Código: **POL.01**	Fecha de Emisión: 14.09.2024	Versión: V3.0
Nivel de acceso: Básico	Fecha de Revisión: 14.09.2024	Pág. 1 de 6

SISTEMA INTEGRADO DE GESTION: Ambiente ☐ Calidad ☐ V/I ☐ SGSI ■	***Política de Seguridad de la Información***

REALIZADOR POR: **Responsable del SGSI**	**REVISADO POR:** **Comité de Seguridad**	**APROBADO POR:** **Comité Ejecutivo**

1. CONTEXTO

La información constituye para la práctica totalidad de los procesos de negocio de las entidades que conforman **PONS**, el hilo conductor imprescindible para la ejecución de los mismos con garantías de eficiencia y calidad, alcanzando, con ello, el cumplimiento de los objetivos estratégicos formalmente establecidos por la Dirección.

Las dimensiones principales de la seguridad de la información que deben ser garantizadas en la ejecución de cualquier proceso de negocio son:

- **Confidencialidad:** Garantiza que la información solo se encuentre accesible a personas, entidades o procesos autorizados.
- **Integridad:** Garantiza que la información es generada, modificada y eliminada solo por personas, entidades o procesos autorizados.
- **Disponibilidad:** Garantiza que la información se encuentre accesible cuando las personas, entidades o procesos autorizados lo precisen.
- **Trazabilidad:** Garantiza que la información relativa a los accesos y actividad ejecutada por personas, entidades o procesos se encuentra disponible para cualquier análisis de patrones de comportamiento anómalos que deba ser efectuado.

Por otro lado, se presentan otras dimensiones de seguridad, tales como la **autenticación de las partes** o el **no repudio** que, de igual forma, deben ser garantizadas cuando el valor de seguridad de la información en el contexto del proceso de negocio en el que esté siendo almacenada, procesada, o transmitida, así lo precise.

La Política de Seguridad de la Información se basa en la adopción de principios claros y bien definidos que aseguren el cumplimiento de las directrices estratégicas, los requerimientos legales, así como los de carácter contractual formalizados con terceros o *stakeholders* y, por tanto, se constituye como el instrumento principal en el que se apoya **PONS** para la utilización segura de las tecnologías de la información y comunicaciones.

La normativa (estándar, procedimientos e instrucciones de seguridad) que emane o se deriven de la Política de Seguridad de la Información de **PONS** pasará a formar parte de la misma una vez haya sido divulgada, siendo de obligado cumplimiento para la totalidad de los empleados y terceras partes que hagan uso de dicha información.

Los empleados serán responsables de garantizar la seguridad de la información que procesan, almacenan o transmiten en el desempeño de sus funciones, y deberán conocer, comprender y cumplir las directrices y normas relativas a la seguridad de la información, velando por la correcta aplicación de las medidas de protección habilitadas.

El acceso a la información por parte de los empleados se limitará al estrictamente necesario para el correcto desempeño de las funciones formalmente asignadas garantizando, con ello, la atención de la política de mínimo privilegio. Por tanto, los responsables de información identificados en las distintas entidades que conforman **PONS** tendrán en cuenta todas las medidas de seguridad de índole técnica y organizativa para definir y mantener los privilegios adecuados de acceso a la información, en función de las actividades de cada puesto de trabajo.

El incumplimiento de las directrices de la Política de Seguridad de la Información podría dar lugar a la aplicación de sanciones administrativas internas.

La Dirección asegurará que esta Política de Seguridad de la Información es entendida e implantada en todas las entidades pertenecientes a **PONS**, facilitando los recursos necesarios para la consecución de los objetivos definidos en este marco de actuación.

2. OBJETIVOS

La Política de Seguridad de la Información queda establecida como el documento de alto nivel que formaliza las distintas directrices de actuación en materia de seguridad adoptadas por **PONS**, y que serán desarrolladas en mayor detalle en la correspondiente normativa de seguridad elaborada a tales efectos.

Bajo esta premisa, por tanto, la Política de Seguridad de la Información contempla los siguientes objetivos principales:

- Dar cumplimiento a la normativa legal de aplicación en el ámbito de la seguridad de la información con impacto en el contexto de la actividad principal desarrollada.
- Contribuir a cumplir con la misión y objetivos estratégicos formalmente establecidos.
- Garantizar la protección adecuada de los distintos activos de información en función del grado de sensibilidad y criticidad alcanzado por los mismos (valor de seguridad de los activos de información según las distintas dimensiones consideradas, y formalizado en el correspondiente **Modelo de Valor de la Información**).
- Alinear la seguridad de la información con los requerimientos demandados por el negocio mediante la formalización y ejecución del proceso de análisis y evaluación de los riesgos a los que se encuentran expuestos los distintos activos de información, alcanzando la definición de una estrategia para la mitigación de los riesgos relacionados con el entorno de la seguridad de la información.
- Garantizar una capacidad de respuesta eficaz a eventuales incidentes de seguridad de la información, minimizando el respectivo impacto operacional, financiero y reputacional.
- Facilitar el dimensionamiento de los recursos necesarios para la correcta implantación de las medidas de seguridad de índole técnica y organizativa recogidas en la normativa de seguridad documentada a tales efectos.
- Fomentar el uso de buenas prácticas en materia de seguridad de la información, así como crear una cultura de seguridad en el contexto de la estructura organizativa.
- Impulsar la definición, implantación y mantenimiento de un Plan de Continuidad de Negocio para los procesos críticos identificados tras la ejecución del Análisis de Impacto en el Negocio *(BIA – Business Impact Analysis)*.
- Establecer los mecanismos de revisión, monitorización, auditoría y mejora continua con el objeto de mantener los niveles de seguridad oportunos demandados por el modelo de negocio.

