

**SOLICITUD DE ACCESO AL PORTAL DE SERVICIOS DE PREVENCIÓN DE
RIESGOS LABORALES (PORTSPRL) DEL SISTEMA DE INFORMACIÓN
SANITARIA Y VIGILANCIA EPIDEMIOLÓGICA LABORAL (SISVEL)**

☐ ALTA ☐ BAJA ☐ MODIFICACIÓN

Actividad profesional del solicitante en el SPRL Marcar todas las que correspondan:	Perfil de acceso Marcar los que se solicitan:
☐ Dirección/Gerencia	☐ Comunicación y consulta de casos de sospechas de EEPP
☐ Técnico de Prevención	☐ Iniciar expedientes administrativos
☐ Recursos Humanos	☐ Consultar expedientes administrativos
☐ Medicina del Trabajo/Empresa	☐ Noticias
☐ Otra especialidad Médica	
☐ Enfermería del trabajo/Empresa	
☐ Otro personal de Enfermería	
☐ Fisioterapeutas	
☐ Personal Administrativo	
☐ Otros (especificar):	

Solicitante	Responsable o Director/a del Servicio de Prevención de Riesgos Laborales
DNI:	DNI:
Fecha de Nacimiento:	Apellido 1º:
Apellido 1º:	Apellido 2º:
Apellido 2º:	Nombre:
Nombre:	Cargo:
SPRL:	Dirección:
Dirección:	Municipio: C.P.:
Municipio: C.P.:	Teléfono:
Teléfono:	E-mail corporativo:
E-mail corporativo:	
Fecha y Firma SOLICITANTE	Fecha, sello y Firma DIRECCIÓN o JEFATURA del SPRL
Fecha:	Fecha:
He leído y acepto las normas básicas de los recursos informáticos de la DGSP (Anexo)	Me comprometo a: - Comunicar inmediatamente las BAJAS y MODIFICACIONES - Velar por el cumplimiento de las normas de uso (Anexo)

Enviar debidamente cumplimentado a: DGSP - Av. Cataluña, 21, 46020 – Valencia, o al correo gesid_dgsp@gva.es

Consideraciones preliminares

Los recursos informáticos de la DGSP tienen la finalidad de servir como herramienta para el desempeño de las tareas que tiene asignadas el personal dependiente de la DGSP, por las características de su puesto y/o funciones.

No está permitida la utilización de estos recursos con fines personales, comerciales o recreativos (juegos, chat o conversación electrónica en tiempo real, etc.).

El uso de los servicios de red es parte integrante de numerosas actividades que se desarrollan dentro de los centros dependientes de la DGSP. Por este motivo se hace necesario establecer una serie de criterios y normas para respetar la información y el trabajo de otras personas que utilizan, de forma compartida, los mismos recursos.

Responsabilidad de los usuarios

Los usuarios se comprometen a respetar la configuración de los ordenadores que utilizan, empleando únicamente los programas instalados o/y autorizados por los servicios informáticos de la DGSP o en quien ésta delegue.

Con el fin de cumplir la normativa vigente, todas las acciones (accesos a recursos internos o externos, modificación de datos, etc.) llevadas a cabo en los equipos/aplicaciones, por parte de los usuarios, serán registradas y auditadas en los diferentes sistemas.

Legalidad

El usuario se compromete a respetar las reglas y normas de funcionamiento establecidas, tanto por los servicios informáticos, como por otros organismos e instituciones con los que puedan interactuar en el marco de las comunicaciones nacionales e internacionales. En concreto, se cumplirán escrupulosamente las normativas legales relativas a propiedad intelectual, protección de datos, etc., tanto en España como en otros países.

Especialmente, quedan prohibidas las actividades de "piratería informática" mediante introducción virus, intento de quebranto de programas o accesos de no autorizados a través potenciales fallos en la seguridad del sistema.

El software instalado en los ordenadores está registrado para su uso en la DGSP. La copia o pirateo de programas y documentación ilegal. El usuario está obligado a cumplir las leyes/normas dictadas al respecto con especial atención a:

- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal.*
- *Ley 11/2022, de 28 de junio, General de Telecomunicaciones.*
- *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*
- *Decreto 66/2012, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.*
- *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.*

Solidaridad

La utilización de los recursos y servicios de forma incorrecta puede llegar a entorpecer el trabajo de otras personas, ocasionar gastos inútiles, molestias, etc.

