientes atribuciones:

   a) Asesoramiento en la definición del planteamiento técnico y operativo de los objetivos, iniciativas y planes estratégicos en seguridad TIC, de acuerdo con las directrices del Comité de Seguridad TIC.

   b) Asesoramiento en la elaboración de propuestas relativas a la revisión del marco normativo de seguridad TIC.

   c) Elaboración de informes y propuestas de cumplimiento legal y normativo.

   d) Elaboración de informes sobre el nivel de seguridad TIC de los activos.

   e) Reporte al Comité Seguridad TIC de informes periódicos sobre el estado de la Seguridad TI del IIS Aragón.

4. La Oficina de Seguridad TIC se regirá por esta Política.

8.5. Otros Responsables

El Responsable de la Información determina los requisitos de seguridad clasificando la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (Disponibilidad, Autenticidad, Trazabilidad, Confidencialidad e Integridad), dentro del marco establecido en el Anexo I del ENS, respecto a la información tratada en SOLITIUM.

El Responsable del Servicio determina la infraestructura hardware y software del sistema de información, los criterios de uso, los servicios ofrecidos, los formatos y cualquier otro aspecto del funcionamiento del sistema de información de SOLITIUM.

El Responsable de Seguridad determina cómo satisfacer los requisitos de seguridad, tanto de la información como de los servicios ofrecidos, incluyendo la definición de procedimientos de

seguridad y, en su caso, la adopción de medidas de urgencia ante posibles deficiencias o amenazas en SOLITIUM.

El administrador del sistema desarrolla, opera y mantiene el sistema de información de SOLITIUM.

Las discrepancias en materia de seguridad serán resueltas atendiendo al criterio de mayor jerarquía.

Las atribuciones de cada responsable, así como los mecanismos de coordinación y resolución de conflictos se explicitan en la Normativa de Roles y Responsabilidades de Seguridad y la Normativa de la Organización de la Seguridad.

9. Desarrollo de la Política de Seguridad

9.1. Instrumentos del desarrollo

La Política de Seguridad de la información y privacidad de SOLITIUM se desarrollará por medio de instrucciones de servicio y circulares que afronten aspectos específicos. Dichas instrucciones y circulares podrán adoptar alguna de las siguientes modalidades:

Se usarán, entre otros, los siguientes instrumentos:

Normas de seguridad: Uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Procedimientos: Concretan flujos de trabajo para la realización de tareas, indicando lo que hay que hacer, paso a paso, pero sin entrar en detalles (de proveedores, marcas comerciales o comandos técnicos). Son útiles en tareas repetitivas.

Instrucciones técnicas (IT): Desarrollan los Procedimientos llegando al máximo nivel de detalle, (indicando proveedores, marcas comerciales y comandos técnicos empleados para la realización de las tareas).

La normativa de seguridad estará disponible en la intranet a disposición de todos los miembros de la organización que necesiten conocerla.

9.2. Aprobación de las normativas

En toda la organización, la aprobación de las normas de seguridad se hará de acuerdo a lo dispuesto en la presente política y las normativas específicas que para ello desarrollará SOLITIUM.

9.3. Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad de la información y privacidad y normas que la desarrollan podrán derivarse las consiguientes responsabilidades disciplinarias, que se sustanciarán conforme a lo establecido en la Ley del Estatuto de los Trabajadores sobre régimen disciplinario de los empleados.

10. Concienciación y Formación

Con la Concienciación y formación se busca alcanzar varios objetivos. Por una parte y fundamental la plena conciencia respecto a que la seguridad de la información y privacidad afecta a todos los miembros de SOLITIUM y a todas las actividades y servicios que lo componen.

Por otra parte, y siguiendo el Principio de Seguridad Integral, la articulación de los medios necesarios para que todas las personas que intervienen en el día a día de SOLITIUM y sus responsables jerárquicos tengan la sensibilidad adecuada hacia la responsabilidad que conlleva al gestionar información de los ciudadanos y de la propia Administración.

