Política de Seguridad de la Información

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.

Política de Seguridad de la Información

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.
- 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

Los principios fundamentales que deben contemplarse a la hora de garantizar las dimensiones de la seguridad de la información son la prevención, detección, respuesta y recuperación, de manera que las potenciales amenazas existentes no se materialicen o, en caso de materializarse, no afecten gravemente a la información precisa para la ejecución de los procesos de negocio, manteniéndose en unos niveles aceptables con relación al impacto causado.

5.1 PREVENCIÓN

Como principio primario de seguridad, es preciso prevenir, y evitar, en la medida de lo posible, que la información de negocio se vea afectada por incidentes de seguridad. Para ello, se debe priorizar las medidas de seguridad de naturaleza preventiva en la estrategia de implantación considerada tras la ejecución del proceso de análisis y evaluación de los riesgos. Estos controles, así como los roles y responsabilidades formalizados en materia de seguridad con el objeto de alcanzar su debida implantación deben estar claramente definidos y documentados.

5.2 DETECCIÓN

Dado que, inevitablemente, con independencia de la formalización de una estrategia preventiva de seguridad, los activos de información pueden verse afectados por la materialización de amenazas de seguridad (incidentes de seguridad), se considera fundamental monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

Esta monitorización es especialmente relevante cuando se establecen líneas de defensa en los términos considerados por las buenas prácticas de referencia en materia de seguridad de la información y, por tanto, actúan como mecanismos de alerta temprana.

En el supuesto de que la degradación sea atribuida directamente a incidentes de seguridad deberán establecerse los mecanismos oportunos de reporte que permitan la notificación al **Responsable de Seguridad** para su análisis e investigación de la causa raíz de forma conjunta con los equipos de respuesta a incidentes.

5.3 RESPUESTA

Se deben establecer mecanismos para responder eficazmente a los incidentes de seguridad. Así, en función de la tipología de incidente acaecido, se deberá formalizar el plan de respuesta oportuno.

5.4 RECUPERACIÓN

Con el objeto de garantizar la continuidad de los procesos críticos, para los cuales, en determinados casos, no podrá aplicarse planes de respuesta a incidentes, se deben desarrollar planes de contingencia de los sistemas de información y comunicaciones como

parte del plan general de continuidad de negocio y actividades de recuperación de la organización.

6. ENFOQUE DE RIESGOS

Los activos de información que conforman el alcance de la presente Política de Seguridad se encuentran sujetos a un análisis y evaluación de riesgos, con el objeto de identificar las potenciales amenazas a las que se encuentran expuestos, evaluar el impacto asociado a la posible materialización de tales amenazas, y determinar las situaciones de riesgos que podrían derivarse.

El resultado de este análisis y evaluación de riesgos permitirá la identificación y proposición de las medidas de seguridad oportunas como estrategia para la mitigación de los mismos.

Este análisis de riesgos atiende a las siguientes características principales:

- Está basado en la aplicación de normas y metodologías de gestión de riesgos reconocidas como buenas prácticas a nivel nacional e internacional.
- Establece una valoración de referencia para la información **(Modelo de Valor de la Información)**, de tal forma que se obtengan resultados homogéneos en la ejecución de las actividades inherentes al análisis de riesgos.
- Se ejecuta con periodicidad anual, o cuando se presentan los siguientes escenarios:
    - Modificación sustancial de la información gestionada o los activos que actúan como soporte a los procesos de negocio.
    - Identificación de nuevos vectores de ataque, amenazas o vulnerabilidades asociadas al activo de información.

El **Comité de Seguridad de la Información** liderará la ejecución periódica del análisis de riesgos en las distintas entidades afectadas, planificando los recursos técnicos, humanos y económicos necesarios a tales efectos.

7. 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**.

8. 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.

9. ENTRADA EN VIGOR

Texto aprobado por el Comité Ejecutivo el día 01 de julio de 2021.

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