REGISTRO DE ACTIVIDADES DEL CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (RAT) COMO RESPONSABLE DE TRATAMIENTO

CONSEJO GENERAL DE ENFERMERÍA

Registro de Actividades de Tratamiento elaborados de acuerdo con los requisitos del art. 30 REGLAMENTO (UE) 2016/679 GENERAL DE DATOS PERSONALES (RGPD)

ÍNDICE

1. IDENTIFICACIÓN DEL RESPONSABLE DE TRATAMIENTO

CONSEJO GENERAL DE ENFERMERÍA

CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)

DOMICILIO SOCIAL	C. de la Sierra de Pajarejo, 13, 28023 Madrid
DATOS DE CONTACTO	+34 91 334 55 20
N.I.F.	Q-2866021-E
DELEGADO DE PROTECCIÓN DE DATOS (DPO)	dpo@consejogeneralenfermeria.org

2. REGISTRO COLEGIADOS

REGISTRO COLEGIADOS	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Censo de colegiados pertenecientes a la organización colegial de enfermería. *Tratamiento automatizado.*
FINALIDAD Y BASE DE LEGITIMACIÓN	• Ejercicio de las funciones atribuidas a los Consejos Generales de los Colegios Profesionales en virtud del art. 9 de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales y Estatutos del CGE que impliquen el tratamiento de datos personales. Base de legitimación: ejercicio de función pública (art. 6.1 e) RGPD) y cumplimiento de obligaciones legales (art. 6.1c) RGPD). - Ejercicio de funciones disciplinarias y arbitrales. - Control de aportaciones económicas de los colegios profesionales. - Adopción de medidas para completar provisionalmente con los colegiados más antiguos las plazas vacantes en las Juntas de Gobierno de los Colegios Profesionales
CATEGORÍAS DE INTERESADOS	• Personas colegiadas en los distintos colegios profesionales de enfermería de España • Miembros de las Juntas de Gobierno de los colegios profesionales y del CGE
CATEGORÍAS DE DATOS	• Datos identificativos básicos (nombre y apellidos, número de colegiación) • Datos de contacto profesional (domicilio, teléfono y cuenta de correo electrónico) • Datos colegiales: altas/bajas, fecha de antigüedad

	• Datos incluidos en expedientes disciplinarios.
CATEGORÍAS DE DESTINATARIOS	• Prestadores externos de servicios auxiliares con acceso a datos personales (Encargados de Tratamiento) tales como gestorías, asesorías, entidades financieras, prestadores de servicios IT con acceso a datos personales (hosting, backup, servicios de soporte y mantenimiento informático, ciberseguridad y otros similares) • Cesionarios tales como órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	Los datos personales se conservarán mientras se mantenga la condición de colegiado y durante los seis años posteriores a la baja como colegiado. No obstante, los datos podrán ser conservados más allá de dicho período si concurren motivos justificados legalmente. La supresión de los datos se realizará de conformidad con lo establecido en la Ley 4/1993 de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002:2013: - Medidas de control de acceso físico a las instalaciones de la organización - Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. - Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. - Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles

	privados VPN) - Gestión de copias de seguridad de la información (cloud + almacenamiento local). - Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), - Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. - Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

3. GESTIÓN DE PROVEEDORES

GESTIÓN DE PROVEEDORES	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Tratamiento de datos personales referidos a proveedores (personas físicas) y a sus representantes legales y comerciales. *Tratamiento mixto.*
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión fiscal, contable y administrativa derivada de transacciones mercantiles con los proveedores. Base de legitimación: Ejecución de contrato mercantil (art. 6.1. b) RGPD) y cumplimiento de obligaciones legales/fiscales (art. 6.1 c) RGPD) en relación con la normativa en materia tributaria.
CATEGORÍAS DE INTERESADOS	• Proveedores (personas físicas) y sus representantes legales y comerciales.
CATEGORÍAS DE DATOS	• Datos identificativos básicos (nombre, apellidos, NIF, firma) • Datos de contacto profesional tratados en el ámbito de la relación contractual y comercial (domicilio, teléfono, cuenta de correo electrónico) • Datos bancarios y económicos vinculados a la transacciones mercantiles.
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales (Encargados de Tratamiento) tales como prestadores de servicios de IT (hosting, servicios de soporte y mantenimiento informático, ciberseguridad y otros similares), gestorías, asesorías fiscales/legales, entidades financieras, órganos y organismos de las Administraciones Públicas, Juzgados y

	Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	Una vez extinguida la relación contractual, los datos incluidos en contratos, facturas y demás documentos de soporte contable se conservarán durante el tiempo necesario para hacer frente a posibles responsabilidades legales y, en todo caso, durante el plazo mínimo de 6 años (art. 30 Código de Comercio).
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002:2013: - Medidas de control de acceso físico a las instalaciones de la Organización - Protección de documentación en papel mediante armarios bajo llave - Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. - Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. - Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) - Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). - Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), - Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. - Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