11. Análisis y Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán ser sometidos a un análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- Al menos una vez al año (mediante revisión y aprobación formal).
- Cuando o curra un incidente grave de seguridad.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

12. Seguridad de la información y privacidad

Se desarrollará una Clasificación de la Información de SOLITIUM de forma que se identifiquen los distintos tipos de información, en base a su sensibilidad, se establezca cómo etiquetar los soportes que la contengan y se determine qué se puede y no se debe hacer con cada nivel de clasificación.

13. Datos de Carácter Personal

Será de aplicación lo contemplado en el RGPD y lo dispuesto en la legislación nacional a tales efectos.

Cada departamento se encargará de gestionar y mantener la seguridad referente a los datos de carácter personal incluidos en las operaciones de tratamiento que a tal efecto sean de su responsabilidad.

Todos los sistemas de información de SOLITIUM se ajustarán a los niveles de seguridad requeridos por esta normativa.

14. Obligaciones del personal

Todos los miembros de la organización y las empresas y personas terceras que realicen servicios de cualquier clase contratados por SOLITIUM o que de alguna manera se presten bajo el control

y/o la dirección de SOLITIUM tienen la obligación de conocer y cumplir esta Política de Seguridad de la información y privacidad y la Normativa de Seguridad. SOLITIUM es responsable de comunicar la política y las normas, así como de disponer de los medios necesarios para que todo el personal las conozca de forma efectiva, en especial, las que puedan afectar a sus funciones.

Se establecerá un programa de concienciación continúa dirigido a todos los miembros de SOLITIUM, en particular a los de nueva incorporación.

El personal deberá usar los procedimientos de notificación de incidentes de seguridad habilitados a tal efecto, en caso de detectar un posible incidente.

Las personas con responsabilidad en el uso, operación o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas.

15. Terceras partes

Cuando SOLITIUM preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la información y privacidad, se establecerán canales para el reporte y coordinación de los respectivos Delegados de Protección de Datos y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando SOLITIUM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte deberá aceptar el quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la información y privacidad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados, así como del responsable del tratamiento previsto en el RGPD, antes de seguir adelante.

16. ANEXO I. Glosario de términos

Activo de tecnologías de la información y comunicaciones: cualquier información o sistema de información que tenga valor para la organización. Incluye datos, servicios, aplicaciones, equipos, comunicaciones, instalaciones, procesos y recursos humanos.

Contingencia grave: Incidente de seguridad TIC cuya ocurrencia causaría la reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, el sufrimiento de un daño significativo a los activos de la organización, el incumplimiento material de alguna ley o regulación, o un perjuicio significativo de difícil reparación a personas.

Incidente de seguridad TIC: Suceso, accidental o intencionado, a consecuencia del cual se ve afectada la integridad, confidencialidad o disponibilidad de la información.

Plan director de seguridad: Estrategia y conjunto de iniciativas planificadas, plasmadas en un documento escrito, para alcanzar un determinado nivel de seguridad en la organización.

Política de seguridad de la información y privacidad y comunicaciones: Conjunto de directrices plasmadas en un documento escrito, que rigen la forma en que una organización gestiona y protege sus activos de tecnologías de la información y comunicaciones.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Sistema de información: Conjunto organizado de recursos destinado a recoger, almacenar, procesar, presentar o transmitir la información.

Sistema de información crítico: Sistema de información cuyo adecuado funcionamiento es indispensable para el funcionamiento de la organización y el cumplimiento de sus obligaciones fundamentales.

POLÍTICAS DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

SOLITIUM, S.L.

Índice del Documento

1. ¿EN QUÉ CONSISTEN LAS POLÍTICAS DE SEGURIDAD?

El presente manual es un documento que tiene por finalidad dar a conocer a los diferentes usuarios de SOLITIUM que tratan con información de gestión y con datos personales, las normas de uso de la información y las condiciones y obligaciones que se derivan de la legislación existente en materia de protección de Datos de Carácter Personal.

En cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, existe la obligación que la entidad responsable de los tratamientos facilite a todo el personal afecto, el conocimiento del contenido del Sistema de Gestión de Protección de Datos Personales, en lo referente a las funciones y obligaciones de cada una de las personas con acceso a datos de carácter personal y a los sistemas de información.

