Política de Seguridad de la Información - ENS

INFORMACIÓN PÚBLICA

Control de Ediciones

Normativa de Organización de la Seguridad de la Información			
Revisión	**Fecha**	**Modificado por**	**Modificación**
0	12-12-23	Responsable de Seguridad	Creación.
1	20-03-24	Responsable de Seguridad	Actualización
1.1	20-04-24	Responsable de Seguridad	Actualización de referencias normativas y firma

INFORMACIÓN PÚBLICA

Índice de Contenidos

INFORMACIÓN PÚBLICA

1 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 5 de febrero de 2024 por el Comité de Seguridad y actualizado en el día 20 de marzo de 2024 por el Responsable de Seguridad.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2 INTRODUCCIÓN

DIAVERUM depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que **DIAVERUM** debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

DIAVERUM debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

DIAVERUM debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

2.1 PREVENCIÓN

DIAVERUM debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello **DIAVERUM** debe implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **DIAVERUM** debe:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 RESPUESTA

DIAVERUM debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 CONSERVACIÓN

Para garantizar la disponibilidad de los servicios críticos, **DIAVERUM** debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3 ALCANCE

Gestión de los Sistemas de Información que tratan los datos de las historias clínicas de los pacientes a partir de las diálisis realizadas en los centros de hemodiálisis.

4 MISIÓN

La misión de **DIAVERUM** es mejorar la calidad de vida de los pacientes renales.

INFORMACIÓN PÚBLICA

DIAVERUM es consciente de la relevancia de una efectiva gestión de un Sistema de Seguridad de la Información, basado en el Esquema Nacional de Seguridad de manera particular para el alcance definido.

En **DIAVERUM la información es un activo fundamental** para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un **compromiso expreso de protección** de sus propiedades más significativas como parte de una estratégica orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La Política de Seguridad se define como aquel conjunto de directrices plasmadas en documento escrito, que rigen la forma en que la organización **gestiona y protege la información** y los servicios que considera críticos.

5 MARCO NORMATIVO

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD).
- Real Decreto 1030/2006, de 15 de septiembre, sobre la Cartera de Servicios comunes al Sistema Nacional de Salud, Real Decreto-Ley 16/2012 de 20 de abril de Medidas Urgentes para Garantizar la Sostenibilidad del Sistema Nacional de Salud y Mejorar la calidad y Seguridad de las Prestaciones, Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios. Anexo III, Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, Decreto 24/2008, de 3 de abril, del Consejo de Gobierno, modificado por Decreto 211/2015, de 29 de septiembre, Orden 1158/2018, de 7 de noviembre, del Consejero de Sanidad, por la que se regulan los requisitos técnicos generales y específicos de los centros y servicios sanitarios sin internamiento, de los servicios sanitarios integrados en una organización no sanitaria y de la asistencia sanitaria prestada por profesionales sanitarios a domicilio en la Comunidad de Madrid, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, Diario Oficial de la Unión Europea L 117, de 5 de mayo de 2017.
- Reglamento (UE) 2020/561 del Parlamento Europeo y del Consejo de 23 de abril de 2020 por el que se modifica el Reglamento (UE) 2017/745 sobre los productos sanitarios en relación con las fechas de aplicación de algunas de sus disposiciones.
- Real Decreto 192/2023, de 21 de marzo, por el que se regulan los productos sanitarios O en su defecto Certificado de cumplimiento de:
  - R.D. 1591/2009 de 16 de octubre por el que se regulan los productos sanitarios
  - Directiva y 93/42/CEE del Consejo de 14 de junio de 1993 relativa a los productos sanitarios DO L 169 de 12 de julio de 1993.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos- RGPD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- LSSI - Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- ITS de Conformidad con el Esquema Nacional de Seguridad y del Informe del Estado de la Seguridad (BOE del 2 de noviembre de 2016): Instrucción técnica que establece los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.
- Instrucción Técnica de Seguridad de Auditoría (BOE del 3 de abril de 2018): Instrucción técnica que establece las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): Ley que adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, completa sus disposiciones, y garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.
- Otra legislación de obligado cumplimiento de la Administración Pública.

