POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Realizado por			Revisado y aprobado por	
Responsable de Seguridad			Dirección	
CONTROL DE VERSIONES				
Versión	**Fecha modificación**	**Fecha revisión**	**Observaciones**	**Aprobado**
01	16/12/2025	11/02/2026	Implantación	19/02/2026

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIO

AP Interactive Solutions S.L. tiene como misión proporcionar servicios de infraestructura cloud, servicios técnicos de ciberseguridad (auditorías, pentesting, gestión de vulnerabilidades, respuesta a incidentes), desarrollo de software personalizado y servicios gestionados para clientes públicos y privados, así como la operación de plataformas SaaS propias.

El objetivo de AP Interactive es ser un referente en servicios técnicos de ciberseguridad e infraestructura cloud, cumpliendo con los requisitos de las normativas de seguridad como la ISO 27001 y el Esquema Nacional de Seguridad (ENS), estableciendo una mejora continua en el Sistema de Gestión de Seguridad de la Información (SGSI) que minimice riesgos, cumpla con las normativas vigentes y refuerce la confianza de nuestros clientes y socios estratégicos.

Por todo ello, el fin del presente documento es garantizar que se proteja la información, propia y de terceros, a un nivel adecuado.

Este documento se aplica a todo el alcance del SGSI; es decir, a todos los tipos de información, independientemente del formato, ya sean documentos en papel o electrónicos, aplicaciones y bases de datos, conocimiento de las personas, etc.

AP Interactive depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Esto implica que la organización debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Disposiciones Generales:

- Revisión: Esta política será revisada y, si procede, actualizada al menos anualmente o tras cambios significativos en el contexto de la organización o los requisitos normativos.
- Difusión: Se comunica a todo el personal y partes interesadas relevantes, asegurando su comprensión y aplicación.
- Aprobación: Firmada y aprobada por dirección como muestra de su compromiso.

2. MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades de AP Interactive, en lo que seguridad de la información se refiere, está constituida por la siguiente legislación:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

- Real Decreto 951/2015, de 23 de octubre, Esquema Nacional de Interoperabilidad (ENI)
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- 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, RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD (sustituye a 15/1999).
- Ley 11/2020, de medidas urgentes en el ámbito de la ciberseguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 40/2015, de 1 de octubre del Régimen Jurídico del Sector Público.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.

El mantenimiento del marco normativo será responsabilidad de la empresa, y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Así mismo, la empresa también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

3. CUMPLIMIENTO DE LOS ARTICULOS ENS

AP Interactive, para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados y el tamaño de la organización.

Seguridad como un proceso integral (artículo 6) y mínimo privilegio (artículo 20)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a la empresa estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica (artículo 10)

La empresa ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas con relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 15) y profesionalidad (artículo 16)

Todos los miembros de AP INTERACTIVE dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad.

Dado el tamaño de AP INTERACTIVE la formación se adaptará al rol específico de cada miembro, siendo más intensiva en desarrollo seguro para desarrolladores y en gestión de riesgos para el Responsable de Seguridad.

Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 25), prevención, detección, reacción y conservación (artículo 8)

AP INTERACTIVE ha implementado un proceso integral de detección, reacción y recuperación frente a incidentes de seguridad mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la empresa, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios.

La empresa, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Punto de contacto designado para comunicaciones sobre incidentes.
- Protocolo para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones con CCN-CERT.
- Medios y técnicas que permitan garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 9) y prevención ante otros sistemas interconectados (artículo 23)

La empresa, ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle:

- Se gane tiempo para una reacción adecuada frente a los incidentes.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Se minimice el impacto final.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas, y se controlará su punto de unión.

Diferenciación de responsabilidades (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)

La empresa, ha organizado su seguridad comprometiendo a todos los mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 17)

La empresa, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 18)

Dado que AP INTERACTIVE opera en modelo 100% remoto, la protección de instalaciones se adapta a este contexto mediante:

- Control de acceso físico a equipos personales (cifrado de disco, bloqueo automático)
- Responsabilidad individual de cada miembro sobre la seguridad física de su espacio de trabajo
- Políticas de teletrabajo seguro
- Prohibición de trabajar con información sensible en espacios públicos no seguros.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 19)

Para la adquisición de productos, la empresa, tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen.

Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)

La empresa, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Registros de actividad y detección del código dañino (artículo 24)

La empresa, ha habilitado registros de la actividad 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. Todo ello con la finalidad exclusiva de lograr el cumplimiento del ENS, con plenas garantías del derecho a la intimidad, y de acuerdo con la normativa sobre protección de datos personales.

4. PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001 y en el Esquema Nacional de Seguridad, así como al cumplimiento de la legislación vigente en materia de protección de datos personales (RGPD) y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar a la empresa.

AP INTERACTIVE aplica los siguientes principios:

- Alcance estratégico: La seguridad de la información deberá contar con el compromiso y apoyo de los miembros de AP Interactive de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas.
- Seguridad integral: La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- Gestión de riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
- Seguridad por defecto: Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

La empresa considera que las funciones de Seguridad de la Información deberán quedar integradas en todos los miembros.

Puesto que la Seguridad de la Información incumbe a toda la empresa, esta Política deberá ser conocida, comprendida y asumida por todos sus miembros, además de cualquier tercero que acceda a los activos de la compañía.

5. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en AP Interactive se establece en la forma que se indica en el documento interno *“Descripción de puestos de trabajo”*

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Responsable de Información, establece los requisitos de seguridad de la información. (Álvaro Peréz Bech)
- Responsable de los Servicios, establece los requisitos de seguridad de los servicios. (Dylan Peréz)
- Responsable de Seguridad, mantiene y verifica el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información. (Alejandro Privado)
- Responsable del Sistema, que desarrolla, operar y mantiene el sistema de información durante todo su ciclo de vida, además de elaborar los procedimientos operativos necesarios. (Álvaro Pérez Bech)

También se ha constituido un Comité de Seguridad de la Información, como órgano colegiado, atenderá las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información, además de asesorar en materia de Seguridad de la Información.

6. MARCO ORGANIZATIVO

6.1 GESTIÓN DE LA SEGURIDAD DE LOS RECURSOS HUMANOS

Se deberá realizar la gestión teniendo en cuenta los criterios de seguridad establecidos en la Política de Seguridad de la Información, siendo este un punto clave para asegurar su cumplimiento.

Se deberán salvaguardar los requisitos establecidos en la presente Política en todo momento, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desistimiento de contratos de los empleados.

6.1.1 FORMACIÓN Y CONCIENCIACIÓN

AP INTERACTIVE deberá asegurar que los miembros reciben un nivel de formación y concienciación adecuado en materia de Seguridad de la Información en los plazos que exija la normativa interna vigente, especialmente en materia de confidencialidad y prevención de fugas de información.

Así mismo, los miembros tienen la obligación de obrar con diligencia con respecto a la información, debiéndose asegurar que dicha información no caiga en poder de personas no autorizados.

6.1.2 POLÍTICA DE ESCRITORIO LIMPIO

- Se deberá bloquear la sesión de los equipos cuando se deje el escritorio, tanto por medios manuales (bloqueo por parte del usuario), como de forma automatizada mediante la configuración del bloqueo de pantalla.
- Se deberá posicionar las pantallas de forma que no sean visibles desde ventanas o por personas no autorizadas en el domicilio. Se deberá mantener ordenado el puesto de trabajo y despejado de documentos o soportes de información que puedan ser vistos o accesibles por otras personas.

6.1.3 TRABAJO REMOTO/ TELETRABAJO

Todos los miembros de AP Interactive trabajan desde ubicaciones remotas, por lo que se establecen las siguientes medidas de seguridad:

- La VPN corporativa se utiliza para la gestión de servidores.
- El acceso a otros sistemas corporativos (repositorios, cloud, etc.) se realiza mediante conexiones seguras (HTTPS, SSH)
- Cualquier colaborador externo que requiera acceso deberá contar con autorización del Responsable de Seguridad

El equipo utilizado para la conexión en la modalidad de trabajo en remoto podrá ser propiedad de los socios. En cualquier caso, es obligatorio que el equipo cumpla con los siguientes requerimientos de seguridad:

A) Capacidad de realizar una conexión a través de una VPN.

B) Disponer de un sistema operativo actualizado con los últimos parches y actualizaciones de seguridad.

