Conscientes de la necesidad de contar con Sistemas Normalizados de reconocimiento internacional, la organización ha alineado su Sistema de Gestión de la Seguridad de la Información (SGSI) a los requisitos de los referenciales UNE-EN ISO/IEC 27001:2017 y del ESQUEMA NACIONAL DE SEGURIDAD.

Mediante la presente política de seguridad, **COMMON MS** articula la gestión continuada de seguridad de la información, de acuerdo con los siguientes principios básicos y requisitos;

a) **Organización e implantación del proceso de seguridad.** *La organización* depende de los sistemas TIC para alcanzar los objetivos. *Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para su consecución, la organización desarrollo y mantiene un proceso de seguridad basado en los siguientes elementos:* ***Prevención, Detección, Respuesta y Recuperación****.*

a) **Análisis y gestión de los riesgos.** *Todos los sistemas sujetos a esta Política realizan análisis de riesgos, según procedimientos internos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá: Regularmente, al menos una vez al año. Cuando cambie la información manejada. Cuando cambien los servicios prestados. Cuando ocurra un incidente grave de seguridad. Cuando se reporten vulnerabilidades graves.*

b) **Gestión de personal y profesionalidad.** *Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.*

c) **Autorización y control de los accesos.** *Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo*

d) **Protección de las instalaciones.** *Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones. Gestión de activos de información inventariados, categorizados y asociados a un responsable.*

e) **Adquisición de productos.** *Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.*

f) **Seguridad por defecto.** *Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.*

g) **Integridad y actualización del sistema.** *Todos los sistemas se mantienen íntegros y actualizados según los requisitos establecidos, y gestión a través de procesos de gestión del cambio y análisis de riesgos.*

h) **Protección de la información almacenada y en tránsito.** *Toda la información es almacenada de forma adecuada, siguiendo directrices establecidas, en todas sus fases.*

i) **Prevención ante otros sistemas de información interconectados.** *El sistema proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.*

j) **Registro de actividad.** *Se registra las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.*

k) **Incidentes de seguridad.** *Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.*

l) **Continuidad de la actividad.** *Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.*

m) **Mejora continua del proceso de seguridad.** *El proceso integral de seguridad implantado es actualizado y mejorado de forma continua. Para ello, se aplican los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.*

Por ello, la Dirección se compromete a liderar y mantener un Sistema de Gestión Seguridad de la Información en la organización basado en la mejora continua y en los siguientes objetivos general:

- El serio compromiso de conocer las necesidades y expectativas de nuestros clientes y partes interesadas, para lograr su satisfacción, y de mejora continua, estableciendo y verificando el cumplimiento de los objetivos y metas anuales.
- El compromiso del cumplimiento de la legislación y reglamentación aplicable, así como de los requisitos que se suscriban.
- Asegurar la seguridad de la información propia y de nuestros clientes. Nuestra actividad implica el tratamiento de información variada como forma de ejecutar procesos básicos propios de su actividad. Sabiendo que los sistemas de información, aplicaciones, infraestructuras de comunicaciones, archivos y bases de datos, constituyen un activo importante de la empresa, la dirección prioriza la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información a la hora de definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas y organizativas y vigila el cumplimiento del marco legal, de las directivas y políticas específicas y de los procedimientos definidos.
- El compromiso por la revisión continua de las competencias y mejora continua, a fin de garantizar la calidad de los servicios y su capacidad de afrontar los retos crecientes que nos plantean nuestros clientes.

COMMON MS utiliza los sistemas TIC (Tecnologías de la información y comunicación) para la prestación de sus servicios y el desempeño de sus procesos, que deben ser administrados y regulados con la aplicación de medidas que garanticen su protección, frente a daños intencionados o de carácter accidental, que pudieran impactar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información que gestionan, teniendo en cuenta que la Organización utiliza la clasificación de uso no restringido para la considerada como pública, así como la categoría uso restringido-confidencial para los datos personales, sensibles e información operacional, indicando su adecuado manejo según lo establecido en SGSI.

Por tanto, la misión de esta Política es garantizar la calidad de la información, su disponibilidad, así como la de los activos y servicios que la sustentan, para proporcionar su uso confiable y seguro a nuestros clientes, empleando para ello técnicas preventivas, seguimiento sobre la práctica diaria, y la identificación de incidentes con su adecuada respuesta.

