# NORMAS DE USO
# de los SISTEMAS DE INFORMACIÓN
# del Servicio Aragonés de Salud (SALUD)

(Sistema de Gestión de la Seguridad de la Información)

salud
servicio aragonés de salud
Centro de Gestión Integrada de Proyectos Corporativos

| ELABORADO POR | REVISADO POR | APROBADO POR | VERSIÓN | FECHA |
|---|---|---|---|---|
| Nuria Borque | Francisco J. Martón | Carlos Barba | 1.00a | 3 marzo 2010 |
| Nuria Borque | Francisco J. Martón | Carlos Barba | 1.00b | 8 marzo 2010 |
| Nuria Borque | Francisco J. Martón | Carlos Barba | 1.00c | 15 marzo 2010 |

# NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN de SALUD

## ÍNDICE

# 1 INTRODUCCIÓN

Este manual pretende que el trabajador del Servicio Aragonés de Salud conozca:

- Su situación respecto al uso de los sistemas de información del Servicio Aragonés de Salud (en adelante SALUD).
- Por qué la seguridad de la información es importante para el SALUD.
- Los riesgos que conllevan la inseguridad.
- Los requisitos legales actuales que obligan a garantizar la seguridad de datos.
- Las normas básicas implantadas en el SALUD.
- Recomendaciones y buenas prácticas a seguir.

## 1.1. DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

El conjunto de la estructura de ordenadores y portátiles conectados a la red informática, de impresoras, de servidores y de programas informáticos sirve para almacenar, procesar y transmitir datos e informaciones. Todos estos elementos asociados forman un sistema automatizado de información, que llamaremos abreviadamente S.I. **Dentro de este sistema tú eres el usuario de un puesto de trabajo.**

Nuestra organización tiene una gran dependencia de los sistemas informáticos; sistemas, que son a su vez vulnerables a agresiones o fallos. La necesidad de la seguridad y del control es evidente.

## 1.2. PROBLEMÁTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de un sistema de información consiste en preservar la disponibilidad, la confidencialidad y la integridad de los datos y de las aplicaciones que utilizamos. Estos factores pueden ponerse en peligro por actos voluntarios o involuntarios de origen interno o externo. Una parte importante de la pérdida se debe a errores humanos y accidentes.

**1. Problemas de seguridad física**

- Catástrofes: incendios, terremotos, inundaciones.
- Fallos en los elementos físicos: cortes de fluido eléctrico, averías en los elementos de sistema (ordenador, discos, elementos de comunicaciones, líneas telefónicas).
- Fallos en el software de base o de aplicación: mal funcionamiento de los programas, o del sistema operativo, o del control de las comunicaciones.
- Sabotajes: Destrucción de elementos físicos, daños al software del sistema, introducción de virus.

**2. Problemas de confidencialidad**

- Accesos no autorizados a informaciones confidenciales.
- Accesos no autorizados para obtener copias piratas de programas.

- Accesos no autorizados para modificar datos de aplicaciones, en provecho propio o como sabotaje (modificación y destrucción de información).

**3. Utilización indebida del ordenador**

- Juegos, trabajos particulares para otra entidad, etc.
- Permitir por ingenuidad el acceso desde el exterior a usuarios maliciosos, no autorizados por el SALUD, que adquieren el control remoto sobre un ordenador del mismo.

En nuestra sociedad tecnológica existen mecanismos adecuados de seguridad para minimizar los riesgos asociados a los problemas anteriores: protección de archivos para evitar su robo o destrucción, se elaboran leyes para proteger la intimidad, los datos de carácter personal y la propiedad intelectual.

Se pueden indicar cuatro niveles de protección:

1. **Prevención de riesgos**
2. **Detección de problemas**, cuando han fallado los mecanismos de prevención
3. **Limitación de pérdidas**: si a pesar de los controles de prevención y detección, ocurre el problema, restringir las pérdidas en lo posible.
4. **Recuperación**: planes de contingencia totalmente probados y documentados para volver a disponer del sistema de información.