C) Software antivirus instalado.

D) Software de firewall/cortafuegos personal instalado.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad.

Para más detalle, la organización cuenta con la *Política de teletrabajo y dispositivos móviles.*

6.2. GESTIÓN DE ACTIVOS

Se deberán tener identificados e inventariados los activos de información necesarios para la prestación de los procesos de negocio de AP INTERACTIVE. Adicionalmente, se deberá mantener actualizado el inventario de activos.

Se deberá realizar la clasificación de los activos en función del tipo de información que se vaya a tratar, de acuerdo con lo dispuesto en el apartado. Clasificación de la información.

Se deberá asignar un responsable encargado de realizar la gestión propia de los activos de información durante todo el ciclo de vida. El responsable deberá mantener un registro formal de los miembros con acceso autorizado a dicho activo.

Además, para cada activo o elemento de información deberá existir un responsable o propietario, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado, correctamente clasificado y adecuadamente protegido.

6.2.1 GESTIÓN DE DISPOSITIVOS PERSONALES

AP INTERACTIVE opera bajo el modelo donde los miembros del equipo utilizan equipos personales para el trabajo diario.

De igual manera, los miembros deberán tener en cuenta una serie de requisitos establecidos en esta Política:

- Se deberán mantener el sistema operativo actualizado con los últimos parches de seguridad.

- Bloqueo automático de sesión tras 5 minutos de inactividad.
- Firewall/cortafuegos personal activado.
- Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de estos dispositivos debe ser reportada al responsable de seguridad.

6.2.2 GESTION DEL CICLO DE VIDA DE LA INFORMACIÓN

AP Interactive deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos durante cualquiera de las fases.

El ciclo de vida de un activo de información consta de las siguientes fases:

1. Creación o recolección: esta fase se ocupa de los registros en su punto de origen. Esto podría incluir su creación por un miembro de la empresa o la recepción de información desde una fuente externa. Incluye correspondencia, formularios, informes, dibujos, entrada/salida del ordenador u otras fuentes.

2. Distribución: es el proceso de gestión de la información una vez que se ha creado o recibido. Esto incluye tanto la distribución interna como externa, ya que la información que sale de la empresa se convierte en un registro de una transacción con terceros.

3. Uso o acceso: se lleva a cabo después de que la información se distribuya internamente, y puede generar decisiones de negocio, generar nueva información, o servir para otros fines. Detalla el conjunto de usuarios autorizados por la empresa a acceder a la información.

4. Almacenamiento: es el proceso de organizar la información en una secuencia predeterminada y la creación de un sistema de gestión para garantizar su utilidad dentro de la empresa. Si no se establece un método de almacenamiento para la presentación de información, su recuperación y uso resultaría casi imposible.

5. Destrucción: establece las prácticas para la eliminación de la información que ha cumplido los periodos de retención definidos y la información que ha dejado de ser útil para la empresa. Los periodos de conservación de la información deberán estar basados en los requisitos normativos, legales y jurídicos que afectan a la empresa. También deberán tenerse en cuenta las necesidades de negocio. Si ninguno de estos requisitos exige que la información sea conservada, deberá ser desechada mediante medios que garanticen su confidencialidad durante el proceso de destrucción.

La empresa deberá identificar medidas de seguridad de acuerdo con la presente Política para asegurar la correcta gestión del ciclo de vida de los activos.

6.2.3 GESTIÓN DE COPIAS DE SEGURIDAD

Se deberán realizar copias de seguridad de la información, del software y del sistema y se deberán verificar periódicamente. Para ello, se deberán realizar copias de seguridad de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiese producido ninguna actualización. En su caso, se podrá establecer una frecuencia más alta de realización de copias de seguridad, si la información a salvaguardar es de impacto alto para la empresa y/o de elevado nivel de transaccionalidad.

Como normal general, la frecuencia con la que se realizarán las copias de seguridad se determinará en función de la sensibilidad de las aplicaciones o datos, de acuerdo con los criterios de clasificación de información declarados en el anexo "Niveles de clasificación".

Las copias de seguridad deberán recibir las mismas protecciones de seguridad que los datos originales, asegurándose su correcta conservación, así como los controles de acceso adecuados.