Por ello, existe la necesidad de que los distintos usuarios de SOLITIUM conozcan la existencia de unas normas y procedimientos, así como a efectuar una declaración de recepción y aceptación del Manual de Seguridad. Este es el objetivo del presente documento, extractado de las Políticas de Seguridad de la entidad, llamado “Política de Seguridad y Protección de Datos Personales” para que todos los emplea-dos usuarios de ficheros con datos personales tengan conocimiento del mismo.

Para la resolución de cualquier duda sobre la temática aquí analizada, cualquier usuario se podrá poner en contacto con el Responsable de Seguridad de SOLITIUM, Manuel de Castro Abellán, a efectos de plantearle la duda correspondiente.

2. ¿QUÉ OBLIGACIONES AFECTAN A LOS USUARIOS DE SOLITIUM?

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 al Responsable de Seguridad las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos más adelante en este documento.

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

Los usuarios que llevan acabo tratamientos sobre datos de carácter personal, o personal que usualmente utiliza el sistema informático de acceso a estos datos, estarán relacionados en un anexo del SGPDP o bien en un registro del sistema operativo de uno de los servidores centrales de SOLITIUM. Este documento es de obligado cumplimiento para todos ellos.

2.1 Respecto de los puestos de trabajo.

Los puestos de trabajo estarán bajo la responsabilidad del usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas. Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse tanto mediante un protector de pantalla con contraseña implementada que impida la visualización de los datos o con del sistema de bloqueo del equipo (con sistemas operativos Windows), presionan-do las teclas Ctrl.+Alt+Sup y luego pulsando la opción Bloquear Equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente al perfil de cada usuario.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Los puestos de trabajo desde los que se tiene acceso a los datos tendrán una configuración fija en sus aplicaciones y sistemas operativos que sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad o por los administradores del sistema. Desde el punto de vista del cumplimiento del principio de actualización de los datos personales y de los tratamientos, deberá existir una conexión y actualización constante entre las diferentes bases de datos existentes en SOLITIUM.

SOLITIUM, se reserva el derecho a comprobar la comunicación profesional de los empleados en su puesto de trabajo. Para ello, en cualquier momento puede acceder al correo electrónico / dispositivo electrónico (ordenador, tablet, etc.…) del empleado para verificar lo establecido en el presente documento de “Política de Seguridad y Protección de Datos Personales”.

2.1.1.Salvaguarda y protección de las contraseñas personales.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder a su cambio.

2.1.2. Correo Electrónico.

El uso del correo electrónico corporativo es una herramienta de trabajo, se limita a los temas directamente relacionados con la actividad de SOLITIUM y los cometidos del puesto de trabajo del usuario.
Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provenga de redes externas debe cumplir los requisitos establecidos en estas normas y, en especial, las referidas a contraseñas, propiedad intelectual y al control de virus.

SOLITIUM se reserva el derecho de auditar, caso de plantearse la apertura de un expediente disciplinario y sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a SOLITIUM como responsable civil subsidiario.

Para el uso del correo electrónico se atenderá a las siguientes buenas prácticas:

1.- No enviar, sin previa autorización, correos con copias a más de 45 destinatarios a la vez. Ya que esta práctica, puede ser considerada “Spam” por determinados operadores.

2.- Enviar copias con la opción “Copia Oculta”. Para evitar realizar cesiones de datos indebidas (Hay que evitar dar a conocer la cuenta de correo de terceros).

3.- El envío de correo electrónico está limitado a 20 mb de capacidad.

4.- Para el envío de información especialmente protegida debe usarse alguna aplicación para cifrar el contenido, estableciendo una contraseña de encriptación. (Está disponible la aplicación 7z o 7zip, consultar Departamento Técnico).

2.1.3. Acceso a Internet.

El uso del sistema informático de SOLITIUM es una herramienta de trabajo, para acceder a redes públicas como Internet y se limita a los temas directamente relacionados con la actividad de SOLITIUM y los cometidos del puesto de trabajo del usuario.

El acceso a debates en tiempo real (Chat /IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido siempre y cuando no responda a temas profesionales.

El acceso a páginas web (www) y otras fu entes de información como FTP, Descarga directa de Ficheros, etc. se limita a aquellos que contengan información relacionada con la actividad de SOLITIUM o con los cometidos del puesto de trabajo del usuario. El acceso a recursos “Peer to Peer” (Como E-mule, Ares, etc.), quedan expresamente prohibidos. SOLITIUM dispondrá de equipos para monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red corporativa.

