Política de Seguridad de la Información

Referencia:	POLI Politica Seguridad Informacion y Privacidad-V6.doc
Autor:	Comité Seguridad y Privacidad
Versión:	06
Clasificación:	Pública

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
04	17/11/2023	Comité de Seguridad	Firmas del nuevo Comité de Seguridad
05	23/11/2023	Comité de Seguridad	Modificaciones puntos 2.6, 15
06	12/07/2024	Comité de SIP	Requisitos ENS

Lista de distribución

Está política, se encuentra al alcance de todas las partes interesadas en la INTRANET de Solitium y en nuestra página WEB.

Control de firmas

Aprobado por:	
MIQUEL ESCOLÀ	PILAR TORRADO
Presidente del Comité Responsable de Seguridad y Privacidad	Secretario del Comité Responsable de la Información

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 GRUPO 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 GRUPO SOLITIUM

SOLITIUM adopta un sistema de gestión integrado, en el que se incluye la Seguridad y Privacidad de la información 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.

GRUPO SOLITIUM, 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 y privacidad de la información y establecer una política de seguridad y privacidad, en el uso de medios electrónicos para conseguir una protección adecuada en GRUPO SOLITIUM.

3. Objetivos de la Política de Seguridad y Privacidad

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

a) Garantizar a los usuarios que los datos alojados en GRUPO 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 GRUPO SOLITIUM, que cubra en un ciclo continuo de mejora los aspectos técnicos, organizativos y procedimentales.
d) Hacer patente el compromiso de GRUPO SOLITIUM con la seguridad y privacidad de la información mediante su apoyo al Comité de Seguridad y Privacidad dotándole de los medios y facultades necesarias para la realización de sus funciones, para lograr el cumplimiento de la legislación aplicable de protección de IIP (Información de Identificación Personal) y los contratos acordados con todas las partes interesadas.
e) 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 GRUPO SOLITIUM.
f) Garantizar la continuidad de los servicios ofrecidos por GRUPO SOLITIUM a los usuarios.
g) Crear y promover de manera continua una “cultura de seguridad y privacidad” 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.
h) Promover el compromiso en la Mejora Continua de los Sistemas de Gestión de Seguridad y Privacidad de la información de nuestras Partes Interesadas, objetivo primordial para nosotros, todo ello dentro del contexto de la organización y apoyando su dirección estratégica.

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 Privacidad y aprobada y difundida por GRPO SOLITIUM para que la conozcan todas las partes interesadas.

En caso de conflictos o diferentes interpretaciones de esta política se recurrirá al Comité de Seguridad y Privacidad 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 y privacidad TIC.

Debido al carácter personal y reservado de la información manejada y a los servicios puestos a disposición de los usuarios, GRUPO 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 311/2022, de 4 de abril, 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 GRUPO 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 y privacidad TIC

La política de seguridad y privacidad TIC de GRUPO 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 y privacidad 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 y privacidad TIC.

j) Principio de mejora continua o de la reevaluación periódica: se revisará el grado de eficacia de los controles de seguridad y privacidad 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 y privacidad 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 y Privacidad

Esta política de seguridad y privacidad 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 y privacidad: La estructura organizativa para la gestión de la seguridad y privacidad de la información será competente para mantener, actualizar y hacer cumplir, la Política de Seguridad y Privacidad de la información de GRUPO SOLITIUM, así como para garantizar el correcto funcionamiento del Sistemas de Gestión de seguridad y privacidad.

b) Análisis y gestión de los riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad y privacidad. 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 y privacidad, 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 y privacidad. Al evaluar el riesgo en relación con la seguridad y privacidad 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 y privacidad de los sistemas recibirá la formación específica necesaria para garantizar la seguridad y privacidad 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 privacidad 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 y privacidad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. La seguridad y privacidad de la información 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 GRUPO 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 y privacidad 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. Este uso de dispositivos móviles no debe conducir a un compromiso de la IIP (Información de Identificación Personal). También forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por GRUPO SOLITIUM.

k) Prevención ante otros sistemas de información interconectados: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad y privacidad, 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 y privacidad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad y privacidad. Así como se recuerda la obligación y concienciación de la notificación de estos, y de las posibles consecuencias para la organización, el personal y el interesado de incumplir las reglas y procedimientos de seguridad y privacidad, especialmente aquellos que abordan la gestión de IIP (Información de Identificación Personal).

