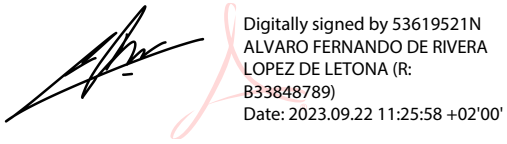
POLÍTICA DE SEGURIDAD

Índice de contenidos

Revisiones

Nº revisión	Fecha	Descripción del cambio	Autor/a
01	11/09/2023	Redacción inicial	Comité de Seguridad Óscar Iglesias Touceda

Aprobaciones

Comité de Gestión	Dirección
Fecha 11/09/2023	Fecha 11/09/2023
Firma  José Luis Fernández	Firma  Digitally signed by 53619521N ALVARO FERNANDO DE RIVERA LOPEZ DE LETONA (R: B33848789) Date: 2023.09.22 11:25:58 +02'00' Álvaro de Rivera

1 Política de Seguridad del Sistema de Gestión de Espiral MS

Espiral MS considera que la información es uno más de los activos relevantes para ofrecer productos y servicios a nuestros clientes y, por tanto, requiere de una protección adecuada. Por tanto, Espiral MS incluye la Gestión de la Seguridad de la Información dentro de su Sistema de Gestión como mecanismo para establecer directrices claras y medidas de seguridad para:

- garantizar la confidencialidad[1], integridad[2] y disponibilidad[3] de la información,
- garantizar el cumplimiento de los requisitos de seguridad establecidos por la propia organización y los acordados con sus clientes,
- garantizar el cumplimiento de la legislación, regulaciones y estándares aplicables,
- garantizar la continuidad de la organización y su operativa de negocio.

La infraestructura que soporta los servicios, así como la información y las aplicaciones que gestionan los servicios prestados por Espiral MS se encuentran dentro del alcance del Sistema de Gestión de la Seguridad de la Información, que está integrado en el Sistema de Gestión, por lo que le son de aplicación las políticas, objetivos y procedimientos allí establecidos.

La aplicación utilizada para la gestión de los activos y el análisis de riesgos permite evaluar el riesgo por servicio. Para ello, se han definido los servicios incluidos en el Sistema de Gestión y se ha identificado qué activos de información intervienen en cada uno de ellos.

El personal de soporte interno de Espiral MS es el responsable de establecer y mantener las medidas de seguridad necesarias para la correcta provisión de los servicios. Cualquier incidencia de seguridad en los sistemas que soportan el servicio, deberá ser informada y registrada.

1.1 Objetivo

El objetivo de esta Política de Seguridad de la Información es establecer directrices claras y medidas de seguridad para proteger la información confidencial de la organización, garantizar la disponibilidad y

[1] El atributo confidencialidad se define como la garantía de que sólo aquellos actores (entidades, personas o procesos) autorizados a acceder a la información pueden acceder en el modo y forma previstos.
[2] El atributo integridad se define como la garantía de que la información no es alterada inadecuadamente durante su almacenamiento, tratamiento o tránsito.
[3] El atributo disponibilidad se define como la garantía de que la información puede ser accedida, en el modo y forma previstos, por aquellos actores autorizados cuando así lo requieran.

confiabilidad de los sistemas de información, y cumplir con las regulaciones y estándares de seguridad aplicables.

La Política de Seguridad es de obligado cumplimiento para todo el personal. Es además de aplicación en todo el ámbito establecido en el Marco indicado a continuación.

1.2 Marco

1.2.1 Actividad empresarial

El grupo Espiral MS es un grupo empresarial fabricante de software constituido en 1998 y con alta actividad internacional. Tiene presencia en más de 15 países a través de oficinas propias o socios comerciales que les representan.

1.2.2 Líneas de negocio

Espiral MS se dedica fundamentalmente a dos áreas de actividad:

a) Proactivanet: es una solución para gestionar activos y servicios TI (ITAM & ITSM).

b) Prosafety: es una herramienta para la gestión de la seguridad laboral.