Como norma general y siempre que sea posible, se deberá requerir que la información en las copias de seguridad esté cifrada. Este requerimiento será obligatorio para determinados tipos de información confidencial.

Se deberán realizar pruebas de restauración de las copias de seguridad disponibles y de los procesos de restauración definidos, a fin de garantizar el funcionamiento correcto de los procesos. Estas se realizarán de forma periódica y quedarán documentadas.

Se deberá establecer un período de retención de las copias de seguridad hasta su destrucción una vez terminado el periodo de existencia.

Las copias de seguridad, tanto de archivos maestros como de aplicaciones y archivos de información se deberán ubicar en lugares seguros con acceso restringido. Asimismo, las copias de respaldo se ubicarán preferentemente en un centro distinto al que las generó.

Se deberá garantizar que existe una copia de seguridad adicional de la información sensible protegida ante escritura, de forma que se garantice su integridad ante la necesidad de recuperación frente a posibles incidencias de seguridad asociadas, por ejemplo, un ransomware.

6.3 CLASIFICACIÓN DE LA INFORMACIÓN

Se deberá definir un modelo de clasificación de la información que permita conocer e implantar las medidas técnicas y organizativas necesarias para mantener su disponibilidad, confidencialidad e integridad. El modelo de clasificación deberá integrar los requisitos y condiciones establecidos en el presente apartado de la Política.

El modelo de clasificación deberá tener un responsable encargado de su actualización cuando se crea conveniente, así como de conocimiento del personal de la empresa.

La organización cuenta con más detalles en el documento interno "*Política de clasificación de la información"*, que a continuación, se transcribe un resumen.

6.3.1 TIPOS DE INFORMACIÓN

La empresa deberá clasificar la información en función del soporte en el que está siendo utilizado:

- Soportes lógicos: información que esté siendo utilizada mediante medios ofimáticos, correo electrónico o sistemas de información desarrollados a medida o adquiridos a un tercero.

6.3.2 NIVELES DE CLASIFICACIÓN

En función de la sensibilidad de la información, AP Interactive deberá catalogar la información en cuatro niveles:

- Uso público

- Uso interno
- Confidencial
- Reservada

6.3.3 GESTIÓN DE INFORMACIÓN PRIVILEGIADA

La información que se considere confidencial o reservada se deberá tratar con especial cuidado. Se deberán definir medidas de seguridad extraordinarias o adicionales para el adecuado tratado de la información privilegiada. Este tipo de información se deberá enviar cifrada y mediante protocolos seguros.

6.3.4 ETIQUETADO DE LA INFORMACIÓN

AP Interactive deberá etiquetar mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.

Se deberán etiquetar los documentos o materiales, así como los anexos, copias, traducciones o extractos de estos, según los niveles de clasificación de la información definidos en el subapartado anterior, exceptuando la información considerada de "Uso público".

Se deberá definir un proceso o procedimiento para el etiquetado de la información de acuerdo con los siguientes requisitos:

- Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.
- Asegurar que las etiquetas sean fácilmente reconocibles entre los miembros.
- Orientar a los miembros sobre dónde y cómo se colocarán o utilizarán las etiquetas, en función del proceso de acceso a la información o a los activos que la soportan.
- Indicar las excepciones en los que se permite omitir el etiquetado, sin que ello suponga una omisión del deber de clasificar la información.

Se deberá prestar especial atención y tratar con cuidado máximo el etiquetado de activos físicos que contengan información reservada o secreta, para evitar su sustracción por ser fácilmente identificable.

La empresa deberá asegurar la formación y capacitación de todos los miembros en el etiquetado de la información.

6.3.5 MANIPULACIÓN DE LA INFORMACIÓN

AP Interactive se encargará de desarrollar e implementar un conjunto adecuado de procedimientos para la correcta manipulación de la información. Se deberán adoptar las medidas necesarias para proteger la información de acuerdo a su clasificación.

La información privilegiada estará en todo momento custodiada durante todo el ciclo de vida de la misma.

6.3.6 PRIVACIDAD DE LA INFORMACIÓN

AP Interactive se compromete a proteger la privacidad de:

- Datos personales de clientes: Cumplimiento RGPD.
- Datos personales de empleados: Cumplimiento RGPD.
- Información confidencial de clientes: Acuerdos de confidencialidad (NDA).