**Las funciones referentes a la seguridad que debe realizar el responsable de un puesto de trabajo son:**

- El conocimiento de la propiedad de los datos a los que se accede y quiénes pueden disponer de estos datos.
- Del conocimiento de la propiedad de los datos se deduce el nivel de importancia de la información que se maneja y en función de ello se tendrá cuidado para evitar que sea visualizada, impresa, fotocopiada, duplicada, por personas no autorizadas, con atención incluso de forma especial a la que se deposita en las papeleras.
- Especial atención merece el uso de contraseñas que se describe en este documento en la sección "Criterios de Buenas Prácticas en materia de Seguridad de la información".

# 2 NORMAS DE USO DE LOS SISTEMAS DE INFORMACIÓN Y CRITERIOS DE BUENAS PRÁCTICAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

A continuación se indican las normas de seguridad que todo usuario del SALUD debe satisfacer. Estas normas se han organizado en la siguiente estructura:

- Normas generales de seguridad
- Normas para el cumplimiento de la LOPD
- Normas y criterios de buenas prácticas del uso de portátiles y dispositivos móviles
- Normas y criterios de buenas prácticas aplicables al uso de Internet.
- Normas y criterios de buenas prácticas sobre el uso del correo electrónico.
- Normas y criterios de buenas prácticas aplicables al uso de las unidades de red
- Normas y criterios de buenas prácticas sobre la gestión de contraseñas

A continuación se detallan cada una de estas secciones.

## 2.1. NORMAS GENERALES DE SEGURIDAD

Son normas para el personal en relación a la seguridad de la información del SALUD las siguientes:

- El personal del SALUD y cualquier otro personal que trabaje bajo contrato para éste deberá acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones.
- El acceso a información residente en los sistemas de información del SALUD deberá realizarse siempre haciendo uso de un identificador de usuario, personal e intransferible, y de su palabra de acceso (contraseña) que deberá permanecer en secreto en todo momento y sólo podrá ser conocida por el empleado a quien se entrega su custodia.
- Bajo esta filosofía, queda expresamente prohibida la utilización de un mismo identificador personal de usuario y de su palabra de acceso por personas distintas a las que hubiera sido asignado. Es responsabilidad de cada empleado del SALUD mantener en secreto su palabra de control de acceso y confeccionarla de forma que no sea adivinable por terceros, ya que cualquier acceso indebido con dicho identificador será responsabilidad de su propietario. El SALUD informará sobre criterios de buenas prácticas para la selección de contraseñas.
- Queda prohibido comunicar a otra persona el identificador personal de usuario y las claves de acceso a los sistemas de información. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del Responsable de Seguridad Informática (Servicio de Informática) correspondiente de su Sector, con el fin de que le asignen una nueva clave. En los casos de ausencia temporal del usuario, el responsable de su unidad directiva, podrá solicitar al Responsable de Seguridad Informático correspondiente, la asignación de los permisos necesarios a la persona por él designada a efectos de evitar la obstaculización de los trabajos en curso.
- La protección de los activos de información del SALUD es una tarea que afecta a todas las personas vinculadas directa o indirectamente con la misma. Por tanto, es responsabilidad de todos preservar la disponibilidad e integridad de la información, comunicando a las áreas competentes y por los cauces establecidos, cualquier evento o incidencia que afecte a los sistemas de información.

- El usuario está obligado a utilizar los sistemas de información del SALUD y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos del SALUD o de terceros, o que puedan atentar contra las normas sociales.
- Toda actividad realizada sobre los sistemas de información del SALUD es susceptible de ser auditada.
- El SALUD prohíbe la divulgación, duplicación, modificación, destrucción, mal uso, robo y acceso no autorizado a información propiedad del SALUD o de otras empresas y personas que le haya sido confiada.
- La utilización de los servicios de Internet y correo electrónico se llevará a cabo teniendo en cuenta que asociado al usuario está el nombre del SALUD. Consecuentemente se seguirá una ética profesional en su utilización.
- Se establece expresamente la prohibición del uso de los activos de información del SALUD para finalidades distintas a las estrictamente profesionales relacionadas con el desempeño habitual de las funciones en la misma y que no hayan sido expresamente aprobadas por la Dirección o que no tengan una justificación evidente. Esto incluye tanto la propia información (de pacientes, de terceros, etc.) como los recursos informáticos (correo electrónico, Internet, ofimática, espacio en disco, etc.).
- Debido a los peligros que tiene la utilización de software dañino o no autorizado, queda prohibida la instalación de aplicaciones que no se encuentren debidamente autorizadas por el SALUD mediante los circuitos establecidos.
    - Aplicaciones de descarga masiva utilizadas para fines no profesionales
    - Programas de mensajería instantánea no homologados
    - Acceso a redes sociales utilizado para fines no profesionales
    - Juegos on-line
    - Programas spyware