1.2.3 Estrategia organizativa

Espiral MS enfoca sus actividades empresariales desde tres pilares maestros: la importancia de la calidad, la importancia de la gestión de los servicios de TI, y la adecuada Seguridad de la Información. En consecuencia, ha implantado un Sistema de Gestión para cada uno de los tres ámbitos, en base a estándares y buenas prácticas internacionales.

Asimismo, Espiral MS entiende que el comportamiento empresarial socialmente responsable es un factor estratégico que contribuye de forma esencial al desarrollo y a la sostenibilidad del negocio.

Los elementos anteriores junto con un equipo humano especializado y de alta capacitación, contribuyen a la búsqueda de oportunidades y la consecución de los resultados esperados por la organización, siempre alineados con su misión, visión y valores.

1.3 Alcance

La política de seguridad es de obligado conocimiento y aceptación por parte de todos los trabajadores de **Espiral MS**. Por ello será puesta a su disposición en todo momento en la Intranet, de modo que pueda ser fácilmente accedida y consultada siempre que se necesite.

Todo empleado de Espiral MS deberá leer y aceptar de forma escrita la política de seguridad de **Espiral MS** antes de desempeñar ninguna labor profesional que implique el manejo de aplicaciones, servicios, sistemas o información de la compañía.

1.4 Responsabilidades

La **alta dirección** es responsable de establecer un entorno de seguridad adecuado, asignar recursos y autoridad para implementar las medidas de seguridad. En **Espiral MS** hay un claro compromiso con la Seguridad de la Información, expresado en la delegación de algunas de sus funciones clave en el Comité de Seguridad

El **personal de la organización** debe cumplir con las políticas y procedimientos de seguridad, informar acerca de cualquier incidente o brecha de seguridad que sea de su conocimiento a la mayor brevedad posible, y participar en programas de capacitación y concienciación cuando así se determine.

1.4.1 Comité de Seguridad

La seguridad de la información es un ámbito especialmente complejo por requerir conocimientos de distintas disciplinas, tanto técnicas como legales y de gestión. Siendo una cuestión transversal y, conscientes de su importancia creciente, Espiral MS cuenta con un Comité de Seguridad que tendrá, entre otras, las siguientes funciones:

- Gestionará y mantendrá la política de seguridad de la organización.
- Será el punto de comunicación y referencia para cuestiones internas y externas en materia de seguridad de la información y ciberseguridad.
- Ostentará las responsabilidades y funciones en materia de protección de datos (DPO).
- Realizará la revisión de las cuestiones técnico-jurídicas en materia de seguridad, ciberseguridad y protección de datos que se requieran en distintos procedimientos (RFI, Licitaciones, contratos, auditorías, etc.).