Para más detalle en la Política de Privacidad.

6.4 PREVENCIÓN DE FUGAS DE INFOMACIÓN

La fuga de información es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

AP Interactive deberá definir procedimientos para evitar la ocurrencia de las situaciones que puedan provocar la pérdida de información, así como procedimientos de actuación en caso de que se notifique una fuga de información.

Todos los miembros reciben formación sobe prevención de fugas de información, incluyendo:

- Proceso para el manejo de dispositivos de alta criticidad conocidos
- Monitorización de red: Detección de transferencias anómalas.
- Uso del correo electrónico
- Transmisión de información de forma oral
- Uso de dispositivos móviles
- Control de dispositivos extraíbles
- Uso de Internet

6.5 CONTROL DE ACCESO

Todos los sistemas de información de AP Interactive deberán contar con un sistema de control de acceso a los mismos. Asimismo, el control de acceso se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado a los sistemas de información, incluyendo medidas como la protección mediante contraseñas.

El control de acceso se entenderá desde la perspectiva lógica (enfocado a sistemas de la información) Para más la organización cuenta con un documento interno "*Política Control de Acceso".*

6.5.1 DERECHOS DE ACCESO

La empresa deberá implementar controles de acceso que garanticen que a los usuarios sólo se les otorguen privilegios y derechos necesarios para desempeñar su función.

Los derechos de acceso deberán ser establecidos en función de:

- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: Solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

6.5.2 CONTROL DE ACCESO LÓGICO

AP INTERACTIVE deberá establecer una Política de contraseñas de acceso adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña y se encuentra más detallado en el documento interno *"Política de uso aceptable".* y deberá ser conocida por todos los miembros de la empresa.

6.6 SEGURIDAD EN LA NUBE O CLOUD

AP INTERACTIVE deberá mantener una política de trabajo en la nube que establezca las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información. Dependiendo de tipo de modelo de servicio en la nube, se deberán aplicar diferentes medidas de seguridad:

- Infraestructura: en primer lugar, se deberá asegurar que el Proveedor monitoriza el entorno para detectar cambios no autorizados. Además, se deberán establecer fuertes niveles de autenticación y control de acceso para los administradores y las operaciones que estos realicen. Por último, las instalaciones y/o configuraciones de los elementos comunes deberán estar registrados y conectados con el objetivo de obtener la trazabilidad adecuada.
- Configuración segura: Hardening de recursos cloud.
- Cifrado: Datos en tránsito y en reposo.
- Backup y DR: Estrategias de recuperación en la nube.
- Plataforma: de forma adicional a las medidas indicadas en el modelo de servicio de Infraestructura, el Proveedor del servicio deberá proporcionar mecanismos de seguridad correspondientes al ciclo de vida del software seguro, de acuerdo con el apartado 6.9 Seguridad en el ciclo de vida del desarrollo de sistemas.
- Software: de forma adicional a las medidas indicadas en el modelo de servicio de Plataforma, la empresa y el Proveedor deberán seguir OWASP (Open Web Application Security) como guía para la seguridad de las aplicaciones.

6.7 SEGURIDAD OPERATIVA

Todos los servicios de información de AP Interactive que procesan o almacenan información de su propiedad deberán contar con las medidas de seguridad oportunas que optimicen su nivel de madurez adecuado (monitorización, control de cambios, revisiones, etc). Asimismo, se deberán gestionar, controlar y monitorizar las redes de manera adecuada, a fin de protegerse de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluidos los controles de acceso a la red, protegiendo así toda la información que se transfiera a través de estos elementos y/o entornos.

6.8 SEGURIDAD EN LAS TELECOMUNICACIONES

Las comunicaciones se realizan mediante telecomunicaciones, lo que convierte su protección en un elemento crítico. Se establecerá el uso obligatorio de VPN corporativa, Firewalls para filtrado de datos, IDS/IPS para detección y prevención de intrusiones, cifrado TLS/SSL para comunicaciones, y autenticación multifactor (MFA) en servicios críticos. Las comunicaciones deberán realizarse exclusivamente a través de redes seguras quedando prohibido el uso de redes públicas sin protección VPN. Todos los miembros serán responsables de utilizar únicamente canales autorizados y reportar inmediatamente cualquier anomalía detectada en las telecomunicaciones.