## 2.2. NORMAS PARA EL CUMPLIMIENTO DE LA LOPD

Son obligaciones de todo trabajador del SALUD, en relación al cumplimiento de la legislación vigente en materia de protección de datos las siguientes:

**Deber de secreto**

- Todo empleado debe guardar secreto de la información de carácter personal que conozca en el desempeño de su trabajo, incluso después de haber abandonado la organización.
- Todo empleado debe proteger los datos de carácter personal del SALUD que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en el propio domicilio o en otras instalaciones alternativas y tanto en equipos fijos como en portátiles.

**Identificación y autenticación de usuarios**

- Cada usuario es responsable de los accesos que se hagan con su identificador personal, por ello es necesario que la contraseña se mantenga en secreto, no comunicándola a otros usuarios.
- Cada usuario es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, debe registrarse como incidencia y proceder a su cambio. El usuario debe comunicar al Responsable de Seguridad Informática (Servicio de Informática) de su sector el olvido o sospecha de conocimiento por terceros de la contraseña.
- Cambiar la contraseña al menos anualmente

**Gestión de soportes**

- No sacar fuera de los locales del fichero ningún soporte sin ser usuario autorizado para ello por el responsable del fichero y sin el correspondiente permiso del mismo para esa extracción en concreto.
- No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso, aplicando las medidas de seguridad que se hayan establecido.
- No introducir en los locales del fichero ninguna información de carácter personal sin ser usuario autorizado para ello por el Responsable de Seguridad Informática (Servicio de Informática).
- Los documentos, disquetes y otros soportes de información deben guardarse en armarios cuando no se usen y, especialmente, fuera del horario normal de trabajo.
- La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o fuera del horario normal de trabajo.
- Los ordenadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.
- No tirar a la basura documentos con información de carácter personal o sensible sin la previa destrucción.
- No hacer copias de seguridad de ninguna información, especialmente si se trata de datos de carácter personal, salvo que sea siguiendo las instrucciones del Responsable de Seguridad Informática (Servicio de Informática).

Uso de almacenamientos removibles o memorias externas (tarjetas de memoria, USB…)

- Las memorias extraíbles utilizadas para el intercambio y copia de información son fuentes habituales de vulnerabilidad en el control de la gestión de datos personales y clínicos, pudiendo estos datos, tan sensibles, acabar en manos de personal ajeno a la prestación de asistencia o de gestión sanitaria.
- Otra debilidad provocada por el uso de este tipo de dispositivos en la infraestructura del Servicio Aragonés de Salud es la facilidad con la que, los virus informáticos y todo tipo de programas indeseados pueden afectar a las plataformas a las que se conectan dado el poco control del estado de salud y cifrado al que son sometidos.
- Por ello, el Servicio Aragonés de Salud podrá, si lo estima necesario, activar medidas de control sobre el uso de estos dispositivos en sus instalaciones, siendo recomendable, en todo caso que, si se requiriese hacer copia en algún dispositivo de almacenamiento extraíble (Tarjeta de memoria, discos externos USB, etc.) o sobre soporte CD o DVD de datos sensibles (personales y clínicos), se notifique al Responsable de Seguridad Informática (Servicio de Informática) para su adecuado inventariado y la aplicación de las medidas de seguridad que éste estime pertinentes.