- Será el encargado de identificar y nombrar personas con responsabilidades en materia de seguridad en la organización, tanto a nivel funcional como en la relación con clientes con demandas específicas, como Defensa, por ejemplo.
- Liderará el Análisis de Riesgos y la elaboración del Plan de Tratamiento de Riesgos al que se refiere la ISO 27001, involucrando a los responsables de procesos y propietarios de activos y servicios en la identificación de dichos riesgos, y el establecimiento de acciones de mitigación, y/o advirtiendo sobre los mismos a la Dirección, que, como último responsable de la gestión del riesgo, será quien asumirá dichos riesgos.
- Promoverá el establecimiento de políticas y estándares de seguridad, siendo el responsable de revisar las políticas y estándares de seguridad de la organización. Esto implica establecer directrices claras y medidas de seguridad para proteger los activos y la información de la organización.
- El comité será responsable de promover y asesorar la ejecución de las evaluaciones de riesgos de seguridad periódicas o de carácter extraordinario para identificar las vulnerabilidades y amenazas potenciales en los sistemas, la infraestructura y los procesos de la organización. Además, fomentará la participación de todos los miembros de la organización, especialmente los responsables de procesos, en la gestión proactiva y la mitigación de los riesgos identificados.
- El comité supervisará la implementación de las cuestiones reflejadas en la política de seguridad y en los documentos relacionados en toda la organización. Esto incluye asegurarse de que se sigan las prácticas adecuadas de seguridad y que se cumplan los estándares establecidos.
- El comité puede revisar y aprobar los cambios y proyectos que afecten la seguridad de la organización. Esto podría incluir la implementación de nuevas tecnologías, actualizaciones de sistemas o sugerencias de modificaciones en los procesos de seguridad existentes.
- El comité será responsable de promover programas de formación y concienciación en seguridad para el personal de la organización, de la difusión de información sobre buenas prácticas de seguridad y la promoción de una cultura de seguridad en toda la organización.
- La organización proporcionará programas de capacitación y concienciación en materia de seguridad de la información para todos los empleados, con el objetivo de promover buenas prácticas de seguridad y concienciar sobre los riesgos asociados con el phishing, el malware y otras amenazas.
- El comité puede promover evaluaciones periódicas del desempeño de seguridad de la organización y recomendar mejoras. Esto puede incluir revisiones de seguridad, auditorías internas y la implementación de controles y medidas adicionales para fortalecer la postura de seguridad de la organización.

1.5 Compromisos

El Comité de Seguridad impulsará la implementación de todos los controles organizativos, procedimentales, físicos y lógicos que sean necesarios para proteger adecuadamente los activos de información de **Espiral MS**, mediante lo indicado en esta política u otros elementos del cuerpo normativo (políticas derivadas,

procedimientos, líneas base, instrucciones técnicas, etc.), y canalizándolos hacia las diferentes áreas y procesos de negocio.

En Espiral MS la importancia de la Seguridad de la Información se manifiesta de manera más concreta en:

- Compromiso con la confidencialidad: La compañía se compromete a proteger la confidencialidad de la información, garantizando que solo las personas autorizadas tengan acceso a ella. El acceso a los sistemas y datos debe ser restringido y otorgado solo a los usuarios autorizados en función de su función y necesidad de conocimiento. Y se deben implementar controles de autenticación oportunos.
- Compromiso con la integridad de la información: La compañía se compromete a garantizar la integridad de la información, evitando cualquier modificación o alteración no autorizada.
- Compromiso con la disponibilidad de la información: La compañía se compromete a garantizar la disponibilidad continua de la información para los usuarios autorizados. Esto implica la implementación de medidas de protección contra interrupciones y fallos, aplicando los planes de continuidad de negocio oportunos.
- Compromiso con la adecuada respuesta ante incidentes de seguridad: la compañía ha establecido un proceso de gestión de incidentes que incluye la notificación, investigación, respuesta y recuperación de incidentes de seguridad. La organización procurará implementar todas aquellas mejoras que puedan ayudar a prevenir futuros incidentes similares.
- Compromiso con la gestión de riesgos: La compañía se compromete a identificar, evaluar y gestionar los riesgos de seguridad de la información.
- Compromiso con la protección de la privacidad: La compañía se compromete a proteger la privacidad de la información personal de los individuos, cumpliendo con las leyes y regulaciones de protección de datos aplicables y obteniendo el consentimiento adecuado cuando sea necesario.
- Compromiso con la educación y concienciación: La compañía se compromete a concienciar y formar en seguridad de la información a todos los empleados, así como la promoción de buenas prácticas en el uso de los recursos tecnológicos.
- Compromiso con la supervisión y cumplimiento: La compañía se compromete a realizar auditorías internas y externas periódicas para garantizar el cumplimiento de las políticas y estándares de seguridad. Además, se compromete a tomar medidas oportunas cuando se identifiquen violaciones de seguridad.
- Compromiso con la mejora continua: La compañía se compromete a revisar y mejorar de forma continua los controles de seguridad de la información, considerando los avances tecnológicos, las nuevas amenazas y las lecciones aprendidas de incidentes anteriores.
- Compromiso con la colaboración externa: La compañía se compromete a colaborar con organismos y entidades externas, como agencias gubernamentales y organizaciones de intercambio de información sobre amenazas, para compartir información relevante y colaborar en la lucha contra el cibercrimen.

