8. POLÍTICA DE CIBERSEGURIDAD

1. Síntesis de la Política

El objetivo de esta Política es establecer los requisitos bajo los cuales, cada uno de los miembros de Gestión de Servicios Residenciales, S. Coop. y Sociedades dependientes (en adelante, nos referiremos de forma genérica a "GSR"), ha definido esta política teniendo en cuenta los desarrollos normativos impulsados desde la Unión Europea y su proyección en nuestro país, así como las recomendaciones, prácticas y estándares establecidos por las autoridades de supervisión y organismos de reconocido prestigio.

Los principios básicos establecidos en la presente Política permitirán a GSR desplegar las estrategias, procedimientos y estándares de Ciberseguridad, alineados con los objetivos de negocio, para la protección de los datos, sistemas y operaciones de GSR.

Además, la Política persigue desplegar procesos y tecnologías que permitan al GSR ofrecer productos y un mejor servicio para los usuarios, los clientes y otros grupos de interés.

Esta Política se aplica a todos los socios, trabajadores, directivos o miembros de un órgano de administración de alguna entidad de GSR, independientemente del cargo que ocupen o de su ubicación geográfica.

Así mismo, la presente Política es aplicable a los terceros de la cadena de valor con quien GSR tenga establecido algún tipo de relación comercial (Socios de Negocio), agentes, proveedores y clientes.

Respecto a las sociedades participadas que no pertenezcan a GSR por no disponer de una participación suficiente que asegure el control, se promoverá que sus principios de actuación sean coherentes con lo establecido en esta Política, respetando siempre la legislación aplicable en cada caso.

2. Alcance.

GSR se guiará por una serie de principios básicos, que presiden la presente Política sobre Ciberseguridad:

• **Alcance estratégico**: La seguridad de la información deberá contar con el compromiso y apoyo de todos los niveles de GSR de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

• **Confidencialidad e integridad**: garantizan que la información solo sea accesible para los usuarios autorizados a acceder a ella y que no podrá ser divulgada a terceros sin la correspondiente autorización, procurando la integridad de la misma, de forma que los datos se mantengan libres de modificaciones no autorizadas y que la información existente no haya sido alterada por personas o procesos no autorizados.

• **Seguridad integral**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. 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. Los sistemas deberán diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

• **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. La reducción de estos niveles se realizará mediante

el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

• **Proporcionalidad y disponibilidad:** 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. La disponibilidad garantiza que la información y los sistemas de información estén accesibles y utilizables cuando los usuarios autorizados lo requieran.

• **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. La seguridad de la información será atendida, revisada y auditada por personal cualificado. Se promocionará en la organización la cultura de la ciberseguridad.

• **Autenticidad, trazabilidad y no repudio.** La autenticidad es la capacidad de garantizar que el origen y las identidades asociadas a la información sean realmente los que aparecen en los atributos de ésta. La trazabilidad es la herramienta que garantiza la posibilidad de determinar en cada momento la identidad de las personas que elaboran, acceden y disponen de la información y la actividad que desarrollan en relación con la misma, así como los distintos estados y rutas que ha seguido la información. Ello va unido al principio de no repudio, que asegura que el usuario no pueda negar la autoría de un acto en el sistema o la vinculación a un dato o conjunto de datos

El establecimiento, despliegue, mantenimiento y comunicación de las políticas, normas y procedimientos de ciberseguridad que son fundamentales para definir los principios, objetivos y responsabilidades en esta materia.

Estos elementos proporcionan directrices claras para el uso de la tecnología, la gestión de datos y la respuesta ante incidentes, promoviendo así la integración de la ciberseguridad en todos los ámbitos de la organización y estableciendo la ciberseguridad por diseño, tal y como se definirá más adelante, como base de nuestras actividades. Además, es esencial definir planes de formación que capaciten a toda la organización en ciberseguridad, adaptándolos a sus áreas de actividad y responsabilidad. Para complementar esto, la concienciación en materia de ciberseguridad es crucial, implicando la educación y sensibilización de todas las personas de la organización sobre los riesgos de ciberseguridad, las amenazas actuales y las mejores prácticas para prevenir incidentes.

Por otro lado, supervisar el cumplimiento de las buenas prácticas requiere establecer acuerdos claros sobre los estándares de seguridad esperados, realizar evaluaciones periódicas de los controles implementados y monitorizar continuamente el desempeño en ciberseguridad.

3. Requisitos generales

Los procesos de trabajo en GSR atenderán a los siguientes objetivos y procedimientos:

1. Gestión de la Seguridad de los Recursos Humanos El departamento de Recursos Humanos deberá realizar su 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, proporcionando un nivel de formación y concienciación adecuado en materia de Seguridad de la Información, especialmente en materia de confidencialidad y prevención de fugas de información.

2. 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.

3. Prevención de fugas de información.

4. Control de acceso Todos los sistemas de información del GSR deberán contar con un sistema de control de acceso a los mismos.

5. Gestión del ciclo de vida de la identidad GSR deberá definir e implementar un adecuado sistema de gestión del ciclo de vida de la identidad. La identidad es el conjunto de características que identifican de forma unívoca a toda persona con acceso físico o lógico a los sistemas de información del GSR. El ciclo de vida de la identidad es el proceso que sigue la identidad de un usuario desde su creación hasta su eliminación.

6. Seguridad Física y del Entorno. Se establecerán mecanismos que impidan el acceso indeseado a los equipos y documentación de GSR.

7. Seguridad en trabajo en la nube o cloud, estableciendo las medidas de seguridad adecuadas para la confidencialidad, integridad y disponibilidad de la información.

8. Seguridad en la operativa, procurando que los sistemas de información que procesan o almacenan información de su propiedad cuenten 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.

9. Seguridad en las telecomunicaciones.

10. 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.

11. Seguridad en los Proveedores 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 medir el cumplimiento de los principios y compromisos establecidos en la Política de Ciberseguridad, GSR ha definido un robusto sistema de monitorización y control basado en indicadores de rendimiento y objetivos claramente definidos a corto, medio y largo plazo.

El seguimiento periódico de los indicadores de rendimiento permite evaluar el progreso hacia el logro de los objetivos a corto, medio y largo plazo que han sido previamente definidos. Esta práctica facilita la identificación de áreas que requieren atención y mejora, posibilitando la correcta toma de decisiones y la implementación de medidas correctivas adecuadas. De esta manera, se asegura un ciclo continuo de mejora continua, y se optimiza el rendimiento y la eficiencia en todos los niveles de la organización.

Para garantizar su eficacia, los indicadores de rendimiento deben ajustarse a los siguientes criterios:

- Relevancia: Los indicadores deben medir y reflejar de manera precisa y significativa el progreso hacia el logro de un objetivo específico, proporcionando información que pueda ser utilizada para la toma de decisiones y acciones.

- Representación fiel: Las fuentes de los datos deben ser confiables, y los métodos de medición deben ser estandarizados. La información presentada a través de los indicadores debe ser completa, neutral y precisa.

- Oportunidad: La frecuencia de medición de los indicadores debe ser adecuada para la oportuna toma de decisiones.

- Facilidad de uso: Deben ser fácilmente comprensibles e interpretables tanto para quienes los recopilan como para quienes se encargan de su análisis.

- Comunicación efectiva: Los resultados de los indicadores deben ser comunicados de forma clara y concisa a todos los niveles de la organización.

4. Incumplimiento de la Política

Cualquier incidencia o acción contraria a la política de Privacidad y Confidencialidad se deberá comunicar a través de correo electrónico al link de compliance habilitado en la página Web: www.gsr.coop.