4. GESTIÓN DE PERSONAL

GESTIÓN DE PERSONAL	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Gestión de recursos humanos (*Tratamiento mixto)*
FINALIDAD Y BASE DE LEGITIMACIÓN	• Procesos de selección de personal. Base de legitimación: consentimiento del interesado (art. 6.1 a) RGPD) • Contratación de beneficios sociales. Base de tratamiento: ejecución de contrato laboral (art. 6.1 b) RGPD) • Acciones formativas preceptivas y optativas. Base de tratamiento: cumplimiento legal (art. 6.1 c) RGPD) y consentimiento del interesado (art. 6.1 a) RGPD). • Gestión laboral (gestión de nóminas, control horario, vacaciones, contratación, despidos, permisos, expedientes disciplinarios, etc.) y de la Seguridad Social. Base de legitimación: ejecución de contrato laboral (art. 6.1 b) RGPD) y cumplimiento de obligaciones legales (art. 6.1 c) RGPD). • Prevención de riesgos laborales. Base de legitimación: cumplimiento legal (art. 6.1 c) RGPD) en relación con la Ley 31/1995 de Prevención de Riesgos Laborales. • Coordinación de actividades empresariales. Base de legitimación: cumplimiento legal (art. 6.1 c) RGPD)
CATEGORÍAS DE INTERESADOS	• Candidatos • Empleados

	• Trabajadores externos
CATEGORÍAS DE DATOS	• Datos laborales (identificativos y de contacto, firma, nº de afiliación a la Seguridad Social, datos económicos incluidos en la nómina, estado civil, nº de hijos, fecha de nacimiento). • Datos curriculares (identificativos, académicos, profesionales).
CATEGORÍAS DE DESTINATARIOS	Prestadores de servicios auxiliares externos con acceso a datos personales (Encargados de Tratamiento) tales como empresas de selección de personal, portales de empleo, gestorías, asesorías fiscales/legales, entidades financieras; prestadores de servicios de IT (hosting, servicios de soporte y mantenimiento informático, ciberseguridad y otros similares). Cesionarios tales como entidades de formación; FUNDAE, mutua de accidentes; inspectores de trabajo; entidades receptoras de información derivadas de las obligaciones en materia de coordinación de actividades empresariales; Instituto de Seguridad e Higiene en el Trabajo y otros órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	Los datos curriculares de los candidatos se conservarán durante el plazo de un año, excepto si el candidato es contratado (en cuyo caso el CV pasará a formar parte del expediente laboral). Los datos derivados del control de jornada se conservarán durante cuatro años, de acuerdo con lo dispuesto en el art. 34.9 del Estatuto de los Trabajadores. El resto de los datos se conservarán durante al menos seis años más, en su caso, el tiempo adicional

	durante el cual se puedan derivar responsabilidades legales.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: - Medidas de control de acceso físico a las instalaciones de la Organización - Protección de documentación en papel mediante armarios bajo llave - Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. - Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. - Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). - Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), - Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. - Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

5. GESTIÓN ADMINISTRATIVA INSTITUCIONAL

GESTIÓN ADMINISTRATIVA INSTITUCIONAL	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Tratamiento de datos personales referidos a los miembros de los órganos del CGE. *Tratamiento mixto*
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión institucional interna: gestión fiscal, contable y administrativa del CGE. Cumplimiento de función pública (art. 6.1 e) RGPD) y obligaciones legales (Art. 6.1.c) RGPD) derivadas de Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales y Estatutos del CGE.
CATEGORÍAS DE INTERESADOS	• Miembros de los órganos del CGE (asamblea general, pleno, comisión ejecutiva, comisión permanente).
CATEGORÍAS DE DATOS	• Datos identificativos básicos (nombre, apellidos, DNI, firma) • Datos de contacto (domicilio, teléfono, cuenta de correo electrónico)
CATEGORÍAS DE DESTINATARIOS	Prestadores de servicios auxiliares externos con acceso a datos personales (Encargados de Tratamiento), tales como gestorías, asesorías fiscales/legales, entidades financieras, prestadores de servicios IT (hosting, servicios de soporte y mantenimiento informático, ciberseguridad y otros similares). Cesionarios tales como notarías, registros, órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS	NO

INTERNACIONALES/DESTINO	
PLAZO DE SUPRESIÓN	Los datos se conservarán mientras el interesado ostente el cargo y, posteriormente, durante los plazos de prescripciones de posibles acciones. Los datos identificativos básicos se mantendrán con fines de archivo en interés público, de acuerdo con el art. 26 LOPD-GDD.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: - Medidas de control de acceso físico a las instalaciones de la Organización - Protección de documentación en papel mediante armarios bajo llave - Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. - Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. - Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), - Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. - Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