Están expresamente prohibidas las siguientes actividades:

1.Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de SOLITIUM.

2.Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de SOLITIUM o de terceros. (Esto puede constituir un delito de daños, previsto en el artículo 264.2 del Código Penal)

3.Enviar mensajes de correo electrónicos de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.

4.Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios (Esta actividad puede constituir un delito de descubrimiento y revelación de secretos, previsto en el artículo 197 y artículo 199. 1 del Código Penal).

5. Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los sistemas informáticos de SOLI-TIUM o de terceros. El usuario tiene la obligación de utilizar los programas antivirus y sus actualizaciones puestos a su disposición para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

6. Utilizar los recursos telemáticos de SOLITIUM, incluida la red Internet, para actividades que no se hallen directa-mente relacionadas con el puesto de trabajo del usuario.

7. Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de SOLITIUM, en la red corporativa de SOLITIUM.

8. Instalar copias ilegales de cualquier programa, incluidos los estandarizados, sin previa autorización de la Dirección de SOLITIUM.

9. Compartir o facilitar los identificadores de usuario y las claves de acceso facilitados por SOLITIUM con otra persona física o jurídica, incluido el personal de SOLITIUM. En caso de incumplimiento de esta prohibición, el usuario es el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada el identificador del usuario.

10. Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de SOLITIUM o de terceros.

11. Intentar aumentar el nivel de privilegios de un usuario en el sistema.

Es necesario que quede clara la idea de que, sobre todo en el caso de que un usuario ejercite cualquiera de sus derechos reconocidos en el RGPD (que más adelante se tratarán), todas las bases de datos deberán actualizar-se según haya el afectado modificado, suprimido, limitado o ejercitado su oposición al tratamiento de sus datos personales. Para facilitar la centralización de la información, se ha articulado un sistema por el que se informa a los afectados de que los derechos podrán ejercitarlos mediante el envío de correo ordinario a SOLITIUM en el que se identifique claramente el derecho que se quiere ejercer.

En todo caso, deberán ser los receptores primarios de estos correos (las personas designadas por el Responsable de Seguridad de SOLITIUM) los que se encarguen de distribuirlos internamente entre todos los usuarios con accesos informáticos a las bases de datos personales a efectos de que el contenido de los diferentes ficheros que-de actualizado.

Respecto a los datos de carácter personal contenidos en un soporte documental, cabe señalar que deberá procederse a su almacenamiento y depósito siempre que sea posible en un armario cerrado con llave cuando no vayan a ser utilizados.
Por ello, en el momento en que una documentación en la que constatasen datos personales haya dejado de ser necesario consultarla, se archivará no dejándola nunca sobre las mesas de trabajo, siendo cada usuario responsable del cumplimiento de esta medida de seguridad.

En el caso en que sea necesario proceder a la destrucción de una documentación dentro de SOLITIUM en la que se contuvieran datos personales, será necesario utilizar, sin

excepción alguna, la máquina destructora o trituradora de documentos, no sin antes informar previamente al Responsable de Seguridad.

Tal es el supuesto en que una vez finalizada una relación y no siendo útil o no cumpliendo dicha información personal alguna de las finalidades de SOLITIUM, el usuario procederá a destruir dicha documentación en la forma indicada anteriormente, salvo que se dispusiera su archivo.

Cabe resaltar que, bajo ningún concepto, se podrán tirar documentos a la papelera conteniendo datos personales por el peligro evidente de que dichos documentos puedan llegar a hacerse públicos antes de ser totalmente destruidos. Por ello, todo documento conteniendo datos personales del que SOLITIUM, se deba desprender deberá ser previamente triturado.