3. ALCANCE

La Política de Seguridad de la Información contempla en su alcance la totalidad de los activos de información existentes en las distintas entidades que conforman **PONS**, y que actúan como infraestructura de soporte para la posible ejecución de sus procesos de negocio.

4. MARCO NORMATIVO

La formalización de la Política de Seguridad de la Información, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la siguiente normativa legal aplicable:

- **Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD – Reglamento General de Protección de Datos)**, 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.
- **Ley Orgánica, 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, Ley 3/2018).**
- **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSICE).**

5. PRINCIPIOS

Con el objeto de garantizar el cumplimiento de los objetivos de seguridad identificados con anterioridad, la Política de Seguridad de la Información formaliza la aplicación de determinados principios de seguridad.

5.1 SEGURIDAD COMO PROCESO INTEGRAL

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información utilizados como soporte para la ejecución de los procesos de negocio. En este sentido, por tanto, todas las actividades de seguridad serán ejecutadas bajo esta perspectiva, evitando cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en la ejecución de los procesos de negocio, y la de los responsables jerárquicos con el objeto de evitar que el desconocimiento, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad de la información.

5.2 GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno de información controlado, minimizando los riesgos hasta niveles aceptables formalizados por la Dirección.

La reducción del riesgo hasta tales niveles se alcanzará mediante la aplicación de medidas de seguridad, de forma equilibrada y proporcionada a la naturaleza de la información tratada, los

servicios a prestar y los riesgos a los que estén expuestos los distintos activos de información utilizados.

5.3 PREVENCIÓN, DETECCIÓN Y RESPUESTA

La seguridad de la información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades existentes, y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información o los servicios prestados.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección estarán orientadas a la alerta temprana de cualquier escenario de materialización de amenazas.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5.4 EXISTENCIA DE LÍNEAS DE DEFENSA

Se deberá garantizar que la estrategia de protección queda conformada por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas se vea comprometida, se pueda reaccionar adecuadamente frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que puedan propagarse.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

5.5 VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de seguridad de los activos de información permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

5.6 DIFERENCIACIÓN DE RESPONSABILIDADES

La responsabilidad de la seguridad de la información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información.

6. TERCERAS PARTES

Cuando alguna de las entidades que conforman **PONS** requiera de la participación de terceras partes para la prestación de un servicio, les hará participes de la normativa de seguridad que

sea de consideración en el contexto de dicha colaboración, quedando éstos sujetos a las obligaciones establecidas en dicha normativa.

Se formalizarán los procedimientos específicos de reporte y resolución de incidentes de seguridad que pudieran presentarse durante la prestación del servicio.

Cuando algún aspecto de la normativa de seguridad no pueda ser satisfecho por una tercera parte, se requerirá la autorización del **Responsable del SGSI** previa identificación de los riesgos en que se incurre y la forma de tratarlos, no siendo posible la formalización de la contratación con carácter previo a la obtención de dicha autorización. En cualquier caso, estas autorizaciones, en función de su categorización serán reportadas al **Comité de Seguridad** con el objeto de que se adopten las decisiones oportunas.

Las excepciones aprobadas quedarán debidamente recogidas en el **Registro de Excepciones**.

7. REVISIÓN

La Política de Seguridad de la Información será revisada anualmente por el **Comité de Seguridad** o cuando exista un cambio significativo (enfoque de la gestión de la seguridad, circunstancias del negocio, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades de control y tendencias relacionadas con amenazas y vulnerabilidades) que obligue a ello.

En el caso de que se obtenga una nueva versión de la Política de Seguridad de la Información, será precisa la aprobación formal del **Comité Ejecutivo** con carácter previo a su divulgación.

8. SANCIONES APLICABLES

El incumplimiento o violación, debidamente acreditado, de las directrices recogidas en la Política de Seguridad de la Información o en las prácticas de actuación y medidas de seguridad identificadas en la normativa derivada de ésta, podría dar lugar a la aplicación de sanciones administrativas internas.

Las excepciones a la presente Política de Seguridad de la Información deberán ser previamente justificadas mediante la aplicación de un proceso formal de aceptación del riesgo. Tales excepciones deberán ser ingresadas en el **Registro de Excepciones**, y serán monitorizadas por el **Comité de Seguridad**.

9. ENTRADA EN VIGOR

Texto aprobado por el Comité Ejecutivo el día **14 de septiembre de 2024**.

Su entrada en vigor supone la derogación de cualquier otra Política que existiera a tales efectos, así como su publicación en la Intranet corporativa.

10. CONTROL DE REVISIONES

Versión	Fecha	Cambio	Solicitado por
1.0	08/09/2021	Primera versión del documento	No aplica
2.0	19/10/2023	Cambios en el Comité de Seguridad	No aplica
3.0	01/04/2024	Actualización de versión para atender requisitos de nueva norma ISO 27001	No aplica