Responsabilidades de los usuarios de los sistemas de información de la CARM.

El presente documento tiene por objeto sintetizar las responsabilidades, normas y principios de uso de los Sistemas de Información de la CARM. Se dirigen a cualquier usuario de los sistemas, tanto desde dependencias administrativas como remotas, siempre que sean de aplicación. Sigue las recomendaciones descritas en la norma ISO/IEC 27002:2005.
El conocimiento y respeto por parte de los usuarios de estas indicaciones es parte de las políticas y principios que en materia de seguridad deben regir en los sistemas de información de la Administración General de la Comunidad Autónoma de la Región de Murcia.

USO APROPIADO.- El usuario empleará los sistemas de información para fines propios de su trabajo, siempre respetando las políticas y normas particulares de uso.

CONFIDENCIALIDAD Y NO DIVULGACIÓN.- El uso de la información y de los sistemas debe ser el adecuado para que se asegure la confidencialidad y no divulgación de la información, en los términos de:
http://rica.carm.es/chacp/areaSeguridad/doc/AcuerdoConfidencialidadyNoDivulgacionUsuarios(1.0).pdf

USO DE CONTRASEÑAS.- El usuario debe tener en cuenta las siguientes indicaciones y ponerlas en práctica:

- Mantener en secreto tanto el login de acceso como la contraseña de todos los sistemas a los que acceda.
- Evitar escribirlas en papel, archivo o cualquier medio que pueda ser consultado por personas ajenas.
- Utilizar contraseñas suficientemente seguras para garantizar que sean fáciles de recordar pero difíciles de adivinar.
- Cambiar la contraseña de forma regular, como mínimo una vez al año o cada vez que considere que puede haber sido adivinada por alguien.
- Cambiar las contraseñas temporales o dadas inicialmente por un administrador.
- No incluir las contraseñas en ningún sistema que facilite su almacenamiento.
- No compartir su contraseña con ninguna otra persona.
- No usar la misma contraseña para entornos de trabajo y personales.

EQUIPO PERSONAL.- Los equipos personales de trabajo, físicos o virtuales, deben ser autorizados por el Servicio de Gestión Informática correspondiente. El usuario es responsable de poner en práctica las siguientes recomendaciones, siempre con la asistencia de su Servicio de Gestión Informática.

- Apagar el ordenador cada vez que termine su jornada laboral.
- Desconectar la sesión cada vez que haya una parada prolongada en su trabajo.
- Disponer de salvapantallas activado con contraseña.
- Mantener los sistemas de protección activos y actualizados, así como aplicar los parches de seguridad.

- Realizar copias de seguridad con cierta frecuencia para evitar la pérdida de datos importantes.

PROPIEDAD INTELECTUAL.- La Administración Regional conserva en todo momento la propiedad intelectual de trabajos, informes, desarrollos informáticos y cualquier tipo de servicio o documento elaborado, por lo que no se podrá hacer uso de los mismos para fines propios, de terceros, o para obtener beneficio o lucro.

AUDITORÍA.- La Administración Regional se reserva el derecho de auditar el uso de los sistemas de información por parte de sus empleados. En caso de detectar un riesgo para la seguridad se podrán aplicar las adecuadas medidas técnicas.

INCIDENCIAS.- En caso de que el empleado público detecte riesgos o incidentes que puedan afectar a la seguridad de los sistemas de información debe alertar a su Servicio de Gestión Informática.

INCUMPLIMIENTO.- El incumplimiento del presente código de uso de los sistemas de información puede suponer el establecimiento de medidas disciplinarias, establecidas en la reglamentación actual, así como encausamiento judicial tal como se describe en el Código Penal.

CONOCIMIENTO.- Es responsabilidad del empleado de la Administración Regional conocer este documento y consultarlo de forma periódica.

Nombre y apellidos del usuario:
Firmado:

En , a fecha