**Control de los accesos físicos**

- Cuando el usuario de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su horario laboral, debe dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse, desconectándose de la aplicación o a través de un protector de pantalla que impida la visualización de los datos. Es recomendable activar el protector con Ctrl+Alt+Supr + Bloquear Equipo). La reanudación del trabajo implica la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras, faxes y dispositivos similares, debemos asegurarnos de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Si es necesario enviar por correo convencional información especialmente protegida, usar un sobre opaco y hacer el envío por un canal seguro y requiriendo confirmación fiable de recepción por parte del destinatario.
- Los usuarios deben respetar la configuración fija de aplicaciones corporativas (ofimática, antivirus,...) de los puestos de trabajo desde los que se tiene acceso a los ficheros y sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad Informática (Servicio de Informática).

**Control de accesos lógicos**

- Acceder únicamente a aquellos ficheros para los que haya sido autorizado y actuar sobre los mismos solamente con el alcance que le haya sido fijado.
- Comunicar al Responsable de Seguridad Informática (Servicio de Informática) cualquier anomalía en el sistema de control de accesos implantado.
- No instalar ningún software o programa no autorizado por el Responsable de Seguridad Informática (Servicio de Informática).
- Periódicamente el SALUD se reserva la posibilidad de hacer auditorias de configuración de los soportes para comprobar el software instalado que pueda ser dañino.

**Comunicación interpersonal**

- No se deben mantener conversaciones confidenciales en lugares públicos o en oficinas abiertas o salas de tabiques finos.
- No se deben dejar mensajes en contestadores automáticos que puedan reproducirse por personas no autorizadas, grabarse en sistemas de uso público o grabarse incorrectamente como resultado de una equivocación en el marcado.
- En relación a las máquinas fax hay que tener en cuenta:
    - El acceso no autorizado a los almacenamientos internos de mensajes para recuperarlos.
    - La programación deliberada o accidental de las máquinas para enviar mensajes a números específicos.
    - El envío de documentos y mensajes a un número equivocado, procedente de marcaje o de recuperación desde el almacenamiento de números.

**Procedimiento de gestión de incidencias**

- Cualquier usuario que tenga conocimiento de una incidencia de seguridad es responsable de su notificación al Responsable de Seguridad Informática (Servicio de Informática). El conocimiento y no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del dato de información por parte de ese usuario.

## 2.3. NORMAS Y CRITERIOS DE BUENAS PRÁCTICAS DEL USO DE PORTATILES Y DISPOSITIVOS MÓVILES

Dado el riesgo existente sobre este tipo de equipos, el usuario debe adoptar unas mínimas medidas preventivas de seguridad. Los equipos portátiles no deben:

- Abandonarse a la vista en coches particulares u otros medios de transporte utilizados.
- Dejarse a la vista en lugares públicos donde puedan ser sustraídos con facilidad.
- No se podrá utilizar un equipo portátil para trabajar con información de nivel CONFIDENCIAL en un lugar público.
- El usuario no podrá instalar software en equipo portátil entregado. Los equipos portátiles o puestos de teletrabajo homologados que vengan configurados, no podrán ser desconfigurados ni podrán instalarse en ellos ningún tipo de software no autorizado o realizar ningún tipo de manipulación cuyo objetivo sea inhabilitar cualquiera de las medidas de seguridad establecidas.
- Cuando se vaya a dejar desatendido un portátil durante un periodo largo de tiempo, por ejemplo, por una reunión, el usuario debe:
    - Cerrar la puerta de su despacho o área con llave si esta opción es posible.
    - En situaciones vulnerables como lugares públicos, salas de espera de aeropuertos, hoteles o salas de conferencia, el portátil no debe dejarse nunca desatendido.
    - No deben guardarse equipos portátiles en bolsas o maletas que puedan revelar que contienen elementos de valor en su interior para no atraer a ladrones.

- Cuando las medidas anteriores no puedan aplicarse por ser inviables o inapropiadas, el propietario del equipo es responsable de adoptar todas las medidas y precauciones que considere razonables con el objetivo de minimizar los riesgos de daño o robo del equipo.

## 2.4. NORMAS Y CRITERIOS DE BUENAS PRÁCTICAS APLICABLES AL USO DE INTERNET

En el SALUD es imprescindible el acceso a Internet para el buen funcionamiento de la organización, pero este acceso es limitado, dado que el recurso de ancho de banda y caudal también lo es.