2 Políticas de Gestión de Seguridad de la Información

2.1 Gestión de Activos y servicios

El Comité de Seguridad liderará y ayudará a los propietarios de los activos de información y servicios en el cumplimiento de la Política de Seguridad.

2.2 Clasificación de la Información

Una política de clasificación de la información es fundamental para establecer cómo se categoriza y se maneja la información dentro de una organización.

La clasificación y gestión en base a niveles permitirá evitar la pérdida, robo o transferencia a entidades no autorizadas.

Toda la información ha de ser clasificada. De no hacerse explícitamente, se considerará por defecto que la información es confidencial. En caso de duda, se consultará al data owner o al Comité de Seguridad.

Adicionalmente, todos los empleados y colaboradores externos firmarán un compromiso de confidencialidad previamente al ejercicio de sus funciones y tener acceso a información alguna.

Independientemente de que esté etiquetada o no de forma electrónica, los empleados de Espiral MS manejarán la información necesaria para su trabajo conforme a los siguientes criterios de clasificación por niveles.

- Datos sin importancia

  Definición: La información catalogada como datos sin importancia, puede asociarse a la información pública, es decir, aquella que no requiere ningún nivel especial de protección y puede ser divulgada a terceros sin restricciones.

  Características:

  - No contiene información sensible o confidencial.
  - No está sujeta a regulaciones de privacidad o protección de datos.
  - Su divulgación no representaría un riesgo significativo para la organización.

  Ejemplos: información de contacto general, información disponible en el sitio web público.

- Datos sin clasificar menores

Definición: La información catalogada como datos sin clasificar menores, puede asociarse a la información interna de la compañía que no requiere ningún nivel especial de protección y puede ser divulgada a terceros sin restricciones, por ejemplo, catálogos comerciales.

Características:

- Puede contener información de la empresa.
- El acceso no está limitado a empleados y contratistas.
- Su divulgación no representaría un riesgo significativo para la organización.

Ejemplos: Documentación de marketing, catálogos comerciales, etc.

- Información Interna

Definición: La información interna es aquella que está destinada al uso interno de la organización. Requiere ciertos controles de acceso y protección, pero puede circular libremente por el interior de la compañía.

Características:

- Puede contener información interna de la empresa, como políticas, procedimientos y documentos internos.
- El acceso está limitado a empleados y contratistas.
- La divulgación no autorizada puede afectar la eficiencia y la reputación de la organización.

Ejemplos: Memos internos, políticas y procedimientos internos, informes internos…

- Información Confidencial

Definición: La información confidencial es aquella que requiere un nivel más alto de protección debido a su sensibilidad y potencial impacto negativo si se divulga o se accede de manera no autorizada. Restringida a determinados individuos o equipos de trabajo.

Características:

- Contiene información sensible, como datos personales, secretos comerciales o información financiera confidencial.
- El acceso está restringido a un grupo selecto de empleados con una necesidad legítima de conocerla.
- La divulgación no autorizada podría resultar en pérdidas financieras, daño a la reputación o violaciones de la privacidad.

Ejemplos: Información financiera confidencial, datos de clientes, acuerdos de confidencialidad, investigación y desarrollo…

- Información confidencial de segundo nivel (secreta)

Definición: La información confidencial de segundo nivel (secreta) es la categoría de mayor nivel de clasificación y abarca los datos más sensibles y críticos para la organización.