2.2 Salvaguarda y protección de las contraseñas personales.

El Responsable de Seguridad comunicará a los usuarios los principios que rigen la política de protección de datos en lo concerniente al control de accesos a los sistemas de tratamiento (las contraseñas personales) y que podemos resumir en lo siguiente:

a) Cada empleado tiene un usuario que se autentica mediante contraseña de forma que no podrán dos emplea-dos compartir un mismo usuario o utilizar, en un momento dado, el usuario de otro empleado para acceder al sistema de información.

b) El usuario será, inicialmente, el nombre seguido de un punto y del apellido. (Ej. ana.garcia)

c) La contraseña debe ser elegida por el usuario que la utiliza, salvo que existan sistemas informáticos de generación de contraseñas que garanticen la confidencialidad de la contraseña generada.

d) La longitud de la contraseña será de ocho caracteres como mínimo.
c) La contraseña estará formada por una conjunción de símbolos, números y letras (mayúsculas y minúsculas).

e) Se evitarán contraseñas como los nombres comunes, números de matrícula de vehículos, teléfonos, nombres de familiares, amigos, etc. y derivados del nombre de usuario (por supuesto, la contraseña nunca podrá ser igual que el usuario) como permutaciones o cambio de orden de las letras, transposiciones, repeticiones de un único carácter y procedimientos análogos.

f) Deberá cambiarse la contraseña, al menos, cada 110 días.

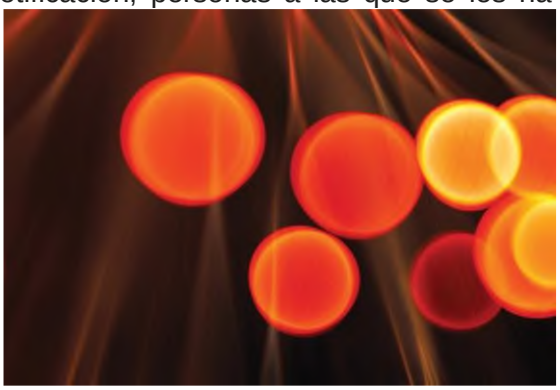
g) No podrá reutilizarse ninguna de las últimas cuatro contraseñas usadas anteriormente.

h) Además de ello, caso de que el nivel de seguridad aplicable sea de nivel alto, los usuarios autorizados a tener acceso a datos correspondientes con los ficheros sometidos a un nivel de seguridad alto deberán tener implanta-dos en su perfil de usuario un número máximo de intentos permitidos de introducción de la contraseña de manera que, en caso de superarlos, el perfil de usuario quedase deshabilitado, no siendo posible su habilitación salvo con conocimiento del Responsable de Seguridad o del Administrador de la red.

2.3. Gestión de incidencias / Violaciones de seguridad

Cualquier usuario que tenga conocimiento de una incidencia relacionada con la seguridad y confidencialidad de los datos personales contenidos dentro de los ficheros de SOLITIUM, es responsable de la comunicación de la misma al Responsable de Seguridad para dar cumplimiento al artículo 33 del RGPD.

Los datos que deberán comunicarse al Responsable de Seguridad son los siguientes: nombre del usuario de los datos (empleado), fecha de notificación, persona que realiza la notificación , tipo de incidencia (Descripción de la naturaleza de la violación de la seguridad de los datos , inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos afectados), momento en que se produce (en su defecto, momento de su descubrimiento), destinatario de la notificación, personas a las que se les ha comunicado la incidencia, descripción de las posibles con-secuencias de la violación de la seguridad de los datos, descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.



El conocimiento y la no notificación de una incidencia por parte de un usuario, así como el incumplimiento de las obligaciones y medidas de seguridad establecidas en este documento por el personal afectado, será considerada como una falta, contra la seguridad del tratamiento por parte de este usuario y será sancionada conforme a las medidas sancionadoras previstas en el estatuto de los trabajadores.

2.4. Deber de secreto y confidencialidad

Como consecuencia de lo dispuesto en la normativa sobre Protección de Datos de Carácter Personal, toda persona con acceso y posibilidad de tratamiento de datos personales estará obligado a cumplir las siguientes obligaciones:

a) Conocer la privacidad de todos los datos que manejan y, por lo tanto, su obligación de mantener el secreto de dicha información.

b) Hacer uso de los datos únicamente para los fines para los cuales han sido recabados, con el fin de garantizar la calidad de los mismos.

c) No divulgar las contraseñas de que dispongan para acceder tanto a los sistemas informáticos como a los fiche-ros que contengan datos de carácter personal.

d) Solicitar las autorizaciones necesarias para el tratamiento de dichos datos siempre que se refieran a las salidas o entradas de soportes informáticos.

e) Comunicar al Responsable de Seguridad cualquier incidencia que afecte a la seguridad de los datos así como de los intentos de acceso no autorizados que hayan podido ser detectados.