6.9 SEGURIDAD EN EL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS

Toda la adquisición, desarrollo y mantenimiento de los sistemas deberá contar con unos requisitos mínimos de seguridad necesarios para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas del sector. Además, deberá realizarse una gestión de las pruebas, el seguimiento de los cambios, y el inventario del software.

AP INTERACTIVE deberá tener en cuenta la seguridad de la información en sus procesos de sistemas y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

6.10 SEGURIDAD EN LOS PROVEEDORES

Se deberá poner especial atención en evaluar la criticidad de todos los servicios susceptibles de ser subcontratados de manera que puedan identificarse aquellos que sean relevantes desde el punto de vista de la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que deban tratarse o la dependencia sobre la continuidad de negocio.

Sobre los proveedores de estos servicios se deberán cuidar los procesos de selección, requerimientos contractuales como la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, al menos, equivalentes a las que se establecen en la presente Política.

Para más detalle, la organización cuenta el documento interno "*Política de compras, gestión de proveedores y terceros*.

6.11 GESTIÓN DE INCIDENTES

Los miembros de AP Interactive tienen la obligación y responsabilidad de la identificación y notificación al responsable de seguridad de la sociedad de cualquier incidente o delito que pudiera comprometer la seguridad de sus activos de información. Asimismo, la empresa deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

Se deberá definir un procedimiento de gestión de respuesta ante incidentes, en el que se defina un proceso de categorización de incidentes, análisis de impactos de negocio y escalado por parte de la función de seguridad de la información y ciberseguridad ante cualquier incidente relacionado con la seguridad de la información.

Para más detalle, la organización cuenta con un documento interno *"Política de gestión de incidentes"*

6.12 CONTINUIDAD DE NEGOCIO

Respondiendo a requerimientos de calidad y buenas prácticas, AP Interactive deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad en la prestación de sus servicios esenciales o críticos y el adecuado manejo de los impactos sobre el negocio ante posibles escenarios de crisis, proporcionando un marco de referencia para que la sociedad actúe en caso de ser necesario.

Este Plan de Continuidad deberá ser actualizado y probado periódicamente. Además, se deberá definir y mantener actualizado un Plan de Recuperación ante Desastres alineado con la continuidad de negocio, este plan abarcará la continuidad del funcionamiento de las tecnologías de información y comunicación.

La empresa deberá encargarse de la formación y capacitación para todos sus empleados en materia de Continuidad del Negocio. La formación en materia de Continuidad del Negocio deberá ser revisada periódicamente con el objetivo de estar totalmente alineada con el Plan existente.

6.13 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

La gestión de claves criptográficas de AP Interactive establece los estándares para asegurar la creación, uso, almacenamiento, y destrucción seguros de claves criptográficas que protegen nuestra información confidencial. Esta política abarca todos los aspectos del ciclo de vida de las claves, desde su generación en entornos seguros hasta su distribución controlada, almacenamiento protegido, y eliminación segura. La responsabilidad de la gestión de claves recae en el Responsable del Sistema quien debe asegurar que las claves sean accesibles únicamente para usuarios y sistemas autorizados.

Esto incluye la gestión de los procedimientos de la gestión de claves, como son la generación, distribución y almacenamiento de claves, así como su uso, renovación, revocación y destrucción.

6.14 CUMPLIMIENTO REGULATORIO DE SISTEMAS

AP Interactive deberá comprometerse a dotar los recursos necesarios para dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable.

6.15 AUDITORIAS DE SEGURIDAD Y GESTIÓN DE VULNERABILIDADES

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo con su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Una vez identificadas las vulnerabilidades, la organización deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos.

6.16 GESTIÓN DE EXCEPCIONES

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al responsable de la Seguridad de la Información de AP Interactive. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la sociedad y, en base a la categorización de estos riesgos, estos deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

6.17 SANCIONES DISCIPLINARIAS

Cualquier violación de la presente Política de Seguridad de la Información puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el proceso interno de AP Interactive. Es responsabilidad de todos los miembros de la empresa notificar al responsable de Seguridad de la Información cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.