6 ORGANIZACIÓN DE SEGURIDAD

El documento NOR-DI.01 Normativa de Organización de la Seguridad de la Información describe detalladamente los diferentes roles, incluyendo sus funciones y responsabilidades.

6.1 DEFINICIÓN DE COMITÉS Y ROLES UNIPERSONALES

- Comité de Seguridad de la Información (CSI)
- Responsable del SSI o Responsable de Seguridad (según ENS)
- Responsable del Sistema
- Responsable del Servicio
- Responsable de la Información
- Responsabilidades sobre la Protección de Datos Personales

6.2 FUNCIONES

- Comité de Seguridad de la Información (CSI).

  El Comité de Seguridad de la Información es la máxima autoridad del SSI (Sistema de Gestión de la Seguridad de la Información) que coordina la Seguridad de la Información a nivel de organización y tiene la responsabilidad de tomar las decisiones finales sobre el establecimiento, implantación, mantenimiento y mejora del Sistema de Seguridad de la Información.

  El Comité está formado como mínimo por:

  - Un miembro de la Dirección (por ejemplo el Director B.U. Tecnológica o el Director Operaciones).
  - El Responsable de Seguridad.
  - El Responsable del Sistema.
  - El Responsable del Servicio
  - El Responsable de la Información
  - Delegado de Protección de Datos.

  El Comité de Seguridad de la Información puede incluir, o invitar a sus reuniones, a otras personas, por ejemplo, a los Responsables de otros departamentos, Técnicos de Mantenimiento, Responsables de Desarrollo, Directores de Clínicas, etc..

6.3 RESPONSABILIDADES

- Comité de Seguridad de la Información (CSI)
  - Definir, aprobar, implementar y control continuado de:
    - La Política de Seguridad de la Información y sus objetivos.
    - Aprobar los criterios de apreciación y aceptación de los riesgos de Seguridad de la Información.
    - Niveles y perfiles de riesgo aceptables (riesgo residual).
    - Planes de actuación vigentes en cada momento.
  - Aprobar las acciones que se consideren oportunas ante modificaciones consideradas significativas en la valoración/apreciación de riesgos de los Activos de la entidad.
  - Revisar y aprobar los documentos “Contexto para el SSI” y el “Manual del SSI”.
  - Revisar el análisis de incidencias de Seguridad del Sistema.
  - Promover la mejora continua del SSI.
  - Aprobar el Informe de Revisión del SSI.
  - Asume la función de Responsable de la Información (como órgano colegiado).

- Asume la función de Responsable del Servicio (como órgano colegiado).

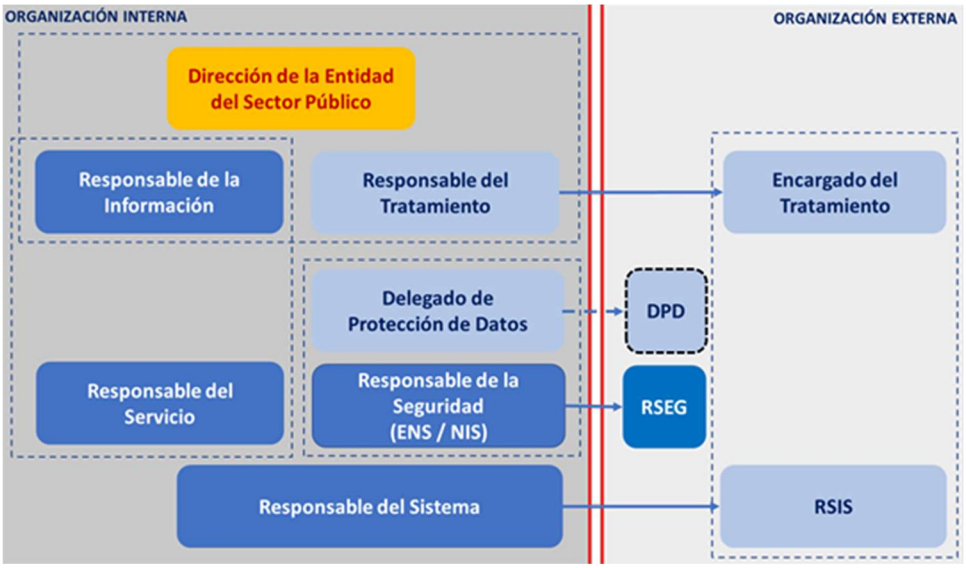
- Responsable de Seguridad (Responsable del SSI)
  - El responsable de la Seguridad de la Información es la persona que se va a encargar de coordinar y aprobar todas las actuaciones en materia de seguridad dentro DIAVERUM, de acuerdo a lo establecido en la Política de Seguridad de la Información.
  - Convocar al Comité de Seguridad.
  - Impulsar la cultura en Seguridad de la Información, gestionando y promoviendo la formación y concienciación en materia de seguridad.
  - Establecer los requisitos de la información en materia de seguridad, esto es, determinar los niveles de Seguridad de la Información.
  - Participar en la categorización de los sistemas y el análisis de riesgos.
  - Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.
  - Mantener el nivel adecuado de Seguridad de la Información manejada y de los servicios prestados por los sistemas.
  - Revisar y aprobar toda la documentación relacionada con la Seguridad del Sistema.
  - Realizar o promover las auditorías periódicas a las que obliga El Marco Normativo para verificar el cumplimiento de los requisitos del mismo, así como realizar el seguimiento de las acciones correctivas y de mejora que se establezcan para resolver las desviaciones detectadas.
  - Acompañar y facilitar a los auditores de certificación el acompañamiento por las instalaciones y el apoyar en la localización de documentación y registros del SSI.
  - Determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.
  - Determinar las excepciones cuando lo justifiquen las exigencias de proporcionalidad en cuanto a los riesgos asumidos en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.
  - Aprobar la Declaración de Aplicabilidad. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto.
  - Analizar los informes de autoevaluación y/o los informes de auditoría y elevar las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