2.5. Control de Acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Exclusiva-mente el Responsable de Seguridad está autorizado para conceder alterar o anular el acceso autorizado sobre los datos y los recursos.

Cualquier persona de SOLITIUM, para solicitar el alta, modificación o baja de las autorizaciones de acceso a los datos, deberá dirigirse al Responsable de Seguridad, indicando su nombre y el motivo de la solicitud.

2.6. Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en el lugar determinado por el Responsable de Seguridad, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:

Todo el personal de SOLITIUM.

El procedimiento establecido para habilitar o retirar el permiso de acceso y los controles de acceso existentes, será la puesta en contacto con el Responsable de Seguridad. El procedimiento a seguir para casos en que personal no autorizado tenga que tener acceso a los locales por razones de urgencia o fuerza mayor, será la autorización escrita o verbal del Responsable de Seguridad.

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

Los soportes que contengan datos objeto de tratamiento, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata o bien como consecuencia de procesos periódicos de respaldo o cualquier otra operación esporádica, deberán estar claramente identificados con una etiqueta externa que indique: Qué tratamiento, Qué tipos de datos contiene, Proceso que los ha originado y Fecha de creación.

Aquellos medios que sean reutilizables y que hayan contenido copias de datos , deberán ser borrados físicamente antes de su reutilización de forma que los datos que contenían no fuesen reutilizables o recuperables.

Los soportes que contengan datos objeto de tratamiento deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para su uso.

El inventario de soportes esta anexado al SGPDP.

La salida de soportes informáticos, ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el Responsable del Tratamiento o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento:
Cualquier persona con firma reconocida en SOLITIUM podrá llevar a cabo la citada autorización.

Los documentos de autorización relativos a la salida de soportes que contengan datos personales, deberán solicitarse al Responsable de Seguridad.

2.7. 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 deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

2.8. Régimen de trabajo fuera de los locales de la ubicación del fichero

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el Responsable del Fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

El procedimiento de autorización será el siguiente: En el caso de tratamientos realizados por personal interno de SOLITIUM, solo podrán realizar el tratamiento fuera de los locales de la ubicación del fichero, cuando lo realicen con equipos y/o infraestructura bajo control de SOLITIUM. Para tratamientos por otros medios, precisarán una autorización por escrito del Responsable de Seguridad.

Para tratamientos realizados por personal externo de SOLITIUM, precisarán una autorización por escrito de Responsable de Seguridad.

En el uso de Informática Móvil (teléfonos móviles, tabletas y ordenadores portátiles) se atenderá a las siguientes buenas prácticas:

a) Permanecer siempre cerca del dispositivo.

b) No dejar desatendidos los equipos.

c) No llamar la atención acerca de portar un equipo valioso.

d) No poner identificaciones de la empresa en el dispositivo, salvo los estrictamente necesarios.

e) No poner datos de contacto técnico en el dispositivo.

f) Mantener cifrada la información clasificada

2.9. Ficheros temporales

Los ficheros temporales deberán cumplir las medidas de seguridad que les corresponda con arreglo a los criterios expresados en el RGPD, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motiva-ron su creación. Se consideran ficheros temporales, las copias de ficheros, bases de datos, expedientes, etc. que contengan datos personales, tanto digitales como en soporte papel (fotocopias).

2.10. Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. 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.

En el caso de la realización de copias de seguridad, deberá ponerlo en conocimiento del Responsable de Seguridad, el informará de los procedimientos de copia y recuperación de respaldo para cada fichero.

2.11. Responsable de Seguridad

El Responsable del Tratamiento designará a un solo Responsable de Seguridad, que con carácter general se en-cargará de coordinar y controlar las medidas definidas en este documento de seguridad. En ningún caso, la designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con el Reglamento de medidas de seguridad.