6. COMUNICACIÓN Y EVENTOS

COMUNICACIÓN Y EVENTOS	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Tratamiento de datos personales (referidos a ponentes, invitados y suscriptores) relacionados con la organización de eventos y comunicaciones institucionales. *Tratamiento mixto.*
FINALIDAD Y BASE DE TRATAMIENTO	• Gestión de inscripción de asistentes a eventos: existencia de consentimiento del interesado (art. 6.1 a) RGPD). • Gestión de desplazamientos y alojamiento de asistentes a eventos: existencia de consentimiento del interesado (art. 6.1 a) RGPD). • Gestión de comunicaciones institucionales: existencia de interés legítimo (art. 6.1 f) RGPD) • Gestión de suscripciones a publicaciones del CGE: existencia de consentimiento del interesado (art. 6.1 a) RGPD).
CATEGORÍAS DE INTERESADOS	• Asistentes a eventos • Suscriptores
CATEGORÍAS DE DATOS	• Datos identificativos básicos y de contacto profesional
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales tales como empresas de marketing; plataformas de e-mail marketing.

	• Cesionarios tales como hoteles, empresas de transporte de pasajeros, arrendamiento de vehículos y otros servicios similares; patrocinadores, colaboradores y ponentes que participen en eventos.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	En el caso de los tratamientos basados en el consentimiento del interesado, los datos se conservarán mientras el mismo no sea revocado o hasta que los datos sean objeto de depuración en la base de datos. En el resto de los casos, se conservarán durante el plazo general de seis años (art. 30 Código de Comercio).
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: - Medidas de control de acceso físico a las instalaciones de la Organización - Protección de documentación en papel mediante armarios bajo llave - Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. - Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. - Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) - Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). - Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad).

7. VOLUNTARIOS

VOLUNTARIOS	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Estudiantes de enfermería que participan como voluntarios en la celebración de eventos
FINALIDAD Y BASE DE LEGITIMACIÓN	Organización de tareas asignadas a voluntarios durante la celebración de eventos: existencia de consentimiento (art. 6.1 a) RGPD).
CATEGORÍAS DE INTERESADOS	Voluntarios
CATEGORÍAS DE DATOS	Datos básicos identificativos y de contacto
CATEGORÍAS DE DESTINATARIOS	Prestadores de servicios auxiliares externos con acceso a datos tales como prestadores de servicios IT, empresas de organización de eventos y otros similares. No se producirán cesiones a terceros, salvo en caso de obligación legal.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	Los datos se conservarán durante el plazo máximo de un año.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002:

	• Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

8. GESTIÓN DE DERECHOS DE LOS INTERESESADOS Y REGISTRO DE VIOLACIONES DE SEGURIDAD

GESTIÓN DE DERECHOS DE LOS INTERESADOS Y REGISTRO DE VIOLACIONES DE SEGURIDAD	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Gestión de peticiones de ejercicio de derechos de los interesados en materia de protección de datos personales y gestión de violaciones de seguridad. *Tratamiento mixto.*
FINALIDAD Y BASE DE LEGITIMACIÓN	Gestión de peticiones de ejercicio de derechos de los interesados en materia de protección de datos personales y gestión de violaciones de seguridad. Base de legitimación: cumplimiento lega (art. 6.1 c) RGPD)
CATEGORÍAS DE INTERESADOS	• Interesados que soliciten alguna petición de ejercicio de derechos en materia de protección de datos personales dirigida al CGE como Responsable de Tratamiento (colegiados, proveedores, miembros de órganos institucionales, empleados, estudiantes en prácticas, trabajadores externos, voluntarios, suscriptores, asistentes a eventos, otros) • Interesados implicados o referidos en los hechos objeto de un procedimiento de gestión de violación de seguridad (colegiados, proveedores, miembros de órganos institucionales, empleados, estudiantes en prácticas, trabajadores externos, voluntarios, suscriptores, asistentes a eventos, otros.
CATEGORÍAS DE DATOS	• Datos básicos identificativos

	• Datos de contacto • Datos personales adicionales que sean objeto del derecho cuyo ejercicio se solicita • Datos personales adicionales vinculados a la violación de seguridad objeto de gestión
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios IT con acceso a datos personales • Agencia Española de Protección de Datos • Juzgados y Tribunales de Justicia
TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A
PLAZO DE SUPRESIÓN	Los datos se conservarán mientras esté vigente el plazo de prescripción de tres años establecido en el art. 78 LOPD-GDD y, en su caso, durante el tiempo adicional mientras existan procedimientos sancionadores en curso.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura,

	humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada

9. CONTROL DE ACCESO (VISITAS)

CONTROL DE ACCESO (VISITAS)	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Control de acceso a las instalaciones del CGE para personal externo (proveedores, visitas, asistentes a eventos, etc.). Seguridad física del edificio.
FINALIDAD Y BASE DE LEGITIMACIÓN	Registro y control de las personas que acceden a las instalaciones del edifico. Base de legitimación: interés legítimo (art. 6.1 f) RGPD)
CATEGORÍAS DE INTERESADOS	• Interesados que quieran acceder a las instalaciones del CGE (proveedores, colegiados, visitas, asistentes a eventos, otros).
CATEGORÍAS DE DATOS	• Datos básicos identificativos • Datos de contacto • Datos profesionales –en su caso-
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios IT con acceso a datos personales • Agencia Española de Protección de Datos • Juzgados y Tribunales de Justicia • Empresas de seguridad

TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A
PLAZO DE SUPRESIÓN	Los datos se conservarán durante un mes desde el acceso de la visita.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada

10. HUELLA DACTILAR

HUELLA DACTILAR	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Tratamiento de la huella dactilar captadas por los dispositivos habilitados al efecto en la entrada y accesos a determinadas zonas de las instalaciones.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Seguridad. Base de legitimación: interés legítimo (art. 6.1 f) RGPD) • Fichaje. Base de legitimación: obligación legal (art.6.1 c) RGPD)
CATEGORÍAS DE INTERESADOS	• Empleados
CATEGORÍAS DE DATOS	• Huella dactilar (datos biométricos)
CATEGORÍAS DE DESTINATARIOS	• Proveedor de la herramienta • Cuerpos y Fuerzas de Seguridad del Estado • Juzgados y Tribunales de Justicia
TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A
PLAZO DE SUPRESIÓN	La plantilla biométrica de la huella dactilar será conservada hasta el cese del empleado. Los datos relativos al registro de control horario de jornada se guardarán durante cuatro años, de acuerdo con el art. 34.9 del Estatuto de los Trabajadores.

MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

11. VIDEOVIGILANCIA

VIDEOVIGILANCIA	
ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Captación y grabación de imágenes. Seguridad física de personas, bienes e instalaciones.
FINALIDAD Y BASE DE LEGITIMACIÓN	Seguridad física de personas de personas, bienes e instalaciones. Base de legitimación: interés legítimo (art. 6.1 f) RGPD)
CATEGORÍAS DE INTERESADOS	• Empleados • Potenciales clientes • Clientes • Proveedores • Visitas
CATEGORÍAS DE DATOS	• Imágenes
CATEGORÍAS DE DESTINATARIOS	• Prosegur S.A. • Cuerpos y Fuerzas de Seguridad del Estado • Juzgados y Tribunales de Justicia
TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A
PLAZO DE SUPRESIÓN	Un mes desde la captación.

MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

12. PREMIOS INVESTIGACIÓN ENFERMERA

ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE) Corresponsable: FUNDACIÓN INSTITUTO ESPAÑOL DE INVESTIGACIÓN ENFERMERA
BREVE DESCRIPCIÓN	Gestión de los participantes en concursos de investigación promovidos por el Instituto de Investigación Enfermera.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión concurso: necesidad para la ejecución de contrato (art. 6.1 b) RGPD) • Comunicaciones comerciales: existencia de interés legítimo (art. 6.1 f) RGPD)
CATEGORÍAS DE INTERESADOS	• Participantes concurso • Ganadores de la/s beca/s • Participantes del proyecto/memoria presentada
CATEGORÍAS DE DATOS	• Datos básicos identificativos y de contacto. • Datos académicos y profesionales. • Datos económicos.
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales tales como prestadores de servicios IT • Entidades financieras, órganos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A

PLAZO DE SUPRESIÓN	Los datos serán conservados durante el concurso y hasta la prescripción de posibles responsabilidades legales derivadas del mismo.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

13. TALONARIO ÓRDENES DE DISPENSACIÓN

ENTIDAD RESPONSABLE	CONSEJO GENERAL DE COLEGIOS OFICIALES DE ENFERMERÍA DE ESPAÑA (CGE)
BREVE DESCRIPCIÓN	Tratamiento de datos relativo a los talonarios de órdenes enfermeras de dispensación.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión de las solicitudes de entrega de talonarios de órdenes enfermeras de dispensación
CATEGORÍAS DE INTERESADOS	• Colegiados/as
CATEGORÍAS DE DATOS	• Datos básicos identificativos y de contacto. • Datos profesionales. • Datos económicos.
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales tales como prestadores de servicios IT • Órganos de las Administraciones Públicas cuando sea legalmente preceptivo
TRANSFERENCIAS INTERNACIONALES/DESTINO	N/A
PLAZO DE SUPRESIÓN	Los datos serán conservados hasta la prescripción de posibles responsabilidades legales.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002:

	• Medidas de control de acceso físico a las instalaciones de la Organización • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.