El acceso a Internet ahorra tiempo y dinero, si realizamos un uso adecuado del mismo. La utilización de Internet, por tanto, debe ser sensata y por motivos profesionales, recordando que durante las horas de trabajo, el uso del tiempo constituye un recurso del SALUD. Así mismo, los usuarios debemos ser conscientes de que todos los contenidos de Internet quedan registrados.

Para facilitar y optimizar el uso del mismo a las personas que lo necesitan diariamente y para el desarrollo y cumplimiento de la actividad, hay instalado un equipo "Firewall" o cortafuegos que entre otras características, posibilita lo siguiente:

- Impide introducirse en nuestras redes locales a usuarios cuya dirección IP no esté incluida dentro del rango autorizado.
- Facilita el acceso a la información más habitual mediante un sistema de caché que vuelca en un ordenador y actualiza semanalmente las páginas más utilizadas por los usuarios.
- Es capaz de imprimir un informe diario con las páginas a las que se accede, tiempo dedicado, usuario, hora, tipo de contenido, etc.
- Impide la descarga masiva de ficheros de video y audio y similares, de alta capacidad y dudoso empleo para las personas que trabajan en el SALUD.
- Impide acceder a los usuarios internos de la empresa, a páginas de violencia, pornografía, pederastia, sectas, simbología nazi, grupos xenófobos, etc. Estas páginas a menudo cambian de sitio o de dirección constantemente. Es responsabilidad del usuario acceder a dichas webs.

Son **normas** aplicables al uso de Internet por parte de todo trabajador del SALUD, las siguientes:

- Los sistemas de comunicación y acceso a la Internet son propiedad del SALUD y deberán ser utilizados exclusivamente como una herramienta de trabajo.
- Las operaciones realizadas a través de Internet pueden generar responsabilidad por parte del SALUD, por lo que se reserva el derecho a auditar los accesos realizados por los usuarios a través de su sistema de información y el acceso a Internet.
- El usuario debe respetar la legislación vigente (Ley de Propiedad Intelectual, Protección de Datos de Carácter Personal) y no utilizar el acceso a Internet con fines ilícitos o delictivos (acceso, uso y difusión de sitios de contenido ilegal: pornografía infantil, odio racial, terrorismo, etc.).

Son **usos no autorizados** en relación a la utilización de Internet los siguientes:

- Navegar por páginas Web cuyos contenidos sean sospechosamente delictivos, ni acceder a sitios Web que proporcionen servicios o contenidos no autorizados o expresamente bloqueados por el SALUD.
- Debes de conocer que el SALUD tiene bloqueadas páginas que por su contenido pueden ser conflictivas o se consideran perjudiciales para la actividad desarrollada.

- Descargar contenidos protegidos por la Ley de Propiedad Intelectual sin la respectiva licencia o autorización de uso o reproducción.
- Instalar programas descargados de Internet sin la debida verificación por parte del antivirus de la no existencia de código malicioso en el programa descargado.

## 2.5. NORMAS Y CRITERIOS DE BUENAS PRÁCTICAS SOBRE EL USO DEL CORREO ELECTRÓNICO

Gran parte de los empleados/as del SALUD disponemos de una dirección de correo electrónico proporcionada por el Gobierno de Aragón. Solicítala a tu responsable en caso de necesitarla para el desarrollo de tu trabajo y no poseerla.

El acceso (vía WEB) a la misma se realiza desde cualquier sitio abriendo un navegador. La dirección para acceder es: https://webmail.aragon.es. También se puede acceder mediante clientes instalados en el PC configurados contra el Servidor de Correo Corporativo.

Una vez accedas al correo, tendrás que dar tu nombre de usuario y tu contraseña.