El Responsable de Seguridad desempeñará las funciones encomendadas durante el periodo de un año prorrogable. Una vez transcurrido este plazo el responsable del fichero podrá nombrar al mismo Responsable de Seguridad o a otro diferente.

En el Anexo II del Documento de Seguridad disponible en SOLITIUM, se encuentran las copias de los nombramientos de Responsable de Seguridad .

2.12. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

3.- OBLIGACIONES DE SOLITIUM Y DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES.

3.1. Deber de información y la obtención del consentimiento.

SOLITIUM, como responsable de los diferentes tratamientos contenidos en soporte informático o documental, deberá cumplir con una serie de obligaciones que el RGPD le impone frente a los diferentes afectados:

Por un lado, y una vez tenido en cuenta la fuente de la que se han obtenido los datos personales, deberá informar de los extremos contenidos en el artículo 13 del RGPD.
Por otro lado, deberá obtener el consentimiento, si procede, para la realización del tratamiento y, en su caso, comunicación de los datos personales.

Dicha labor deberá ser realizada de forma completa por parte del responsable, con la firma de un contrato que deberá firmar con sus Terceros, Proveedores y Empleados, cumpliendo de esta manera con una de las obligaciones más importantes contenidas en la legislación sobre protección de datos personales.

3.2. Los derechos de los afectados.

Es necesario que todos los empleados de SOLITIUM tengan conocimiento de los diferentes derechos que la legislación concede a los titulares de los datos personales frente a los tenedores de dichos datos (los diferentes Responsables de los tratamientos).

En este sentido, si cualquiera de los empleados de SOLITIUM tuviesen conocimiento de la solicitud por parte de un afectado del ejercicio de alguno de los derechos reflejados a continuación, deberá ponerlo inmediatamente en conocimiento del Responsable de Seguridad quien tomará las medidas oportunas en comunicación con el auditor de datos.

Como ya se ha advertido con anterioridad, se vuelve a reiterar que, sobre todo en el caso de que un usuario ejercite cualquiera de sus derechos reconocidos en el RGPD, todas las bases de datos deberán actualizarse según haya el afectado modificado, suprimido, limitado o ejercitado su oposición al tratamiento de sus datos personales.
Para facilitar la centralización de la información, se ha articulado un sistema por el que se informa a los afectados de que los derechos podrán ejercitarlos mediante el envío de un correo ordinario a SOLITIUM.

En todo caso, deberán ser los receptores primarios de estos correos (el Responsable de Seguridad o la persona que este haya designado) los que se encarguen de distribuirlos internamente entre todos los usuarios con accesos informáticos a las bases de datos personales a efectos de que el contenido de los diferentes ficheros quede actualizado.

3.2.1. El derecho de acceso.

Se ejercerá mediante petición o solicitud dirigida al Responsable del Tratamiento, formulada por escrito con acuse de recibo en el que conste el fichero o ficheros a consultar.

El interesado podrá solicitar a SOLITIUM y obtener información sobre los el plazo previsto de conservación o los criterios para determinarlo, la existencia del derecho a suprimir, rectificar, limitar u oponerse al tratamiento, el derecho a presentar una reclamación ante la autoridad de control, información sobre el origen de los datos y la existencia de decisiones automatizadas. Para ello, deberá enviar una solicitud por escrito donde indique su nombre, apellidos, D.N.I., domicilio, fecha y firma. Deberá adjuntar fotocopia del D.N.I. ya que, en caso contrario, se denegará dicha solicitud. En el supuesto de que faltase cualquier otro dato de los mencionados, el responsable solicitará la subsanación por parte del solicitante.

Si el afectado solicitase un formulario para realizar la solicitud, se le facilitará un modelo.

El afectado podrá optar por uno de los siguientes sistemas de consulta del tratamiento, siempre que sea posible:

- Escrito, copia o fotocopia remitida por correo.
- Fax.
- Certificado emitido por el Encargado del Tratamiento con la aprobación del Responsable.

Ante dichas solicitudes, el Responsable del Tratamiento contestará por escrito en el plazo de un mes, a contar desde la recepción de la solicitud.

Si la resolución fuese estimatoria, el acceso a la información se hará efectivo en el plazo de diez días siguientes a dicha notificación.