- Responsable del Sistema

  - Operar el sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
  - Analizar las conclusiones del Responsable de la Seguridad sobre los informes de autoevaluación y/o los informes de auditoría para adoptar las medidas correctoras adecuadas.
  - (Sólo en el caso de sistema de categoría ALTA) Visto el dictamen de auditoría, acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
- Responsable de la Información
  - Determinar los requisitos (de seguridad) de la información tratada.
  - Aprobar los niveles de seguridad de la información.
  - Valorar las consecuencias de un impacto negativo sobre la seguridad de la información, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de las personas.
- Responsable del Servicio
  - Determinar los requisitos (de seguridad) de los servicios prestados.
  - Aprobar los niveles de seguridad de los servicios.
  - Definir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
  - Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de las personas.
- Responsabilidades sobre la Protección de Datos Personales

  Sus responsabilidades están definidas en el Sistema de Gestión de Protección de Datos.

6.4 MECANISMOS DE COORDINACIÓN



6.5 PROCEDIMIENTOS DE DESIGNACIÓN DE PERSONAS

Es función de la Dirección de la entidad designar:

- Al Responsable de la Información, que puede ser un cargo unipersonal o un órgano colegiado (por ejemplo, el Comité de Seguridad de la Información).
- Al Responsable del Servicio, que puede ser un cargo unipersonal o un órgano colegiado (por ejemplo, el Comité de Seguridad de la Información).
- A los miembros del Comité de Seguridad de la Información.
- Al Responsable de la Seguridad, que reporta directamente al Comité de Seguridad de la Información.
- Al Responsable del Sistema, que, en materia de seguridad, reporta al Responsable de la Seguridad. Esta designación podrá ser:

El nombramiento de los responsables mencionados se hace con carácter formal, cuyas evidencias serán los Actas del Comité firmados en el momento de producirse cada nombramiento.

6.6 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política es aprobada por el Comité de Seguridad de la Información y difundida para que la conozcan todas las partes afectadas.

7 DATOS DE CARÁCTER PERSONAL

DIAVERUM trata datos de carácter personal según lo especifico en la RGPD del 14 de abril de 2016. Se han creado diferentes registros de tratamiento de datos, al que tendrán acceso sólo las personas autorizadas, donde se recogen los diferentes tratamientos de los datos de carácter personal y su ciclo del dato, así como los responsables correspondientes. Todos los sistemas de información de **DIAVERUM** se ajustan a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en los tratamientos de datos y en el análisis de riesgos de cada uno de los tratamientos.

