POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

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-ISO/IEC 27001:2014 y del ESQUEMA NACIONAL DE SEGURIDAD.

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 Ca&Ma), 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 del Servicio e Información serán las siguientes;

- 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).
- Determinar los niveles de seguridad de la información y servicio,

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 la 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.

La información documentada del sistema de gestión de seguridad de la información queda estructurada desde el "Listado de Documentos en vigor", recogiendo para cada uno de éstos, de forma inequívoca,

- Sus campos descriptivos,
- Sus campos de objeto, alcance, responsabilidades y referencias asociadas
- Así como de su campo de estado de revisión.

Toda la documentación del sistema, así estructurada, es accesible a las partes internas interesadas, desde las plataformas de comunicación internas y para las partes externas interesadas, por peticiones al área de sistemas.

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"

Y que incluye información y servicios como activos fundamentales, así como los secundarios que guardan relaciones con ellos.

El Marco Normativo general aplicable a la presente Política es los siguientes:

- 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
- 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 de Protección de Datos)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales

Le revisión de referencias legales aplicables se realiza de forma periódica (mínima anual), recogiéndose en el Anexo "Informe Listado Referencias Legales (Tipo "Seguridad de la Información").

Política de Seguridad ESN rev3, Aprobado en acta del Comité CSI – CSTI, en fecha 30/06/2020

Informe Listado Referencias Legales

Grupo

S. INFORMACION

Tipo

Seguridad Información

Ambito

EUROPEO

CODIGO	NUMERO	FECHA	FECHA ALTA	REFERENCIA	Aplica
ESSI00	**(UE) 2016/679**	**27/04/2016**	**30/01/2018**	**Protección de Datos de Carácter Personal y a la libre circulación de estos**	☑
Título	REGLAMENTO (UE) 2016/679, PROTECCION DE DATOS				

ESTATAL

CODIGO	NUMERO	FECHA	FECHA ALTA	REFERENCIA	Aplica
ESSI00	**3/2018**	**05/12/2018**	**30/01/2018**	**Protección de Datos de Carácter Personal.**	☑
Título	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.				
ESSI09	**9/2014**	**09/05/2014**	**30/01/2018**	**General de Telecomunicaciones**	☐
Título	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. (Texto consolidado. Última modificación: 7 de marzo de 2016).				
ESSI04	**3/2010**	**08/01/2010**	**30/01/2018**	**Esquema Nacional de Seguridad**	☐
Título	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. (Texto consolidado. Última modificación: 4 de noviembre de 2015).				
ESSI11	**899/2009**	**22/05/2009**	**30/01/2018**	**Carta de derechos del usuario de los servicios de comunicaciones electrónicas**	☑
Título	Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas. (Texto consolidado. Última modificación: sin modificaciones).				
ESSI02	**1720/2007**	**21/12/2007**	**30/01/2018**	**Reglamento de desarrollo de la Ley Orgánica 15/1999**	☑
Título	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (Texto consolidado. Última modificación: 8 de marzo de 2012).				
ESSI12	**1/2006**	**08/11/2006**	**30/01/2018**	**Sistemas de cámaras o videocámaras**	☐
Título	Instrucción 1/2006, de 8 de noviembre, aepd, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. (Texto consolidado. Última modificación: sin modificaciones).				
ESSI08		**28/04/2005**	**30/01/2018**	**Delitos informáticos**	☑
Título	Código Penal. Artículos relativos a delitos informáticos. (Texto consolidado. Última modificación: 28 de abril de 2015).				
ESSI01	**62/2003**	**30/12/2003**	**30/01/2018**	**Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social**	☐
Título	Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social. (Texto consolidado. Última modificación: 30 de octubre de 2015).				
ESSI05	**59/2003**	**19/12/2003**	**30/01/2018**	**Firma electrónica**	☑
Título	Ley 59/2003, de 19 de diciembre, de firma electrónica. (Texto consolidado. Última modificación: 2 de octubre de 2015).				

Informe Listado Referencias Legales

Grupo

ESSI06	**209/2003**	**21/02/2003**	**30/01/2018**	**Registros y las notificaciones telemáticas**	☐
Título	Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas				
ESSI10	**34/2002**	**11/07/2002**	**30/01/2018**	**Servicios de la sociedad de la información y de comercio electrónico**	☑
Título	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. (Texto consolidado. Última modificación: 10 de mayo de 2014).				
ESSI07	**4/1997**	**04/08/1997**	**30/01/2018**	**Utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad**	☐
Título	Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. (Texto consolidado. Última modificación: sin modificaciones).				
ESSI13	**1/1996**	**12/04/1996**	**30/01/2018**	**Ley de Propiedad Intelectual**	☑
Título	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.				
ESSI03	**428/1993**	**26/03/1993**	**30/01/2018**	**Estatuto de la Agencia Española de Protección de Datos**	☐
Título	Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos. (Texto consolidado. Última modificación: 5 de noviembre de 2008).				