ORG.2 - Normativa de Seguridad

1. Objetivo

La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para Juaneda Hospitales:

- **Facilitar y agilizar** la tramitación de procedimientos administrativos mediante herramientas informáticas y aplicaciones de gestión.
- **Proporcionar información** completa, homogénea, actualizada y fiable.

El uso de equipamiento informático y de comunicaciones es una necesidad en cualquier organización. Estos medios se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, por lo que corresponde a Juaneda Hospitales determinar las **normas, condiciones y responsabilidades** bajo las cuales deben utilizarse.

Por tanto, el presente documento tiene como objetivo **establecer normas** encaminadas a alcanzar la mayor eficacia y seguridad en el uso de dichos recursos.
Documento de uso interno: No podrá ser divulgado salvo autorización expresa del Responsable de Seguridad.

---

2. Ámbito de aplicación

Esta normativa es de aplicación y de obligado cumplimiento para:

- Todo el personal o usuarios que, de manera permanente o eventual, preste servicios o trabaje internamente en Juaneda Hospitales.
- Personal de **proveedores externos**, cuando sean usuarios de los Sistemas de Información de Juaneda Hospitales.

Cuando estos usuarios actúen como **integradores de tecnología** en el sistema, será obligatorio cumplir este documento y el **documento de normativa de usuarios avanzados**.

3. Vigencia

El presente documento ha sido aprobado por el **Comité de Seguridad**, estableciendo las directrices generales para el uso adecuado de los recursos de tratamiento de información puestos a disposición de los usuarios, quienes asumen las obligaciones descritas y se comprometen a cumplirlas.
Cualquier modificación posterior entrará en vigor **inmediatamente** después de su publicación.

---

4. Revisión y evaluación

La gestión de esta normativa corresponde al **Comité de Seguridad**, competente para:

- Interpretar dudas que puedan surgir en su aplicación.
- Revisar el documento cuando sea necesario para actualizar su contenido o por cumplimiento de plazos máximos.
- Verificar su efectividad.

El documento se someterá a **revisión y aprobación anual** si existiesen modificaciones.

La revisión se orientará a:

- Identificación de oportunidades de mejora en la gestión de la seguridad de la información.
- Adaptación a cambios en el marco legal, infraestructura tecnológica, organización, etc.

El **Responsable de Seguridad** es la persona encargada de la **custodia y divulgación** de la versión aprobada.

---

5. Referencias y marco normativo

El marco normativo aplicable incluye todas aquellas normas que integren la seguridad de la información en el ámbito del servicio prestado por la organización, en especial:

- **Esquema Nacional de Seguridad (ENS)**
- Cualquier norma derivada o relacionada con el ENS.

6. Sanciones e incumplimientos

Todos los usuarios del Sistema de Gestión de Seguridad de la Información (**SGSI**) están obligados a cumplir y aceptar lo prescrito en este documento.

El incumplimiento manifiesto de acciones contrarias a esta normativa, especialmente las relacionadas con el marco normativo, podrá conllevar:

- Inicio de medidas disciplinarias.
- Responsabilidades legales correspondientes.
- Suspensión temporal o definitiva del uso de los recursos informáticos asignados.

---

7. Uso de equipos tecnológicos y comunicaciones

Juaneda Hospitales facilita a los usuarios que lo precisen los equipos tecnológicos y dispositivos de comunicaciones (fijos o móviles) necesarios para su actividad profesional.

Todo lo integrado o utilizado por estos equipos (datos, dispositivos, programas, servicios, etc.) se debe utilizar **exclusivamente con fines profesionales**.

- Queda **estrictamente prohibido** cualquier uso distinto al autorizado o de ámbito personal.
- Las autorizaciones excepcionales deberán estar aprobadas por:
  - El responsable del departamento correspondiente, y
  - El responsable de tecnologías.

---

8. Directrices generales

8.1 Tecnologías y usuarios (RS)

- Los equipos tecnológicos serán asignados por el **Departamento de Informática**, encargado de su mantenimiento y revisión periódica.
- Los usuarios son responsables de:
  - Los equipos asignados.
  - Las cuentas de usuario entregadas o puestas a su disposición.
- Los usuarios deberán custodiar debidamente los equipos, leer y firmar esta normativa antes de su aceptación.
- Se aplica una estrategia de **mínimo privilegio**:
  - Cualquier permiso especial requerirá autorización previa de los responsables.

- Si el personal de ciberseguridad detecta anomalías o uso incorrecto, lo comunicará al Comité de Seguridad para adoptar medidas correctoras.
- Todos los usuarios recibirán concienciación o formación en ciberseguridad según sus funciones.
- Todos los equipos tecnológicos (sobremesas, portátiles, pantallas, pizarras, flipcharts, etc.) deberán apagarse al finalizar la jornada por seguridad y eficiencia energética.