Características:

- Contiene información altamente sensible, como secretos comerciales, datos de investigación innovadora o información clasificada.
- El acceso está estrictamente controlado y se limita a un grupo extremadamente reducido de personas con autorización especial.
- La divulgación no autorizada puede tener consecuencias graves para la organización, como pérdidas financieras significativas, impacto legal, daño grave a la reputación o amenazas a la seguridad nacional. Ejemplos: Planes de producto futuros, estrategias competitivas, datos de M&A´s o investigación altamente confidenciales, información gubernamental clasificada…

2.3 Transmisión de la Información

Espiral MS aplicará los controles y procedimientos de seguridad oportunos para la transmisión segura de la información, de acuerdo a su nivel de clasificación.

2.4 Seguridad Física y del Entorno

Espiral MS aplicará los controles y procedimientos de seguridad oportunos para garantizar la protección de la seguridad física y del entorno de la empresa.

2.5 Equipos Informáticos, Comunicaciones y Software

Con el fin de asegurar el correcto desempeño de los empleados de Espiral MS en el uso y operación de los equipos y programas software, Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen el uso adecuado de equipos informáticos y dispositivos.

2.6 Dispositivos móviles

Espiral MS podrá definir la modalidad y perfil de acceso de los empleados con respecto a la información de la compañía en terminales móviles, y en su caso definir en políticas derivadas las responsabilidades y obligaciones correspondientes a cada una de ellas, y aplicará los controles y procedimientos de seguridad oportunos.

2.7 Identificación y autenticación

Las necesidades de acceso a la información se definirán a nivel de área funcional, y a los empleados se les facilitará la mínima imprescindible para realizar su labor en buenas condiciones. Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen la correcta identificación y autenticación para el acceso a la información por parte de los empleados en función de la clasificación de la información.

2.8 Gestión de contraseñas

La contraseña es uno de los elementos principales para la autenticación de los empleados y el acceso a dispositivos, sistemas y servicios de IT. Por ello deben observarse las recomendaciones y políticas establecidas por la organización en la creación, renovación y protección de la misma.

Se proporcionará capacitación y concienciación a los empleados sobre la importancia de elegir contraseñas seguras, protegerlas adecuadamente y seguir las directrices establecidas al respecto.

2.9 Revisión de derechos de acceso

Los privilegios de acceso a sistemas, servicios, aplicaciones e información deben realizarse siempre observando el principio de mínimos privilegios. Debido a los cambios que se producen en las organizaciones, como pueden ser altas, bajas y movimientos de personal horizontales y verticales, son frecuentes los desajustes en roles y permisos de usuario, normalmente por exceso.

Con la periodicidad que se defina, los responsables funcionales revisarán que los permisos concedidos a los usuarios son adecuados.

2.10 Acceso a la Red

Se prohíbe el acceso a la red corporativa, ya sea a sus sistemas, servicios, aplicaciones o información, a usuarios no autorizados.

Aquellos individuos ajenos a la organización que necesiten conexión a Internet desde las oficinas de Espiral MS, lo harán a través de la red Wifi de invitados que no dará acceso a la red corporativa o bien por sus propios medios.

2.11 Controles Criptográficos y Certificados Digitales

Se utilizarán mecanismos de cifrado en los siguientes supuestos:

- Requisitos legales o contractuales.
- Necesidades para la operativa de negocio

Los controles criptográficos y certificados digitales estarán a disposición únicamente de los empleados que los necesiten. Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen el correcto uso de los mismos.

2.12 Seguridad en el Entorno Cloud

Espiral MS considera los elementos de seguridad para la prestación de servicios en modo cloud. Se emplearán controles de seguridad, para riesgos derivados de la tipología del servicio manteniendo protección frente a accesos indebidos, violaciones de datos, con una gobernanza adecuada.