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 con las necesidades de nivel de servicio de sus usuarios.

o) Mejora continua del Sistema de Gestión de seguridad y privacidad: Las medidas de seguridad y privacidad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad y privacidad de la información 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 y privacidad TIC será considerada objetivo común de todas las personas al servicio de GRUPO 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 y privacidad indicadas en la presente política y las obligaciones derivadas de ellas, GRUPO 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 y privacidad, quedan desarrolladas en la presente política algunas de las funciones de los órganos que GRUPO SOLITIUM estima necesarios para la correcta gestión de la seguridad y privacidad.

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

8.2. Comité de Seguridad y Privacidad

1. Se crea el Comité de Seguridad y Privacidad de GRUPO SOLITIUM, como órgano colegiado de carácter transversal para la coordinación y gobierno en materia de seguridad y privacidad.
2. El Comité estará formado por un presidente, un secretario y una serie de vocales que representan las unidades de GRUPO SOLITIUM.

3. Serán funciones propias del Comité:

    a) Definición, aprobación y seguimiento de los objetivos, iniciativas y planes estratégicos en seguridad y privacidad 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 y privacidad TIC al órgano competente para su reglamentaria tramitación.

    d) Establecimiento de directrices comunes y supervisión del cumplimiento de la normativa en materia de seguridad y privacidad 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 y Privacidad 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 será el encargado de dar respuesta a incidentes TIC, deberá realizar la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad y privacidad de los sistemas de información críticos de GRUPO SOLITIUM.

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

8.3. Responsable de Seguridad y Privacidad

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

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

- Promover y participar en el desarrollo e implantación de la política de Seguridad y Privacidad de la Información, normativas, procedimientos, estándares y directrices asociados a la Seguridad y Privacidad de la Información.

- Gestionar la Seguridad y Privacidad de la Información en línea con las directrices generales que emanan de la Política de Seguridad.

- Establecer canales de comunicación con los diferentes agentes que intervienen en la Seguridad y Pirivacidad de la Información.

- Coordinación de responsables técnicos para la implementación de las políticas y procedimientos de seguridad dentro de la organización.

- Ostenta la propiedad de las políticas y procedimientos de seguridad aprobados por el Comité de Seguridad y Privacidad, así como de aquellos registros de auditoría, registro de eventos, incidencias, inventario, etc. generados en la gestión de los sistemas de información.

- Realización de un informe anual sobre la gestión realizada en materia de seguridad durante el año corriente, estrategias para el próximo ejercicio, auditorías realizadas, incidencias destacables, etc. para su aprobación por el Comité de seguridad y Privacidad.

- Proponer al Comité de Seguridad y Privacidad la implantación de cualquier control o salvaguarda que en materia de seguridad pudiera surgir en función de las incidencias ocurridas o necesidades detectadas.

- Mantener contacto con grupos de interés, asesores y autoridades en materia de seguridad informática para mantener actualizados los conocimientos de la compañía en esta materia y promover posibles iniciativas.

- En caso de necesidad por cumplimiento legal, ostenta la figura de responsable del Plan de Contingencias y por tanto su propiedad asegurándose de su comunicación a los responsables afectados, su mantenimiento gestionar su actualización y la realización de las oportunas pruebas.

- Colaborar en impulsar proyectos relacionados con la Seguridad de la Información y Privacidad, promoviendo aquellos que pudieran cubrir las necesidades de la entidad.

- Escalar cualquier conflicto o aspecto no resuelto que afecte a varias áreas o departamentos al Comité de Seguridad de la Información y Privacidad.

- Realizar periódicamente un análisis de riesgos que permita la identificación del nivel de exposición (vulnerabilidades) frente a las amenazas que afecten a la entidad e identificar las opciones o líneas de actuación que permitan reducir los riesgos a un nivel aceptable.