El correo electrónico constituye uno de los canales de comunicación interna y externa más importantes del SALUD, por ello:

- Los servicios de e-mail nos ayudan a desempeñar nuestro trabajo diario, pero su uso inadecuado o incorrecto podría ocasionarnos problemas.
- Algunos de nuestros formatos de correo, en cierta forma, representan cartas formales y podrían suponer compromisos legales. Debemos ser conscientes de que los mensajes se pueden revelar en cualquier acción legal contra el SALUD. Los mensajes enviados por e-mail los tenemos que considerar como otra forma más de comunicación, de la cual se guarda copia.
- Si recibimos algún e-mail que no sea nuestro, tenemos que notificarlo a la persona que lo ha enviado y/o redirigirlo a la persona adecuada siempre que sea posible. Además, si la información es confidencial, no debemos ni distribuirla ni usarla. Debemos comunicar estos hechos al Responsable de Seguridad Informática (Servicio de Informática) del sector correspondiente.
- El envío de e-mail tiene un coste inferior al uso del teléfono, utilicemos este sistema siempre que podamos.
- No se deben realizar envíos de información o comunicación indiscriminados.
- El sistema de correo electrónico es propiedad del SALUD y es parte íntegra de sus sistemas de información, por lo que se reserva el derecho a auditar el uso adecuado del mismo.
- El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de trabajo. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen del SALUD o de sus empleados.
- El SALUD establece las siguientes directrices en relación al envío de información mediante el uso de correo electrónico.
    - Actualmente el número máximo de destinatarios de un correo electrónico está limitado a 100 destinatarios simultáneos si accedemos desde redes internas, o a 20 si accedemos desde redes externas a la RACI. Con ello evitamos problemas de spam y de saturación de líneas. En caso de que por motivos profesionales, se necesite enviar un mensaje a más de ese número de destinatarios, se debe poner en conocimiento del responsable inmediato superior que gestionará la excepción.

- El tamaño máximo para recibir o enviar un correo electrónico concreto es de 20 Mb. Este tamaño es el del mensaje una vez procesado. Es decir antes de la codificación, la cual suele aumentar el tamaño del mensaje un 35% aproximadamente. Este tamaño es suficiente para el habitual tráfico de correos y para evitar saturaciones en la red. Para recibir/enviar cualquier tamaño superior de correo se recomienda utilizar otros soportes y/o herramientas. En caso de que sobrepasemos este límite, recibiremos un mensaje del servidor alertándonos de que nuestro correo no ha podido ser enviado por exceder el tamaño máximo de mensaje.
- Actualmente el tamaño máximo de cada buzón de correo de usuario reside en un servidor del cual se realiza copias de seguridad y cada usuario dispone de 60 Mb de espacio en el servidor. Dicho límite y su ocupación son visibles cuando el usuario accede al correo via web (webmail). Sin embargo si el usuario accede con otro programa no se le avisa de este hecho, por ello es recomendable descargar los correos electrónicos más antiguos a local para evitar que dicho espacio se llene.
- Tenemos instalado un sistema ANTISPAM contratado como servicio externo cuya url de acceso es https://antispam.aragon.es. Está basado en el producto Spamina y nos protege frente al Spam (correo basura), los virus, el phishing (suplantación de identidad) y recepción de correo malintencionado o procedente de remitentes no confiables almacenándolo en un servidor diferente al de nuestro correo. Permite la creación por usuario de listas blancas y negras para que cada usuario se gestione su propio spam, así como para que cada usuario pueda rescatar del contenedor, correos de falsos positivos.

- El SALUD es responsable de establecer las normas mediante las cuales se asignan las cuentas de correo electrónico, incluyendo las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas, los controles de acceso al servidor, los sistemas para auditar el uso del sistema, la integridad y seguridad de los datos y las comunicaciones enviadas.

Son **usos no autorizados** en relación a la utilización del correo electrónico los siguientes:

- Reenviar mensajes en cadena o rumores no fiables (Hoax). Dada la velocidad de retrasmisión de mensajes, circulan a menudo rumores falsos o correos con contenido difamatorio que solicitan al receptor que reenvíe el correo para dar a conocer el contenido. No participe reenviando este tipo de mensajes.
- Enviar correos electrónicos masivos cuyo contenido no se ajuste a actividades relacionadas con el SALUD. Son ejemplos de este tipo de contenidos los juegos, animaciones, tarjetas de felicitación, ficheros de música, videos, etc.