Se producirá la denegación del acceso a los datos de carácter personal registrados en ficheros de titularidad priva-da, cuando la solicitud se formule por persona distinta del afectado. En caso de que el afectado sea incapaz, se entenderá capacitado para ejercer sus derechos quien ostente la representación legal suficiente basada en escritura o sentencia judicial.

3.2.2. El derecho de rectificación.

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Para ello, deberá enviar una solicitud por escrito donde indique su nombre, apellidos, D.N.I., domicilio, fecha y firma. Deberá adjuntar fotocopia del D.N.I. ya que, en caso contrario, se denegará dicha solicitud. En el supuesto de que faltase cualquiera de los datos mencionados anteriormente, el Responsable solicitará la subsanación por parte del solicitante. Si el afectado solicitase un formulario para realizar la solicitud, se le facilitará un modelo. La rectificación se hará efectiva sin dilación indebida y se efectuará la notificación al interesado acerca de dicha rectificación.

3.2.3. El derecho de supresión.

El interesado podrá solicitar, si procede, del Responsable del Tratamiento la supresión de sus datos personales, cuando dichos datos sean ya no sean necesarios para los fines con los que se recogieron, el interesado retire el consentimiento en que se basa el tratamiento, el interesado se oponga y no prevalezcan intereses legítimos, los datos hayan sido tratados ilícitamente, los datos deban suprimirse en cumplimiento de obligaciones legales o los datos se hayan obtenido en relación con oferta de servicios de la sociedad de la información.

Para ello, deberá enviar una solicitud por escrito donde indique su nombre, apellidos, D.N.I., domicilio, fecha y firma. Deberá adjuntar fotocopia del D.N.I. ya que, en caso contrario, se denegará dicha solicitud. En el supuesto de que faltase cualquiera de los

datos mencionados anteriormente, el Responsable solicitará la subsanación por parte del solicitante.

Si el afectado solicitase un formulario para realizar la solicitud, se le facilitará un modelo. La supresión se hará efectiva por el Responsable del Tratamiento a más tardar en el plazo de un mes desde la recepción de la solicitud. Dentro de dicho plazo, se efectuará la notificación al interesado acerca de dicha supresión. En caso de que el Responsable del Tratamiento considere que no procede acceder a lo solicitado por el afectado, se lo comunicará de modo motivado dentro del plazo señalado con anterioridad, a fin de que el afectado pueda ejercitar la reclamación prevista en el artículo 18.1 de la RGPD ante la Agencia de Protección de Datos.

Por último, si transcurriese el plazo señalado en el párrafo anterior sin que se respondiera de forma expresa al afecta-do, podrá entenderse desestimada a los efectos de la interposición de la reclamación correspondiente.

3.2.4. El derecho de oposición.

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, aparta-do 1, letras e) o f) del RGPD, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el trata-miento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Con la finalidad de facilitar el cumplimiento de la normativa en Protección de Datos, todas las dudas o consultas sobre la materia podrán ser remitidas al Responsable de Seguridad de SOLITIUM que se encargará de hacerlas llegar a quien se precise para que las resuelva finalmente.

3.2.5. El derecho de limitación.

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a.- el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b.- el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c.- el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d.- el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, RGPD mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Si el afectado solicitase un formulario para realizar la solicitud, se le facilitará un modelo. Con la finalidad de facilitar el cumplimiento de la normativa en Protección de Datos, todas las dudas o consultas sobre la materia podrán ser remitidas al Responsable de Seguridad de SOLITIUM que se encargará de hacerlas llegar a quien se precise para que las resuelva finalmente.

3.2.6. El derecho de portabilidad.

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado al responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), del RGPD y

b) el tratamiento se efectúe por medios automatizados.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Con la finalidad de facilitar el cumplimiento de la normativa en Protección de Datos, todas las dudas o consultas sobre la materia podrán ser remitidas al Responsable de Seguridad de SOLITIUM que se encargará de hacerlas llegar a quien se precise para que las resuelva finalmente.

3.3. Política de Gestión de Derechos

Existe una Política de Gestión de Derechos en el SGPDP que regula el contenido y alcance de los mismos según el RGPD y que amplía y regula el contenido de este Manual.