La colaboración de las diferentes Áreas de Negocio interno, avala la repuesta ante la posible materialización de amenazas, las cuáles, trabajan conforme a las directrices que son desplegadas desde el Sistema de Gestión de Seguridad de la Información, y el Esquema Nacional de Seguridad que engloban, Buenas Prácticas de seguridad Lógica y física, las relacionadas con el manejo de datos e información, así como vías de comunicación para incidencias, junto con la batería de medidas técnicas que corresponden al mantenimiento de Infraestructuras y Servicios TI internos.

Así pues, se constituyen procesos que permiten la prevención y detección de incidentes de seguridad, y la posterior recuperación conforme al acuerdo del Artículo 7 del Esquema Nacional de Seguridad, especificados como:

- Prevención: La Organización evita en la medida de lo posible, los incidentes de seguridad que puedan perjudicar a la información o a los servicios, mediante la implementación de las medidas mínimas especificadas por el ENS, las indicadas desde el entorno del Sistema de Gestión de Seguridad, y adicionalmente, cualquiera que sea considerada necesaria por el Área interna encargada de la gestión de la seguridad que puedan derivarse del análisis y evaluación de riesgos, vulnerabilidades y amenazas, identificando los responsables involucrados.
- Detección: Se realizan seguimientos sobre la actividad diaria, para la detección de incidentes y anomalías según lo indicado en el Artículo 9 den ENS, estableciendo mecanismos que permitan la identificación activa, el análisis y el reporte de los mismos a los responsables designados.
- Respuesta: Se dispone de procesos que posibiliten la respuesta frente a los incidentes, contando con vías de comunicación claras a disposición de las partes interesadas, y el intercambio de información en los casos necesarios con las unidades que puedan responder a emergencias.
- Recuperación: La disponibilidad de los servicios y la información se garantiza a través de planes de continuidad.

La organización de la seguridad se articula desde la creación del comité de Seguridad TIC, que queda conformado por los perfiles del Responsable de Seguridad de la Información, la Dirección o Responsable de Sistemas y el Responsable de Certificaciones (Sistemas de Gestión), que a su vez actúa en la función de secretaría, convocando las reuniones necesarias con registro de las mismas mediante actas.

Las funciones del Comité serán las siguientes:

- En lo casos necesarios, reportará al Comité de Dirección
- Coordinar y aprobar las acciones pertinentes en materia de seguridad
- Promover la concienciación y formación en seguridad de la información
- Definir la categoría del Sistema y el análisis de riesgos
- Revisión y aprobación conjunta de la documentación relacionada con la seguridad, así como de los registros asociados
- Participar en la resolución de problemas y discrepancias relacionadas con la gestión de la seguridad.

Las responsabilidades del Responsable de Seguridad, quedan definidas como:

- Mantenimiento de los niveles de seguridad adecuados para la información y servicios bajo alcance
- Gestionar la formación y concienciación en materia de seguridad
- Comprobar que las medidas de seguridad son adecuadas a los objetivos y necesidades de la Organización
- Revisar toda la documentación relacionada con la seguridad del sistema
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y medios de auditoría
- Realizar las auditorías que se considerarán necesarias en función del ENS
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta la resolución, aportando informes para el Comité en los casos relevantes
- Operar y mantener el sistema de información durante todo su ciclo de vida.
- Definir el alance del ENS, identificar los activos, su evaluación en cada dimensión y establecer la categoría del sistema.
- Revisar la evaluación de riesgos y plantear las salvaguardas, así como las medidas
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad
- El Responsable del Sistema podría proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, será tomada por el Comité de Dirección.

Las responsabilidades del Responsable de Sistemas serán las siguientes:

- Promover y organizar las auditorías periódicas según ENS en colaboración con el Responsable de Seguridad
- Describir la documentación relacionada con la seguridad
- Participar en la formación y concienciación en materia de seguridad
- Registrar y realizar el seguimiento de las incidencias de seguridad así como de los cambios que se puedan originar
- Promover las confluencias entre el SGSI y el Esquema Nacional de Seguridad
- Realizar la evaluación de riesgos y amenazas
- Dar soporte al Responsable del Sistema en la definición del alance del ENS, identificación de los activos, así como en la evaluación de los mismos.
- Colaborar con el RSI y la Dirección en cualquier tarea relacionada con la seguridad que consideren necesaria.