Se consideran **criterios de buenas prácticas** en el uso del correo electrónico los siguientes:

- No abrir ni ejecutar ficheros que se reciban por correo electrónico especialmente si proceden de un remitente desconocido, salvo que se tenga la total certeza de su inocuidad, y siempre después de revisarlo con el programa antivirus.
- Tener en cuenta todas las medidas de seguridad indicadas al utilizar el correo electrónico para transmitir mensajes que contengan o lleven adjuntos, datos de carácter personal, que por sus características, volumen o destinatarios pudieran poner en peligro la confidencialidad.
- Ser profesional y cuidadoso en lo que se escribe, sobre todo, cuando dichos correos electrónicos se dirijan a contactos del SALUD. Para ello, lea cuidadosamente el texto del mensaje antes de enviarlo para evitar malas interpretaciones.
- Asegurar que los destinatarios de su correo son EXCLUSIVAMENTE las personas interesadas en el asunto del mismo.

- En el envío de correo hacia terceros, tratar de proteger su dirección de correo y la de los compañeros siempre que sea posible. La difusión de virus y spam se realiza a partir de direcciones de correo válidas. Evitar por tanto el reenvío de mensajes donde aparezcan las direcciones de correo de otros compañeros como parte del mensaje.
- En el reenvío de correo, revisar el cuerpo del mensaje, para no revelar a personas extrañas contenidos internos o confidenciales. El "reenvío de correo" debe siempre hacerse previa revisión del contenido integro del mensaje. En mensajes que hayan sido reenviados a usted, evitar que aparezca la secuencia de reenvíos en el texto del mensaje.
- Intentar no hacer pública tu dirección de correo del SALUD salvo a contactos profesionales.
- Leer y entender la política de privacidad cuando se suministre la dirección de e-mail en un sitio Web. Mirar si la política de privacidad permite a la compañía vender a terceras personas tu correo. Si esto fuera así, no envíe su dirección de correo a estos sitios. Si no existe Política de Privacidad, le parece sospechosa o no tiene claro quién es el responsable de un Web mejor no dar el e-mail.
- Evitar el envío o almacenamiento en la cuenta de correo de ficheros que no estén relacionados con el trabajo. Normalmente correos con bromas, presentaciones PowerPoint o videos humorísticos consumen recursos corporativos en almacenamiento que no estén relacionados con el uso y destino de los sistemas de información del SALUD. Si se reciben este tipo de correos, eliminar el mismo una vez recibido o leído.
- El correo electrónico no es un sistema de almacenamiento de información sino de intercambio y comunicación. Por tanto, los documentos y archivos necesarios para el trabajo deben guardarse en carpetas de trabajo, no en el buzón de correo.
- Elimine periódicamente todos aquellos correos innecesarios o cuya información haya caducado y no sea útil. El buzón de correo tiene un tamaño limitado y por tanto, debe gestionar adecuadamente su uso.

## 2.6. NORMAS Y CRITERIOS DE BUENAS PRÁCTICAS APLICABLES AL USO DE LAS UNIDADES DE RED

Cada empleado de SALUD con acceso a activos de información posee un usuario con el que tiene privilegios para acceder a información compartida en la red del SALUD. Esta información se organiza en una serie de unidades de red que se mapean automáticamente cuando se inicia sesión en el dominio de Windows correspondiente. Dichas unidades son de carácter público, departamental o privado.

Cada usuario únicamente posee permisos de acceso a dichas unidades, por lo que está prohibido el acceso al resto de unidades.

Existe un backup de las unidades de red, por lo que es vital que la información que se almacene en las mismas sea estrictamente profesional y se revise periódicamente para evitar saturaciones de capacidad.

## 2.7. NORMAS Y CRITERIOS DE BUENAS PRÁCTICAS SOBRE LA GESTIÓN DE CONTRASEÑAS

Mediante el acceso al portal del empleado, cada usuario podrá modificarse su contraseña de acceso. La contraseña se modificará en los sistemas de la siguiente lista en los que el usuario disponga de cuenta:

- Correo electrónico
- Portal del empleado
- Acceso a PC y unidades de red (SAMBA)
- Directorio activo del SALUD
- Directorio OID del SALUD