La organización proporcionará programas de capacitación y concienciación en materia de seguridad de la información para todos los empleados, con el objetivo de promover buenas prácticas de seguridad y concienciar sobre los riesgos asociados con el phishing, el malware y otras amenazas

Espiral MS tiene en cuenta la gestión de los riesgos en el entorno cloud, en base a la diferenciación de cómo se diseñan, cómo funcionan y cómo se gestionan y acceden los recursos, y especialmente el proceso de gestión del cambio. El entorno cloud tiene sus propios tipos de fuentes de riesgo. Se considerará la responsabilidad de cada parte ante la gestión compartida de los requisitos de seguridad.

Espiral MS establecerá pautas de seguridad para mantener el aislamiento en los activos e información del servicio cloud, y garantizará una gestión adecuada de accesos y autenticación en el entorno cloud. De la misma manera, se aplicarán todos los controles técnicos pertinentes para alcanzar un nivel de seguridad adecuado al riesgo.

Espiral MS, cuenta con procedimiento de devolución de la información de los clientes, incluyendo la eliminación segura tras la finalización de la relación comercial y los plazos de retención de dicha información.

Espiral MS mantendrá una gestión adecuada de eventos, investigaciones y análisis, realizando un adecuado tratamiento de los incidentes de seguridad, cumpliendo los más altos estándares recomendados por las mejores prácticas del mercado internacional.

Para la prestación de los servicios cloud, Espiral MS contará con proveedores de referencia en el ámbito internacional, mediante la evaluación y selección de proveedores de servicios en la nube confiables y seguros. Esto implica considerar aspectos como su reputación, las medidas de seguridad implementadas, sus certificaciones de seguridad y la capacidad de cumplir con los requisitos regulatorios aplicables.

2.12.1 Matriz de responsabilidades Cloud

Tratando específicamente del servicio Cloud, ESPIRALMS ha establecido la siguiente matriz de responsabilidades que resultará de aplicación al servicio ofertado a los clientes que cuenten con esta modalidad de licenciamiento:

		ESPIRAL MS	CLIENTE	PROVEEDOR (AWS)
	RESPONSABILIADES ASOCIADAS A SERVICIOS CLOUD			
Seguridad en los servicios	**Política de seguridad servicios cloud**	x		x
	Pautas de seguridad para los usuarios.	x	x	
	Determinación de los niveles de seguridad requeridos por la INFORMACIÓN implicada en el servicio		x	
	Determinación de los niveles de seguridad requeridos por el servicio (IaaS, PaaS, SaaS, DaaS, STaaS, DRaaS y BaaS)	x		
Información general del servicio	**Procedimientos operativos de seguridad para operaciones críticas del servicio.**	x		
	Documentación de seguridad del servicio.	x		
	Documentación cumplimiento protección de datos	x	x	
	Norma de uso administradores	x		
	Norma de uso del Software (usuarios, contraseña…)		x	
	Canales de comunicación y puntos de contacto	x		

	Norma de solicitud de copia de seguridad y restauración (todas las modalidades)	x		
	Sincronización de reloj. Sellado de tiempo.	x		
	Configuración de seguridad de la infraestructura de red: Securización de la red: Técnicas de defensa en profundidad (p. Ej., Análisis profundo de paquetes, aceleración del tráfico y holing black) para la detección y respuesta oportuna a ataques basados en la red asociados con patrones de tráfico de entrada o salida anómalos (p. Ej., Suplantación de MAC y ataques de envenenamiento por ARP) y / o ataques de denegación de servicio distribuido (DDoS).)	x		x
Dimensionamiento y capacidades	Planificación de la capacidad (procesamiento, almacenamiento, comunicación y capacitación)	x		
	Medición y seguimiento de la capacidad. Dimensionamiento y rendimiento del sistema.	x		
	Control de la disponibilidad	x		
Planificación de la seguridad: seguridad	Control de seguridad, amenazas y vulnerabilidades del sistema (antivirus, antimalware y otros protocolos)	x		
	Detección de intrusiones. Análisis y Registros asociados a la red.	x		x
Planificación de identidades y accesos. Mecanismo de autenticación y autorizaciones	Protocolo de proveedor gestión identidades y control de accesos	x	x	
	Controles de Acceso al servicio / infraestructura. Múltiples factores. Gestión de identidades.	x	x	
	Controles de Acceso al servicio / infraestructura. Gestión de identidades.	x	x	
	Política de derechos de acceso. Gestión de derechos de Acceso. ID, Roles, permisos, revocación, modificación, suspensión.		x	
	Acceso al servicio. Derechos y obligaciones. Ultimo acceso. Información suministrada.	x	x	
	Accesos privilegiados. Control, registro y protección	x	x	
	Autorizaciones de acceso de terceros.	x	x	
	Revisiones autorizaciones y accesos al servicio.	x	x	
	Interconexiones con terceros o plataformas.	x	x	