Las responsabilidades del Responsable de la Información serán las siguientes;

- Responsable último del uso que se haga de la información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Aprobación de los niveles de seguridad establecidos.

Las responsabilidades del Responsable del Servicio serán las siguientes;

- Responsable de establecer los requisitos de los servicios en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.

Las responsabilidades de la Dirección Responsable de Sistemas son:

- Aprobación de la documentación final de la documentación del Sistema de Seguridad
- Promover el desarrollo del Esquema
- Dotar de los recursos económicos necesarios para su desarrollo, así como de la presente Política
- Interlocutor en los casos necesarios con el Comité de Dirección

Como usuarios, la Organización entiende, a cualquier empleado o a terceros externos en aquellos casos que acontezca, que para el desempeño de su actividad diaria, dentro de las Áreas de negocio de la compañía, requieran la utilización de los Sistemas de Información, debiendo colaborar con el R. de Seguridad en todas las actividades que les sean indicadas, así como restringir el uso de los Sistemas según las especificaciones aprobadas por el R. de Sistemas. Podrán ser designados como responsables de los activos o de los riesgos, dependiendo de su implicación con los mismos.

La designación de los miembros del Comité de Seguridad TIC, se asimila al Comité de Seguridad descrito por el SGSI, siendo los encargados de cualquier actuación relativa a la seguridad históricamente dentro de la Organización.

Respecto a los datos personales, los datos recogidos dentro de la información relevante al alcance del Esquema Nacional de Seguridad, así como los tratados por lo servicios indicados pertenecen a la clasificación de tipología baja, contando la Organización según el cumplimiento exigido dentro del SGSI, con un alto desempeño mantenido mediante auditorías de los requisitos asociados a su tratamiento.

El sistema es sometido a un análisis de riesgos, que evalúa las amenazas y los niveles de riesgo registrados al que se encuentra expuesto con frecuencia anual, siempre y cuando no se produzcan incidentes graves, o cambios que pudieran alterar las condiciones iniciales respecto a la información manejada, los servicios prestados, o la aparición de vulnerabilidades.

Una vez establecidas los controles disponibles para la contención de las amenazas, el riesgo final es considerado como “riesgo residual o trivial”, estableciéndose categorías de tratamiento según su nivel.

El desarrollo de esta Política se realiza de manera complementaria a las actividades relacionadas en el ámbito del SGSI, encontrándose a disposición de todo el personal de **COMMON MS**, y constituyendo un elemento de carácter público que podrá ser comunicado tanto a proveedores como clientes.

Se organizarán jornadas de concienciación e información en seguridad para los empleados de Organización, el personal con responsabilidad en el uso, operación, o administración de sistemas TIC, recibirán la formación necesaria en las medidas de seguridad necesarias en cada caso.

En los casos en lo que **COMMON MS**, utilice a terceros para la provisión de servicios bajo alcance, transmitirá sus requisitos a través de las comunicaciones establecidas en los “Criterios de Evaluación”, clasificando a los proveedores según las características establecidas en el mismo.

Se proporcionará una vía de comunicación para que puedan transmitir de manera rápida y directa cualquier incidencia de seguridad relacionada con el servicio o la información objeto de su prestación de servicios. Cuando alguna de las terceras partes, no cumpla con los requisitos mínimos recogidos en los “Criterios de Evaluación” anteriormente citado, se solicitará su reprobación al Responsable del Área de negocio afectada.

El alcance de esta Política queda establecido como: "**Desarrollo, implementación y mantenimiento de software de gestión. Servicios de consultoría informática**", que incluye información y servicios como activos fundamentales, así como los secundarios que guardan relaciones con ellos.

Y que incluye información y servicios como activos fundamentales, así como los secundarios que guardan relaciones con ellos.
El Marco Normativo aplicable a la presente Política es los siguientes:

- ✓ Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.
- ✓ Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- ✓ 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.
- ✓ Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- ✓ Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- ✓ Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- ✓ Ley 59/2003, de 19 de diciembre, de firma electrónica
- ✓ Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- ✓ Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- ✓ Guías CCN-STIC.
- ✓ Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas) y de Auditoría de la Seguridad de los Sistemas de Información (Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública).
- ✓ UNE-ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- ✓ UNE-ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ✓ UNE-EN-ISO 9001:2015 Sistemas de gestión de la calidad.

Política de Seguridad ESN rev3
Aprobado en acta del Comité CSI – CSTI,
Fecha 30/05/2022