Si se utilizan las redes de forma indebida o abusiva, se puede estar privando a otras personas de los medios necesarios para desarrollar su trabajo. Debe evitarse la utilización indiscriminada de imágenes, vídeo, sonidos, etc., puesto que su tamaño satura las líneas de comunicaciones y disminuye la velocidad de transmisión, perjudicando a otros usuarios.

Seguridad

A los usuarios se les facilitará una cuenta de acceso a la red, así como las correspondientes a las diferentes aplicaciones a las que por sus funciones se le dé acceso.

Los usuarios no podrán utilizar los equipos informáticos hasta que no se les comunique por parte los servicios informáticos los datos de acceso, y siempre que previamente se haya solicitado el acceso a los recursos por parte del responsable del centro/área/departamento en que desempeña sus funciones el usuario.

El usuario se compromete a no acceder a los recursos a los que no esté autorizado. En caso de poder acceder a recursos a los que no debería o que no estén relacionados con el desempeño de sus funciones, deberá comunicar de inmediato a los servicios informáticos de la DGSP la anomalía para que pueda ser corregida.

Las cuentas de usuario son personales e intransferibles, quedando totalmente prohibido facilitar su utilización a terceras personas. En general las cuentas de acceso serán de uso personal por cada usuario salvo que se indique lo contrario. En casos especiales de acceso común a algún recurso y siempre previa autorización de los servicios informáticos de la DGSP podrán existir claves de uso común, responsabilizándose de las obligaciones individuales el responsable de la cuenta.

Los responsables de los centros/áreas/servicios serán los únicos habilitados para solicitar las altas/bajas/modificaciones de los accesos asignados a cada usuario. Asumiendo la responsabilidad de comunicar las bajas de usuarios inmediatamente. Estas solicitudes se realizarán únicamente utilizando los modelos de alta/baja/modificación de accesos de usuarios cuya plantilla facilitará a los responsables de los usuarios.

Los usuarios se comprometen a garantizar la privacidad de sus contraseñas, así como a evitar la difusión de las mismas. Esto muy importante, ya que es las acciones realizadas desde una cuenta de usuario (quedan registradas y asociadas al propietario de la cuenta) son responsabilidad del propietario. El usuario deberá cerrar o salir de las aplicaciones en las que se encuentre trabajando y bloquear el ordenador (pulsando las teclas Ctrl-Alt-Supr y seleccionando la opción *Bloquear estación*) al abandonar el puesto de trabajo.

Todos los equipos deben tener configurado un salvapantallas protegido por contraseña. En ningún caso, salvo autorización expresa, deben permanecer encendidos los ordenadores fuera del horario laboral. Los servicios informáticos no se responsabilizarán de los datos almacenados localmente en los ordenadores de los usuarios. Si se trata de información de uso compartido deberá permanecer en el servidor habilitado al efecto del cual se realizarán copias de seguridad diariamente.

Los equipos deberán tener instalado y activo el antivirus corporativo de la DGSP. Si detecta la ausencia o mal funcionamiento del antivirus deberá comunicarlo a los servicios de informática.

El correo electrónico

Las cuentas de correo electrónico asignadas al personal dependiente de la DGSP se proporcionan esencialmente para la satisfacción de las finalidades derivadas del desempeño de las funciones asignadas en marco del puesto de trabajo.

Las direcciones de correo electrónico referidas en punto anterior pueden ser difundidas con la indicación clara de las finalidades de estas direcciones y la advertencia expresa de que no serán utilizadas para la remisión mensajes con otras finalidades.

El usuario no debe abrir nunca ficheros o anexos a los mensajes de correo electrónico de procedencia desconocida o sospechosa, los cuales deben ser borrados directamente sin abrirlos.

En ningún caso se deben atender las indicaciones enviadas por correo por parte de compañeros/conocidos para realizar acciones en la configuración de los ordenadores amparándose en que han sido publicadas por empresas de reconocido prestigio. En la mayoría de los casos se trata de informaciones falsas que solo pretenden provocar el mal funcionamiento de los ordenadores eliminando o cambiando los ficheros necesarios para el correcto funcionamiento de los mismos.

Los únicos autorizados a remitir instrucciones de cómo realizar acciones sobre los ordenadores son los servicios informáticos de la DGSP. En todo caso y ante la duda de la procedencia las informaciones remitidas deberán ponerse en contacto con estos.