	Gestión de claves. Configuración, control de acceso y supervisión.	x	x	
	Gestión de claves. Uso y custodia.	x	x	
Monitorización	Gestión de logs y trazabilidades. Configuración.	x		x
	Gestión de logs y trazabilidades. Registro de eventos para operaciones privilegiadas.	x		x
	Gestión de logs y trazabilidades. Registro acciones de monitoreo.	x		x
	Gestión de logs y trazabilidades. Revisiones.	x		
	Gestión de logs y trazabilidades. Acceso cliente a logs.		x	
	Gestión de logs y trazabilidades. Retenciones	x		x
	Gestión de Logs aplicación. *SaaS: Solo sobre la app*	x		
	Gestión de alertas y eventos. Correlación. *a) IaaS: solo para infraestructura (proveedor). Maquinas cliente* *b) SaaS: Solo sobre la app* *c) PaaS: Solo sobre la parte de la plataforma.*	x		
Continuidad del servicio	Política de copias de seguridad. Alcance y calendario de las copias de seguridad: - métodos de copia de seguridad y formatos de datos, incluido el cifrado, si procede; - períodos de retención de datos de respaldo; - ubicación de almacenamiento de copias de seguridad.)	x		
	Política de restauración - procedimientos para verificar la integridad de los datos de respaldo; - procedimientos y plazos involucrados en la restauración de datos de apoyo; - procedimientos para probar las capacidades de respaldo;	x		
	Política de retención de copias	x		
	Sanitización. Borrado.	x		
	Planes de continuidad	x		
	Suspensión temporal del servicio	x		x
	Control de seguridad, amenazas y vulnerabilidades del sistema (antivirus y otros protocolos)	x		x

	Política criptográfica. Cifrado adecuado.	x		x
	Restitución de la información.	x		
	Metadatos y etiquetado de datos	x		
	Planes de concienciación y formación	x	x	
Gestión de cambios y actualizaciones	Ciclo de vida del servicio: especificación, arquitectura, desarrollo, operación, cambios	x		
	Requisitos de interconexión	x		
	Procedimiento de migraciones al sistema	x		
	Protocolo de actualizaciones, parches y mantenimiento.	x		
Protección de aplicaciones	Política de desarrollo seguro	x		
	Pruebas de aceptación y puesta en servicio. (Análisis de vulnerabilidades y pruebas de penetración)	x		
	Pruebas de aceptación y puesta en servicio. (Análisis de coherencia y auditoria de código)	x		
Gestión de incidentes	Gestión de incidentes de seguridad (preventiva)	x		
	Respuesta a incidentes de seguridad (reactiva). Coordinación cliente / proveedores.	x	x	x
	Seguimiento de incidentes de seguridad	x		x
	Notificación de incidentes de seguridad a autoridades competentes	x	x	x
	Gestión de evidencias y cadena de custodia.	x	x	x
Gestión de suministros y proveedores	Gestión de la cadena de suministro	x		
	Acuerdos de nivel de servicio.	x		
	Comunicación cambios o suspensiones acuerdos de nivel de servicio.	x		
Auditoria y revisiones	Auditoría y supervisión de los sistemas. Supervisión de las medidas de seguridad	x		x
	Auditoría y supervisión de los sistemas. Requisitos legales, normativos y necesidades.	x		x
	Protección de servicios y aplicaciones web	x		x

2.13 Uso de Correo Electrónico

Espiral MS establecerá una política de uso de correo electrónico para proteger la información confidencial y garantizar la Seguridad de la Información, que establece directrices claras para manejar adecuadamente la información sensible, previene la divulgación no autorizada, y promueve prácticas de seguridad que ayudan a mitigar ciberataques como el phishing o la introducción de malware.