8.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Existe un órgano consultivo y estratégico para la toma de decisiones en materia de seguridad de la información denominado:

- **Comité de Seguridad de la Información**

8.3 Identificación, acceso y firma en los sistemas de información y datos

- La generación de un usuario será iniciada por el **Departamento de Recursos Humanos**.
- El acceso a los sistemas requerirá autenticación **MultiFactor (MFA)**:
  - Usuario
  - Contraseña
  - Otro factor adicional

Reglas de uso de credenciales

- Está prohibido revelar o entregar credenciales o tarjeta criptográfica a terceros.
- Está prohibido mantener credenciales anotadas a la vista o accesibles.
- Está prohibido usar el acceso autorizado de otro usuario, aunque exista consentimiento del titular.
- La información alojada en los sistemas tendrá un **responsable asignado** para conceder o revocar accesos autorizados.

Política de contraseñas robustas

Todas las contraseñas deberán cumplir:

- Longitud mínima: **12 caracteres**.
- No debe contener (parcial o totalmente) el nombre de usuario.
- Debe contener al menos **3 de 4** conjuntos:
  - Mayúsculas
  - Minúsculas
  - Números
  - Símbolos/caracteres especiales
- No debe basarse en datos personales (nombre, apellidos, fecha de nacimiento, teléfono, etc.).
- No debe ser refranes, frases famosas, letras de canciones o frases de películas/obras literarias.
- No podrá ser igual a ninguna de las **5 últimas contraseñas**, ni concatenación de ellas.
- Debe cambiarse si existe evidencia de compromiso.
- Prohibido apuntarla en papel o contenedores no seguros.
- Se cambiará con una periodicidad definida.
- Queda prohibido acceder con credenciales de otros usuarios incluso si se conoce la contraseña.

Firma y certificados digitales

Los usuarios podrán firmar y autenticarse con certificados digitales para su trabajo, conforme al procedimiento de criptografía aplicable.

8.4 Equipos tecnológicos para usuarios

- Los equipos proporcionados por la organización son exclusivos para fines profesionales.
- Solo personal autorizado puede:
  - Distribuir, instalar o desinstalar software/hardware
  - Modificar configuraciones
- Los usuarios deberán notificar lo antes posible cualquier comportamiento anómalo, incidente o riesgo de seguridad.
- Para instalar dispositivos no provistos por la organización se requerirá autorización previa.
- El usuario deberá bloquear el puesto de trabajo (PC, portátil, móvil, etc.) cada vez que se ausente, aunque sea por segundos.
- Prohibida la conexión a la red de equipos no autorizados.
- Cualquier uso de componentes tecnológicos fuera de la organización requerirá autorización.
- Prohibida cualquier conexión de acceso remoto desde el exterior sin autorización previa.
- En teletrabajo se aplicará esta normativa igual que en instalaciones.

- En general, los portátiles no deberán conectarse directamente a redes externas (incluyendo internet del domicilio).
- Los equipos que salgan fuera deben:
  - Estar vigilados y bajo control del usuario
  - Transportarse de forma segura
  - Evitar exposición de información (visual o audible) a personas no autorizadas

8.5 Equipos personales (BYOD)

Los dispositivos personales (BYOD) deberán utilizarse únicamente para fines autorizados por la organización y sólo por usuarios expresamente autorizados.

---

9. Tratamiento de la información

9.1 Clasificación de la información

- Toda la información contenida o que circule por los sistemas/redes es propiedad de Juaneda Hospitales.
- Está prohibido incumplir el procedimiento de clasificación.
- Existe un procedimiento con niveles de clasificación de obligado cumplimiento.
- Está prohibido el uso, reproducción, cesión, transformación o comunicación pública de obras protegidas (propiedad intelectual o por clasificación) sin autorización.

9.2 Manejo y tratamiento de la información

- Prohibido tratar, almacenar o usar información privada que no sea necesaria para la actividad profesional.
- Prohibido el uso de memorias USB salvo autorización.
- **Puesto despejado (clean desk):**
  - Mantener solo lo necesario.
  - Al finalizar la jornada, recoger todo y custodiar bajo llave si es sensible.
- Tras el uso, el material se guardará en lugar cerrado cuando sea posible.
- Los usuarios recibirán formación sobre datos personales y deberán garantizar privacidad y cumplimiento normativo vigente (europeo y nacional).
- La información se manejará según el nivel autorizado; para otros niveles se requerirá autorización previa.
- Se realizará limpieza de metadatos para datos a publicar conforme al procedimiento de limpieza de metadatos.

9.3 Almacenamiento de la información

- La información sólo podrá almacenarse en dispositivos habilitados por la organización.
- Prohibido almacenarla en dispositivos no verificados o no autorizados.
- El usuario será responsable de la información extraída fuera de la organización.

9.4 Impresoras, digitalización, fotocopiadoras y faxes

- Imprimir únicamente lo estrictamente necesario.
- Preferentemente a doble cara y evitando color.
- Usar impresoras/fotocopiadoras en red propiedad de la organización y autorizadas.
- Evitar que la documentación permanezca en bandejas de salida.
- Retirar originales tras copiar/escaneo.
- Si se encuentra documentación sensible abandonada:
  - Intentar localizar al propietario
  - Si no se localiza, comunicarlo inmediatamente a la organización
- Documentos por fax: retirar inmediatamente.
- Al digitalizar, revisar cuidadosamente el destino (email, carpeta, etc.).
- En caso de error, notificar inmediatamente.
- Por razones ecológicas y de seguridad, verificar la necesidad real antes de imprimir.