8 CONCIENCIACIÓN Y FORMACIÓN

DIAVERUM tiene como objetivo lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros de la organización y a todas las actividades, de acuerdo al principio de Seguridad como proceso Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

9 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deben realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repite:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establece una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamiza la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de **DIAVERUM** en diferentes materias:

- PSI-DI.01 Gestión de la Documentación
- PSI-DI.02 Procedimiento de Análisis y Gestión de Riesgos del SSI
- PSI-DI.03 Procedimiento de Clasificación, Etiquetado y Protección de la Información
- PSI-DI.04 Procedimiento de Mantenimiento, Reutilización y Eliminación de Soportes de Información
- PSI-DI.05 Procedimiento de Control y Respuesta Antimalware
- PSI-DI.06 Procedimiento de Gestión de Usuarios y Contraseñas
- PSI-DI.07 Procedimiento de Gestión de Incidencias de Seguridad
- PSI-DI.08 Procedimiento de Backup y Recuperación de Datos
- PSI-DI.09 Procedimiento para la Gestión de Cambios
- PSI-DI.10 Procedimiento para la Gestión del Correo Electrónico
- PSI-DI.11 Procedimiento de Gestión y Configuración de Redes
- PSI-DI.12 Procedimiento de Navegación WEB
- PSI-DI.13 Procedimiento para la Generación y Uso de LOGS
- PSI-DI.14 Procedimiento para la identificación y Cumplimiento de la Legislación Aplicable
- PSI-DI.15 Procedimiento para la Gestión de Proyectos TIC
- PSI-DI.16 Procedimiento de Diseño y Desarrollo de SW
- PSI-DI.17 Gestión de No Conformidades y Acciones Correctivas
- PSI-DI.18 Auditoría Interna
- PSI-DI.19 Gestión de la Comunicación Interna y Externa
- PSI-DI.20 Operación y Gestión Instrucciones Técnicas
- PSI-DI.21 Uso Controles Criptográficos
- PSI-DI.22 Gestión de la Configuración
- PSI-DI.23 Limpieza de Metadatos
- PSI-DI.24 Gestión de Parches y Actualizaciones
- PSI-DI.25 Gestión de Compras IT
- NOR-DI.01 Normativa de Organización de la Seguridad de la Información
- NOR-DI.02 Normativa de Gestión de Servicios ofrecidos por terceros

- NOR-DI.03 Normativa de Buenas Prácticas en Seguridad de la Información
- NOR-DI.04 Normativa de Seguridad Física
- NOR-DI.05 Normativa de Trabajo fuera de las instalaciones
- NOR-DI.06 Normativa de Bastionado de Sistemas

Esta Política se desarrolla por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad está a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad está disponible en un recurso compartido en la red de la empresa, con acceso de lectura a todos los empleados de la empresa.

\\ESFAP02\NORMATIVASEGURIDAD

11 Obligaciones Del Personal

Todos los miembros de **DIAVERUM** dentro del alcance de esta política tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **DIAVERUM** dentro del alcance de esta política atienden a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establece un programa de concienciación continua para atender a todos los miembros de **DIAVERUM** dentro del alcance de esta política, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciben formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación es obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12 Consecuencias ante incumplimiento

Ante incumplimiento de esta Política de Seguridad de la Información por parte de cualquiera de los miembros de DIAVERUM, el Régimen Disciplinario a seguir será el estipulado en los Contratos y Acuerdos Laborales.

Las medidas legales a adoptar se coordinarán por el Departamento de RRHH una vez se haya realizado la notificación de incumplimiento por parte del Responsable de Seguridad.

13 Terceras Partes

Cuando **DIAVERUM** preste servicios a otros organismos o maneje información de otros organismos, se les hace partícipes de esta Política de Seguridad de la Información, se establecen canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecen procedimientos de actuación para la reacción ante incidentes de seguridad.

INFORMACIÓN PÚBLICA

Cuando **DIAVERUM** utilice servicios de terceros o ceda información a terceros, se les hace partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte queda sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecen procedimientos específicos de reporte y resolución de incidencias. Se garantiza que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requiere un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requiere la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

FIRMADO:

JOSÉ MARÍA ORDÓÑEZ

DAVID DÍEZ MARTÍN - RESPONSABLE DE SEGURIDAD