2.14 Filtrado de contenidos maliciosos

Para asegurar en la medida de lo posible el bloqueo y supresión de contenidos potencialmente dañinos, Espiral MS incluye en su operativa las medidas de seguridad pertinentes.

2.15 Desarrollo Seguro

Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen el desarrollo seguro, como parte de las actividades de negocio.

2.16 Escritorio Limpio y Zona de Trabajo Despejada

Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen el establecimiento de una política de escritorio limpio y zona de trabajo despejada.

2.17 Mantenimiento de archivos y equipos y uso razonable de recursos

Cada usuario es responsable del uso profesional de los recursos que la organización pone a su disposición, y de la conservación y uso de los dispositivos que se le asignen y sean propiedad de Espiral MS, que aplicará los controles y procedimientos de seguridad oportunos que permitan un uso responsable, garantizando la seguridad de la información almacenada en los mismos.

2.18 Seguridad en el acceso por terceros

Hoy en día la gestión adecuada de la cadena de suministro es crucial. En este concepto se engloban proveedores de hardware y software, servicios en la nube, desarrollo, outsourcing o intercambios de información con terceras entidades (empresas o clientes). En ese sentido, desde Espiral MS se pondrá especial atención en:

- La adecuada evaluación de proveedores antes de establecer relaciones comerciales.
- A nivel contractual, se procurará cuando sea posible la inclusión de cláusulas de seguridad en los contratos con proveedores para garantizar la protección de la información y los activos de la empresa.
- Espiral MS aplicará los controles y procedimientos de seguridad oportunos que garanticen la seguridad de sus sistemas y la información almacenada por parte de terceros.

2.19 Gestión de incidencias

Los empleados están obligados a elevar inmediatamente un incidente de seguridad en base a los procesos establecidos en cuanto tengan constancia de cualquier incidencia a nivel físico (agua, fuego, etc.), de servicios o suministros (luz, agua, comunicaciones), o de software o sistemas (pérdida de datos, presencia de virus, ser víctima de un ataque de phishing, etc.) que puedan tener impacto a nivel de Seguridad de la Información.

Espiral MS tiene un plan de continuidad de negocio para minimizar el impacto ante eventos disruptivos, comunicado a los roles involucrados, y sus empleados se comprometen a informar a sus responsables o al Comité de Seguridad a través de los cauces reglamentarios en caso de cualquier incidente.

2.20 Normativa

Todo el personal cumplirá sus obligaciones considerando las directrices establecidas en esta Política y el resto de documentos que componen el Sistema de Gestión, y la compañía se compromete al cumplimiento de la legislación que le resulte de aplicación, así como del cumplimiento de los contratos vigentes.

Asimismo, los empleados y colaboradores se comprometen expresamente al uso y tratamiento de los datos personales adoptando las precauciones necesarias para garantizar el nivel de seguridad exigido por el marco legal vigente en materia de Protección de Datos de Carácter Personal, así como al aseguramiento de los derechos y libertades de los interesados cuyos datos se gestionan.

3 Sanciones

El incumplimiento de las Políticas de Seguridad de la Información y del resto de políticas recogidas en el sistema de Gestión, podrá dar lugar a sanciones disciplinarias, que se aplicarán de conformidad con lo recogido en la legislación laboral aplicable en cada momento, y con lo establecido en las políticas internas de la compañía.

4 Registros y documentos asociados

- Conjunto de documentación del Sistema de Gestión.