9.5 Pizarras y flipcharts

Antes de abandonar salas o permitir acceso a terceros:

- Limpiar adecuadamente pizarras y flipcharts.
- Evitar dejar información sensible reutilizable por atacantes.

---

10. Propiedad intelectual

- Prohibida la utilización de software sin licencia de uso.
- El software propio o licenciado está protegido por la legislación de propiedad intelectual.
- Prohibida su reproducción, modificación, cesión, transformación o comunicación salvo que el licenciamiento lo permita y exista autorización previa.
- Por tanto, para utilizarlo con la IA, está prohibido la utilización de información con propiedad intelectual, confidencial

11. Confidencialidad

Toda persona (interna o externa) que por razón de su actividad haya accedido a información gestionada por Juaneda Hospitales (datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberá mantener:

- **Reserva absoluta por tiempo indefinido**
- Prohibida su divulgación salvo autorización

Está prohibido el uso exterior de información (en soporte electrónico o cualquier medio) no autorizada previamente.

Dentro de la organización:

- No se difundirá información a quienes no deban conocerla por sus funciones o autorización.

El deber de confidencialidad es exigible:

- Durante la relación profesional/laboral/formativa
- Tras su finalización

Aplica también a terceras partes, incluido personal subcontratado.
La negativa a aceptar este punto es un obstáculo grave para mantener la confianza, pudiendo implicar:

- Veto para desarrollar actividades dentro de Juaneda Hospitales.

---

12. Contratación

Los contratos con entidades prestadoras de servicios deberán incluir la obligación de aceptación de:

- Normativa de usuarios
- Normativa de usuarios avanzados
- POC (Punto de Comunicación)
- Cualquier otra documentación requerida por el Responsable de Seguridad (intercambio de información, retirada de material por terceros, supervisión, revisión de acuerdos, etc.)

13. Acceso a Internet, otras herramientas y correo electrónico

13.1 Acceso a internet y otras herramientas

Internet es un recurso para el desempeño laboral y propósito profesional.

- Prohibido suplantar la identidad de usuarios en internet, correo o herramientas colaborativas.
- Prohibido la utilización de cualquier IA que no esté aprobada por la organización.
- Prohibido visitar páginas:
  - Poco éticas, pornográficas, no fiables, sospechosas, ofensivas o ilegales
- Prohibido instalar complementos en el navegador sin autorización.
- Prohibido descargar archivos/programas/código voluminoso o sospechoso, especialmente en horarios de atención al público, salvo autorización.
- Tras finalizar el trabajo, cerrar sesiones abiertas en aplicaciones.
- Prohibido publicar en redes o medios contenidos que contravengan normativas (protección de datos, honor, intimidad, imagen, propiedad intelectual, etc.).
- Cookies:
  - Prohibido aceptar cookies salvo las necesarias para el funcionamiento del servicio de la web.

13.2 Correo electrónico

- El correo corporativo se utilizará única y exclusivamente para funciones profesionales.
- Solo podrán usarse herramientas de correo suministradas, instaladas y configuradas por la organización.
- Prohibido el envío o reenvío masivo.
- Prohibido:
  - Abrir, contestar, reenviar o ejecutar spam/correos con virus y adjuntos
- Prohibido usar el correo como almacenamiento; usar los sistemas corporativos habilitados.
- Notificar a la organización anomalías y correos no deseados para ajustar medidas de seguridad.
- Adjuntos:
  - No abrir ficheros de fuentes no fiables
  - En caso de duda, notificar a la organización

14. Incidencias o incidentes de seguridad

Si un usuario detecta una anomalía o incidencia que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información o la imagen de la organización, deberá:

- Informar **inmediatamente** a la organización
- La organización lo registrará y lo elevará según corresponda

---

15. Específicamente prohibidos

Quedan prohibidos:

- Instalación y/o uso de programas, hardware o contenidos que vulneren propiedad intelectual, normas vigentes o supongan amenaza para la organización.

Este comportamiento podrá conllevar responsabilidades disciplinarias, administrativas, civiles o penales conforme a la ley.

---

16. Análisis y monitorización de seguridad

Juaneda Hospitales, por motivos legales, de seguridad y calidad, y cumpliendo requisitos legales aplicables, dispone de sistemas de ciberseguridad que monitorizan el estado del SGSI, incluyendo:

- Revisión periódica del estado de equipos, software instalado, dispositivos y redes de comunicaciones.
- Monitorización de accesos a información y redes.
- Auditoría de seguridad de credenciales y aplicaciones.
- Monitorización de servicios de internet, correo y herramientas colaborativas.

17. Aceptación

La persona firmante (en adelante, el usuario) declara haber leído y entendido las condiciones establecidas en la presente normativa y en la política de seguridad de la organización, manifestando su conformidad y aceptación, así como su compromiso de aplicación dentro de la organización.