**La contraseña debe cumplir los siguientes requisitos**:

- Debe ser diferente de la antigua
- Debe tener una longitud mínima de 8 caracteres
- No debe contener partes significativas del nombre de usuario
- Debe contener caracteres de al menos tres de los siguientes cuatro grupos:
    - Letras minúsculas, de la "a" a la "z".
    - Letras mayúsculas, de la "A" a la "Z".
    - Caracteres numéricos del "0" al "9"
    - Caracteres no alfabéticos, por ejemplo ".", "!", "$", "&" ...
- No pueden reutilizarse las 6 últimas contraseñas
- Distinguir mayúsculas de minúsculas

Ejemplo de contraseñas válidas: Mmigo.77, q3-lomas, 2003.Abt
Ejemplo de contraseñas no válidas: Mmigo, usuario7, Aragon

(*) La contraseña tiene asociados unos **periodos de validez**:

- El tiempo máximo de validez de la contraseña es de 90 días, pasados los cuales deberá cambiarse.
- Se establece un periodo de gracia de 15 días (posteriores a los 90 de validez) dentro de los cuales puede cambiarse la contraseña pero el acceso a los sistemas estará bloqueado.
- El tiempo mínimo de vida de la contraseña es de 3 días, en los que no podrá volver a cambiarse

Se consideran criterios de buenas prácticas respecto a la selección y utilización de contraseñas los siguientes:

- Mantener la confidencialidad de las contraseñas.
- Evitar el guardar un registro de la claves (por ejemplo en papel, en un fichero de software o en un dispositivo manual), a menos que este pueda ser almacenado de forma segura.
- Cambiar las contraseñas siempre que haya cualquier indicación de posible compromiso en el sistema o en la contraseña.
- Cambiar las contraseñas temporales en la primera entrada.
- No usar la misma contraseña para propósitos profesionales que para no profesionales.
- Seleccionar contraseñas de calidad que cumplan los requisitos pero que:
    - sean fáciles de recordar
    - no estén basadas en algo que alguien más pueda fácilmente adivinar u obtener usando la información relativa a la persona, por ejemplo nombres, números de teléfono, y fechas de nacimiento.

- no sean vulnerables a ataques de diccionario (por ejemplo, que no consistan en palabras incluidas en diccionario)
- no contengan caracteres consecutivos, idénticos, todos numéricos o todos alfanuméricos. No utilizar caracteres repetidos, bien todo números o todo letras (como lo son 123456, aaaaaaa, qwertyuiop, etc).

Como recomendaciones de contraseñas de calidad se sugieren las siguientes:

- Utilizar reglas nemotécnicas: LleSeupm (La lluvia en Sevilla es una pura maravilla)
- Cambiar una palabra de orden: aremlap (palmera al revés)
- Mezclar palabras: SagoCaos (Dos primeras letras y dos últimas letras de los nombres de los hijos/hermanos/padres) (Santiago y Carlos)
- Usar caracteres para recordar frases: esto-es-solo-un-ejemplo.
- Sustituir números por letras como el 4 por la letra A, el 0 por la o y el 1 por la letra i: Buen4c0ntr4señ4.

# 3 ANEXO A: TIPOS DE INFORMACION

- **Confidencial:** aquella información sensible cuya revelación, pérdida e indisponibilidad puede representar un riesgo no aceptable y cuyo acceso debe ser expresamente autorizado por el propietario del activo y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales. Toda información cuyo nivel de seguridad establecido por el R.D. 1720/2007 de desarrollo de la Ley de Protección de Datos sea determinado ALTO será clasificada como "confidencial" y deben aplicarse además las medidas de seguridad contempladas para el nivel que corresponda según el R.D. 1720/2007 de desarrollo de la LOPD.
- **Uso interno:** aquella cuya revelación, indisponibilidad y pérdida suponga un riesgo aceptable para la seguridad de la información.
- **Uso público:** aquella cuya disponibilidad, revelación y pérdida no supone ningún riesgo para la seguridad de la información. Cualquier información de carácter personal no podrá ser clasificada como información de carácter público

Zaragoza, 13 de mayo de 2010

EL DIRECTOR DEL CENTRO DE GESTIÓN INTEGRADA

DE PROYECTOS CORPORATIVOS

Carlos Barba Mir