- Identificar qué leyes, normativas o reglamentos pueden tener incidencia, en términos de Seguridad de la Información y Privacidad con el fin de evaluar su impacto y proponer las medidas que resulten de aplicación.
- Aportar su visión en el uso de la metodología de análisis de riesgos.
- Colaborar en la definición un Plan de Análisis del Riesgo para la gestión y mejora continua de la Seguridad de la Información y Privacidad.
- Participar activamente en el diseño de un sistema de gestión de la Seguridad de la Información y Privacidad.
- Contribuir al diseño de acciones de concienciación y sensibilización relativas a la seguridad y dirigidas a todo el personal.
- Establecer y gestionar un sistema de gestión de incidencias que responda a las necesidades de la entidad.
- Realizar recomendaciones, en el ámbito de su responsabilidad, al Comité de Seguridad de la Información y Privacidad.
- Verificar que los esfuerzos en materia de Seguridad de la Información y Privacidad son consistentes y coherentes de cara a SOLITIUM identificando duplicidades o ámbitos no cubiertos.
- Gestionar la revisión periódicamente la efectividad de los controles implantados en la infraestructura tecnológica.
- Verificar la vigencia y actualidad de los planes de continuidad de negocio, llegado el caso.
- Revisar la efectividad de los planes de concienciación y sensibilización del personal en materia de Seguridad de la Información y Privacidad.
- Actuar como contacto de referencia en la organización en aspectos relacionados con la Seguridad de la Información y Privacidad.
- Presentar los resultados del análisis de riesgos al Comité de la Seguridad de la Información y Privacidad.
- Analizar las incidencias de seguridad y resultados de la monitorización de actividades identificando aquellos aspectos que pudieran ser relevantes para informar al Comité de la Seguridad de la Información y Privacidad.
- Reportar cualquier otro aspecto que por su relevancia o criticidad debiera ser conocido por el Comité de la Seguridad de la Información y Privacidad.

En el caso de GRUPO SOLITIUM se concreta la función en una persona.

8.4. Oficina de Seguridad y Privacidad

1. La Oficina de Seguridad y Privacidad estará compuesto por técnicos de las diferentes unidades de GRUPO 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 y Privacidad estará también el Responsable de Seguridad y Privacidad de GRUPO SOLITIUM que tendrá funciones sobre la revisión y elaboración de propuestas para ser presentadas y debatidas en el Comité de Seguridad y Privacidad TIC.

3. La Oficina de Seguridad y Privacidad 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 y Privacidad TIC.

    b) Asesoramiento en la elaboración de propuestas relativas a la revisión del marco normativo de seguridad y privacidad 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 y Privacidad TIC de informes periódicos sobre el estado de la Seguridad TI del IIS.

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

8.5. Otros Responsables

El responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El responsable de la información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
El Esquema Nacional de Seguridad asigna al responsable de la información la potestad de establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de Seguridad y Privacidad de la Información
En el caso de GRUPO SOLITIUM se concreta la función en una persona.

Aunque la aprobación formal de los niveles corresponda al responsable de la información, se puede recabar una propuesta al responsable de la seguridad y privacidad y conviene que se escuche la opinión del responsable del sistema.
La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Esquema Nacional de Seguridad.
Los criterios de valoración es importante que estén respaldados por esta Política de Seguridad y Privacidad de la Información en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

El responsable del Sistema tiene las funciones generales de:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad y Privacidad, antes de ser ejecutada.

En el caso de GRUPO SOLITIUM se concreta la función en una persona.

El ENS asigna al **responsable del Servicio** la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
En el caso de GRUPO SOLITIUM, tiene la forma de órgano colegiado en el Comité de Seguridad y Privacidad.

La prestación de un servicio siempre debe atender a los requisitos de Seguridad y Privacidad de la Información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

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 y Privacidad

9.1. Instrumentos del desarrollo

La Política de Seguridad y Privacidad de la información de GRUPO 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 y privacidad 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 y privacidad se hará de acuerdo a lo dispuesto en la presente política y las normativas específicas que para ello desarrollará GRUPO SOLITIUM.

9.3. Sanciones previstas por incumplimiento

Del incumplimiento de la Política de Seguridad y Privacidad de la información 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 y privacidad de la información afecta a todos los miembros de GRUPO 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 GRUPO 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 ocurra 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 GRUPO 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 GRUPO 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 GRUPO SOLITIUM o que de alguna manera se presten bajo el control y/o la dirección de GRUPO SOLITIUM tienen la obligación de conocer y cumplir esta Política de Seguridad y Privacidad de la información y la Normativa de Seguridad y Privacidad. GRUPO 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 GRUPO 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.

El personal deberá limitar al mínimo necesario la impresión de documentos que incluyan datos IIP (Información de Identificación Personal).

15. Terceras partes

Cuando GRUPO SOLITIUM preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad y Privacidad de la información, 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 y privacidad. Para GRUPO SOLITIUM el contacto del Delegado de Protección de Datos es **privacidad@gruposolitium.es.**

Cuando GRUPO SOLITIUM utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y Privacidad 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 y privacidad, 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 y Privacidad de la información 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.